**CYBERYOUTH**

**Nonformal education for cyber-security training & resilience of youth organisations and young people**

***Cybersecurity online youth academy***

****

**Implementation of Security Solutions**

Table of contents

[Introduction](#_heading=h.fpb3yt6tcffi)

[What you will learn](#_heading=h.bd1t10x6k115)

[Why it is important and How it can help you in everyday life](#_heading=h.1fqj6c1n3ygs)

[What career you can pursue](#_heading=h.l25siuf1d90q)

[Pre-requisites](#_heading=h.obikvf4haym5)

[Material](#_heading=h.snpqznqbwxs)

4[.1 Secure Protocols](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

 [HTTPS](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

 [SSH](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

 [LDAPS](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

 [SSL/TLS](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

 [SNMP](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

 [IPsec](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

 [Kerberos](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

 Conclusions

4[.2](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.wv8lmqsplpdd) Application Security Solutions

 Endpoint Protection

 Endpoint Protection Platforms (EPP),

 Endpoint Detection and Response (EDR),

 Extended Detection and Response (XDR)

 Database Protection

 Data Discovery and Classification.

 Firewalls.

 Intrusion Detection & Prevention Systems (IDPS)

 Security Information and Event Management (SIEM)

 Data Loss Prevention (DLP)

 Data-Centric Audit and Protection (DCAP)

 Application Security

 Code Review

 Sandboxing

 Web Application Firewall (WAF)

 Runtime Application Self-Protection (RASP)

 Software Composition Analysis (SCA)

 Static Application Security Testing (SAST)

 Dynamic Application Security Testing (DAST)

 Interactive Application Security Testing (IAST)

 Conclusions

4[.3](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.g98km9urykdd) Secure Network Design

 VPN

 Network Segmentation

 Access Control

 Data loss prevent (DLP)

 Anomaly detection

 Endpoint security

 Intrusion prevention systems

 Conclusions

4[.4](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.7pii0khen2cd) Secure Cloud Controls and Solutions

 Cloud Security Controls

 Security Operations, and Threat Detection

 Solutions

 Cloud Access Security Broker

 Firewalls

 Conclusions

 The Geek’s Corner

Conclusions

 Quiz

 References

#

# **Introduction**

## **What you will learn**

In this unit, you will learn various security controls and solutions which are parameters implemented to protect various forms of data and infrastructure important to an organization ranging from the key design, architectural and implementation solutions\choices made by organizations in satisfying specified security requirements for systems or system components.

## **Why it is important and How it can help you in everyday life**

This module is essential for you and your organisation as the implementation of security solutions are important since they become an integral part of any data related operations for organizations and individuals of all sizes and industries. A robust information security program helps protecting your technology assets and physical space from malicious attacks outside and inside your organization. These are important security solutions to keep you and your employees and physical infrastructure safe from harm by defending your and your business's critical data and information from hackers and other cyber security threats. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. It also keeps you compliant with updated laws and regulations in your country or region.

## **What career you can pursue**

There are various career options that you can pursue under security field where some of the most important ones are;

-Security Engineer, who works to keep individuals and organizations’ security systems up and running, which involves implementing and testing new security features, planning computer and network upgrades, troubleshooting, responding to security incidents and many others.

-Application Security Engineer, who works to anticipate structural vulnerabilities and determine how to correct them. Their work includes updating software, creating firewalls, and running encryption programs within a computer network or application.

-Cloud Engineer/Architect, who works to upgrade cloud-based systems to improve operations and protect against data breaches and cybersecurity threats, troubleshooting any actual or potential problems with cloud computing platforms, providing necessary cloud support services that help individuals and companies use applications in new ways.

## **Pre-requisites**

In general, a security engineer or cloud architect must have the following qualifications:

* Degree in Computer Science, IT, Systems Engineering, or a similar field
* Two years of work experience in cyber security-related duties such as incident detection and response, and forensics
* Experience with the functionality, operation, and maintenance of f[irewalls](https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall) and various forms of endpoint security
* Proficiency in languages/tools such as C++, Java, Node, Python, Ruby, Go, or Power Shell
* The ability to work in a fast-paced environment, often under pressure
* Possess the right eye for detail and outstanding problem-solving skills
* Up to date knowledge of the latest [cybersecurity trends](https://www.simplilearn.com/top-cybersecurity-trends-article) and hacker tactics.

Note that different organizations may have more or fewer qualifications or attach lesser or

greater importance to any of the given criteria.

# **Material**

## **4**[**.1 Secure Protocols**](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

##

## [**HTTPS**](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

Hypertext transfer protocol secure (HTTPS) is the secure version of [HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/), which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provider.

Any website, especially those that require login credentials, should use HTTPS. In modern web browsers such as Chrome, websites that do not use HTTPS are marked differently than those that are. Look for a padlock in the URL bar to signify the webpage is secure. Web browsers take HTTPS seriously; [Google Chrome and other browsers flag all non-HTTPS websites as not secure.](https://www.cloudflare.com/learning/ssl/why-use-https/)[3]

**SSH**

[SSH](http://en.wikipedia.org/wiki/Secure_Shell) or Secure Shell is a network communication protocol that enables two computers to communicate (c.f [http](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) or hypertext transfer protocol, which is the protocol used to transfer hypertext such as web pages) and share data. An inherent feature of ssh is that the communication between the two computers is encrypted meaning that it is suitable for use on insecure networks.

SSH is often used to "login" and perform operations on remote computers but it may also be used for transferring data.

**How do I use SSH?**

You use a program on your computer (ssh client), to connect to our service (server) and transfer the data to/from our storage using either a graphical user interface or command line. There are many programs available that enable you to perform this transfer and some operating systems such as Mac OS X and Linux have this capability built in.

**LDAPS**

Lightweight directory access protocol (LDAP) is a protocol that makes it possible for applications to query user information rapidly.

Companies store usernames, passwords, email addresses, printer connections, and other static data within directories. LDAP is an open, vendor-neutral application protocol for accessing and maintaining that data. LDAP can also tackle authentication, so users can sign on just once and access many different files on the server.

[LDAP](https://www.okta.com/integrations/ldap/) is a protocol, so it doesn't specify how directory programs work. Instead, it's a form of language that allows users to find the information they need very quickly.

LDAP is vender-neutral, so it can be used with a variety of different directory programs. Typically, a directory [contains data that is](https://tldp.org/HOWTO/LDAP-HOWTO/whatisldap.html):

Descriptive. Multiple points, such as name and location, come together to define an asset.

Static. The information doesn’t change much, and when it does, the shifts are subtle.

Valuable. Data stored within the directory is critical to core business functions, and it's touched over and over again.[7]

Sometimes, people use LDAP in concert with other systems throughout the workday. For example, your employees may use LDAP to connect with printers or verify passwords. Those employees may then switch to Google for email, which doesn't rely on LDAP at all.

**SSL\TSL**

SSL, or Secure Sockets Layer, is an [encryption](https://www.cloudflare.com/learning/ssl/what-is-encryption/)-based Internet security [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/). It was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications. SSL is the predecessor to the modern [TLS](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/) encryption used today.

A website that implements SSL/TLS has "[HTTPS](https://www.cloudflare.com/learning/ssl/what-is-https/)" in its URL instead of "[HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/)."

Transport Layer Security, or TLS, is a widely adopted security [protocol](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and [voice over IP (VoIP)](https://www.cloudflare.com/learning/video/what-is-voip/) ([www.cloudflare.com](http://www.cloudflare.com), 16)

## **What is the difference between TLS and SSL?**

TLS evolved from a previous encryption protocol called Secure Sockets Layer ([SSL](https://www.cloudflare.com/learning/ssl/what-is-ssl/)), which

was developed by Netscape. TLS version 1.0 actually began development as SSL version

3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape. Because of this history, the terms TLS and SSL are sometimes used interchangeably.

**SNMP**

Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a [Local Area Network (LAN)](https://cyberhoot.com/cybrary/local-area-network-lan/) or [Wide Area Network (WAN)](https://cyberhoot.com/cybrary/wide-area-network-wan/). The purpose of SNMP is to provide network devices, such as routers, servers, and printers with a common language for sharing information within a Network Management System (NMS).[34]

SNMP’s client-server architecture has the three following components:

SNMP manager

SNMP agent

Management Information Base (MIB).

The SNMP manager acts as the client, the SNMP agent acts as the server and the MIB acts as the server’s database. When the SNMP manager asks the agent a question, the agent uses the MIB to supply the answer.

SNMP is so popular that most network devices come pre-bundled with SNMP agents. To make use of the protocol, however, network administrators must first change the default configuration settings of their network devices so SNMP agents can communicate with the network’s management system.

SNMP is part of the original [Internet Protocol (IP)](https://cyberhoot.com/cybrary/internet-protocol-security-ipsec/) suite as defined by the Internet Engineering Task Force (IETF). Multiple versions of the SNMP protocol exist. The most recent version, SNMPv3, includes security mechanisms for [authentication](https://cyberhoot.com/cybrary/authentication/), [encryption](https://cyberhoot.com/cybrary/encryption/), and [access control](https://cyberhoot.com/cybrary/network-access-control-nac/).

**IPsec**

**What is IPsec?**

IPsec is a group of protocols for securing connections between devices. IPsec helps keep data sent over public networks secure. It is often used to set up [VPNs](https://www.cloudflare.com/learning/access-management/what-is-a-vpn/), and it works by encrypting [IP](https://www.cloudflare.com/learning/network-layer/internet-protocol/) packets, along with authenticating the source where the packets come from.

Within the term "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure." The Internet Protocol is the main routing protocol used on the Internet; it designates where data will go using [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/). IPsec is secure because it adds encryption\* and authentication to this process.

\*Encryption is the process of concealing information by mathematically altering data so that it appears random. In simpler terms, encryption is the use of a "secret code" that only authorized parties can interpret.[32]

**Why is IPsec important?**

Security protocols like IPsec are necessary because networking methods are not encrypted by default.

When sending mail through a postal service, a person typically would not write their message on the outside of the envelope. Instead, they enclose their message inside the envelope so that no one who handles the mail between sender and recipient can read their message. However, networking protocol suites like TCP/IP are only concerned with connection and delivery, and messages sent are not concealed. Anyone in the middle can read them. IPsec, and other protocols that encrypt data, essentially put an envelope around data as it traverses networks, keeping it secure.

[**Kerberos**](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.2yz7x8bu8zb5)

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.

The main components of Kerberos are:

Authentication Server (AS): The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.

Database: The Authentication Server verifies the access rights of users in the database.

Ticket Granting Server (TGS): The Ticket Granting Server issues the ticket for the Server

**Conclusions**

Security controls and solutions are critical subjects which continuously develop to reach the highest security level, where organisations become more aware of its importance with the fast paced technological developments and related security concerns. Security solutions provided by the experts are subjected to be more important in this sense where efforts to produce satisfying security requirements for systems will continue playing critical roles to protect various forms of data and infrastructure.

**4**[**.2**](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.wv8lmqsplpdd) **Application Security Solutions**

**Endpoint Protection**

**Endpoint Protection Platforms (EPP)**

Endpoint protection provides essential security for many types of endpoints, from smart phones to printers. An endpoint protection platform (EPP) is an integrated suite of endpoint protection technologies—such as antivirus, data encryption, intrusion prevention, and data loss prevention—that detects and stops a variety of threats at the endpoint.

An endpoint protection platform provides a framework for data sharing between endpoint protection technologies. This provides a more effective approach than a collection of siloed security products that lack the ability to communicate.

The volume and sophistication of cyberattacks are on the rise, and information technology (IT) systems and data are under constant threat of attack. Cyberattacks have become increasingly layered, using multiple, coordinated techniques to slip into an organization's IT systems. Endpoints are frequently the door through which attackers gain initial access. [13]

**Endpoint Detection and Response (EDR)**

Endpoint detection and response (EDR), also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. The term was suggested by [Anton Chuvakin](https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/) at Gartner to describe emerging security systems that detect and investigate suspicious activities on hosts and endpoints, employing a high degree of automation to enable security teams to quickly identify and respond to threats. [4]

The primary functions of an EDR security system are to:

Monitor and collect activity data from endpoints that could indicate a threat

Analyze this data to identify threat patterns

Automatically respond to identified threats to remove or contain them, and notify security personnel

Forensics and analysis tools to research identified threats and search for suspicious activities

**Extended Detection and Response (XDR)**

According to analyst firm Gartner, Extended Detection and Response (XDR) is “a SaaS-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components.”

XDR enables an enterprise to go beyond typical detective controls by providing a holistic and yet simpler view of threats across the entire technology landscape. XDR delivers real-time actionable threat information to security operations for better, faster outcomes.[29]

Extended Detection and Response (XDR) primary advantages are:

Improved protection, detection, and response capabilities

Improved productivity of operational security personnel

Lower total cost of ownership for effective detection and response of security threats

Extended Detection and Response (XDR) holds the promise of consolidating multiple products into a cohesive, unified security incident detection and response platform. XDR is a logical evolution of endpoint detection and response (EDR) solutions into a primary incident response tool.

**Database Protection**

**Data Discovery and Classification.**

Data discovery and data classification are two separate processes, but they go hand-in-hand to give your organization complete visibility into the data across your entire environment. Before we get into how they work together, let’s look at a quick definition of each.

**Data discovery**

Data discovery is the process of scanning your entire environment to find and identify where both structured and unstructured data resides across your business. This means looking across your entire network, including file servers and hardware, to determine where sensitive and regulated data lives.​​

In essence, data discovery allows businesses to identify, classify and track sensitive data so that they have complete visibility into where their data lives. This helps companies to better protect their data, as well as ensure they are meeting regulatory compliance requirements.[2]

**Data classification**

Data classification is the process of identifying the types of data that a business has discovered, and then tagging that data to organize it into categories based on file type, content and other metadata.

The process of data classification makes it easier to locate and retrieve sensitive data, as well as eliminate multiple duplications of data. This helps reduce storage and backup costs, increases visibility into where data lives and allows businesses to classify data by the type of regulation it is governed by - making compliance goals easier to achieve.

Data discovery and classification go hand-in-hand. [19]

Data discovery and classification work together to give businesses complete visibility into what data they have, where it lives and what policies need to be put in place to protect the data and ensure it complies with data protection regulations. In short, data discovery and classification dramatically improves your data protection and enables your business to implement the controls required to achieve compliance.

**Firewalls.**

A firewall is a security device that protects your network from unauthorized access to private data. Firewalls also secure computers from malicious software, creating a barrier between secured internal networks and untrusted outside networks.

Firewalls deliver different protection levels depending on your client’s security needs. For over 25 years, firewalls have offered the first line of defense in network security systems. Read on to find out about the value of firewalls in cyber security.

**What is the role of firewalls in cybersecurity?**

Firewalls keep an eye on attempts by unwanted traffic to access your client’s operating system. They form barriers between computers and other networks.

Firewalls also serve as traffic controllers, managing and validating your client’s network access. Most operating systems and security software have a pre-installed firewall.

With firewalls, managed service providers (MSPs) can remove the guesswork from host-level protection. Firewalls with an integrated intrusion prevention system will block malware and application-layer attacks. In addition, they react quickly and seamlessly to detect attacks throughout your network.Network security firewalls are invaluable in web traffic management as they minimize the spread of web threats.

**How does a firewall work?**

Firewalls typically welcome incoming connections that are allowed to access a network. The security systems will allow or block data packets based on existing security rules. Firewalls build checkpoints that filter web traffic. These systems let you review and act upon rogue network traffic before the attacked network experiences any adverse effects.

With a dependable firewall in place, only trusted sources and IP addresses can access your client’s systems. Some firewalls can also monitor audit logs to find connections and traffic that have gotten through.

Use firewalls to gate the borders of private networks and the host devices. Ensure that you include robust firewalls when setting up user access controls. You can set up these barriers on user computers or dedicated computers on the network.

**Intrusion Detection & Prevention Systems (IDPS)**

An intrusion detection and prevention system (IDPS) monitors a network for possible threats

to alert the administrator, thereby preventing potential attacks.



[www.spicework.com](http://www.spicework.com)

An intrusion detection and prevention system is like the baggage and security check at airports. A ticket or a boarding pass is required to enter an airport, and once inside, passengers are not allowed to board their flights until the necessary security checks have been made. Similarly, an intrusion detection system (IDS) only monitors and alerts bad traffic or policy violations. It is the predecessor of the intrusion prevention system (IPS), also

known as an intrusion detection and prevention system. Besides monitoring and alerting, the IPS also works to prevent possible incidents with automated courses of action. [17]

**Basic functions of an IDPS**

An intrusion detection and prevention system offers the following features:



**Basic Functions of an IDPS**

**Security Information and Event Management (SIEM)**

SIEM is a security solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses artificial intelligence to automate many of the manual processes associated with threat detection and incident response and has become a staple in modern-day security operation centers (SOCs) for security and compliance management use cases.[24]

Over the years, SIEM has matured to become more than the log management tools that preceded it. Today, SIEM offers advanced user and entity behavior analytics (UEBA) thanks to the power of AI and machine learning. It is a highly efficient data orchestration system for managing ever-evolving threats as well as regulatory compliance and reporting.

**How does SIEM work?**

At the most basic level, all SIEM solutions perform some level of data aggregation, consolidation and sorting functions in order to identify threats and adhere to data compliance requirements. While some solutions vary in capability, most offer the same core set of functionality: [41]

**Log Management**

SIEM captures event data from a wide range of source across an organization’s entire network. Logs and flow data from users, applications, assets, cloud environments, and networks is collected, stored and analyzed in real-time, giving IT and security teams the ability to automatically manage their network's event log and network flow data in one centralized location.

Some SIEM solutions also integrate with third-party threat intelligence feeds in order to correlate their internal security data against previously recognized threat signatures and profiles. Integration with real-time threat feeds enable teams to block or detect new types of attack signatures.[11]

**Event Correlation and Analytics**

Event correlation is an essential part of any SIEM solution. Utilizing advanced analytics to identify and understand intricate data patterns, event correlation provides insights to quickly locate and mitigate potential threats to business security. SIEM solutions significantly improve mean time to detect (MTTD) and mean time to resond (MTTR) for IT security teams by offloading the manual workflows associated with the in-depth analysis of security events.[11, 18]

**Incident Monitoring and Security Alerts**

Because they enable centralized management of on-premise and cloud-based infrastructure, SIEM solutions are able to identify all entities of the IT environment. This allows SIEM technology to monitor for security incidents across all connected users, devices, and applications while classifying abnormal behavior as it is detected in the network. Using customizable, predefined correlation rules, administrators can be alerted immediately and take appropriate actions to mitigate it before it materializes into more significant security issues.[11, 19]

**Compliance Management and Reporting**

SIEM solutions are a popular choice for organizations subject to different forms of regulatory compliance. Due to the automated data collection and analysis that it provides, SIEM is a valuable tool for gathering and verifying compliance data across the entire business infrastructure. SIEM solutions can generate real-time compliance reports for PCI-DSS, GDPR, HIPPA, SOX, and other compliance standards, reducing the burden of security management and detecting potential violations early so they can be addressed. Many of the SIEM solutions come with pre-built, out-of-the-box add-ons that can generate automated reports designed to meet compliance requirements.[5]

**Data Loss Prevention (DLP)**

Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.

**What is data loss prevention (DLP) Software?**

DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance requirements such as HIPAA, PCI-DSS, or GDPR.

Once those violations are identified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could create organizational risks.

Data loss prevention software and tools monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use. DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response.

**Do I Need Data Loss Prevention? 3 Main Uses Cases for DLP**

Data loss prevention solves three main objectives that are common pain points for many organizations: personal information protection / compliance, intellectual property (IP) protection, and data visibility.

**Personal Information Protection / Compliance:** Does your organization collect and store Personally Identifiable Information (PII), Protected Health Information (PHI), or payment card information (PCI)? If so, you are more than likely subject to compliance regulations, such as HIPAA (for PHI) and GDPR (for personal data of EU residents), that require you to protect your customers’ sensitive data. DLP can identify, classify, and tag sensitive data and monitor activities and events surrounding that data. In addition, reporting capabilities provide the details needed for compliance audits. [8, 36]

**IP Protection:** Does your organization have important intellectual property and trade or state secrets that could put your organization’s financial health and brand image at risk if lost or stolen? DLP solutions like Digital Guardian that use context-based classification can classify intellectual property in both structured and unstructured forms. With policies and controls in place, you can protect against unwanted exfiltration of this data.[8]

**Data Visibility:** Is your organization seeking to gain additional visibility into data movement? A comprehensive enterprise DLP solution can help you see and track your data on endpoints, networks, and the cloud. This will provide you with visibility into how individual users within your organization interact with data.

**Data-Centric Audit and Protection (DCAP)**

Data-centric audit and protection (DCAP) is a term used by Gartner, a business research and consulting company, to describe a type of data-centric security. The goal of DCAP is to protect an organization’s data privacy and apply it to specific pieces of data, not the entire organization.

DCAP focuses on:

● Classifying data

● Storing sensitive data

● Data security governance

● Protecting data against unauthorized access

● Data monitoring and auditing

**How Data-Centric Audit and Protection Works**

Data-centric audit and protection is about protecting the data, not about preventing unauthorized users from hacking into systems. This layer of protection relies on several steps to secure data:

**Classifying data**

In order to protect sensitive data, business organizations need to know where the information is located and how much can be accessed. The first step is to classify data as it is created. There is content discovery technology that will classify data found in the organization’s assets. The sensitive data needs to be classified so it can be protected. For example, access rights to the data are assigned based upon common schema and policies.

**Storing sensitive data**

Digital rights management tools help protect sensitive data with access controls and encryption.

Identity and access management (IAM) keeps sensitive data available to only authorized users.

Persistent encryption will remain with data in storage and as it is being shared is the most secure method. Just as important as encrypting data in storage and in transmission is making sure authorized users have the proper encryption keys. This should go hand-in- hand with access controls.[45]

**Data security governance**

Data governance policies will define what is sensitive data, who has authorized access to it, and how they can handle it. Data governance needs to protect data and allow users to work with it.

**Data monitoring and auditing**

Data-centric audit and protection is to keep data secure while it is being used. To ensure that security, monitoring technology can be used to help protect it. This entails using activity monitoring, access management, logical control and application security technologies.

**Protecting data against unauthorized access**

Data security is a primary goal of DCAP. It is possible to create such secure processes that it hinders the ability to actually utilize business data. Data-centric security needs to be balanced with productivity. Otherwise, organizations risk losing the benefits of leveraging big data, or users will bring the data outside of the secure environment — putting the data at risk.

Business data is more valuable when it is shared — inside and outside of the business organization. This also means the data can end up outside of an organization’s control.

Encryption can also help protect sensitive data from unauthorized access outside of

organizational control.

**Benefits of of Data-Centric Audit and Protection**

Data-centric audit and protection is designed to protect business data without getting in the way of harnessing the analytical use of it. Good data-centric security can help:

● Allow businesses to safely use IT services and vendors.

● Mitigate the risk of data breaches.

● Comply with regulatory mandates.

● Manage data, where it’s stored, when it’s shared and how it’s protected.

● Assess risks to data and prioritize investment in data protection.[41]

**Best Practices of Data-Centric Audit and Protection**

Data-centric security is a holistic strategy. It doesn’t discriminate against device, storage technology or platform. Ensure complete data-centric audit and protection with best practices such as:

**Secure infrastructure**

Data-centric audit and protection focuses on securing data but systems still need to be protected from unauthorized access.

**Reporting and auditing**

Track your data so you know who is using the data and how. This is especially important to

demonstrate legal and regulatory compliance.

**Encryption key management**

Support authorized users so they can access data with proper encryption keys and protect against access by malicious users.

**Data discovery**

Authorized users may be keeping data in unsecured files. Use data discovery tools to find structured and unstructured data stored in local files.

**Search and destroy**

Business data isn’t meant to live forever. Make sure temporary files cannot be recovered when it is not needed any more using:

● Crypto-shredding

● Secure deletion

● Physical destruction of devices and disk storage

Content discovery technology can help discover data hiding where it should be. Business organizations need to find it before unauthorized users do.

Data-centric audit and protection is vital for modern enterprises that leverage big data to support business processes. By finding the right balance between adequately protecting your organization’s data and supporting the use of data within the organization, you’ll create a more robust security posture without hindering productivity or sacrificing the benefits of big data.[33, 41]

**Application Security**

**Code Review**

Secure code review is a manual or automated process that examines an application’s source code. The goal of this examination is to identify any existing security flaws or vulnerabilities. Code review specifically looks for logic errors, examines spec implementation, and checks style guidelines, among other activities.

Automated code review is a process in which a tool automatically reviews the source code of an application, using a predefined set of rules to look for inferior code. Automated review can find issues in source code faster than identifying them manually.

Manual code review involves a human looking at source code, line by line, to find vulnerabilities. Manual code review helps to clarify the context of coding decisions. [12, 22]

Automated tools are faster but they cannot take the developer’s intentions and general business logic into consideration. Manual review is more strategic and looks at specific issues.

**How does the code review process work?**

Code review—manual, automated, or a mixture of the two—can be initiated via an automated notification or by a human. Current best practices for performing robust and secure code review involve using manual and automated reviews together. This tandem approach catches the most potential issues.

Secure code review can occur at any time during the software development life cycle (SDLC), but it’s most impactful when performed earlier, because that’s when it’s easiest and fastest to make fixes to the code. In particular, using automated code review when developers are actually writing code allows for immediate changes as needed. Manual code review is very helpful when performed during the commit phase, or when a merge request is submitted to the repository. It also is a way to review code while taking into account business logic and developer intentions.

Automated review enables large codebases to be quickly and efficiently analyzed. Developers perform this review using either open source or commercial tools while they are coding, to help find vulnerabilities in real time. The most advanced development teams also include SAST tools, which can provide additional inputs, help find vulnerabilities, and enable developers to fix them before the code is checked in. The most successful development processes also involve developers performing their own self-reviews as they code.

Manual review involves a thorough review of the entire codebase by a senior or more experienced developer. This process can be extremely tedious and time-consuming, but it identifies flaws, such as business logic problems, that automated tools may miss. Layering in QA tests can help as well, but there are still scenarios that manual testing can miss. The best practice is a combination of automated and manual review.[16, 27, 39]

**Why is secure code review important?**

Secure code review is a critical process employed by the most successful development teams. It can:

Reduce the number of delivery defects found at a later stage in the SDLC

Decrease the amount of time developers spend fixing late-stage defects, thereby increasing productivity

Reduce the number of bugs and security vulnerabilities going into production

Improve consistency across codebases and increase maintainability

Improve collaboration, knowledge sharing, and developer productivity, and lessons learned can help inform future code development

Improve ROI by helping make processes faster and more secure, and use less resources and time

**Code Signing**

Code signing is a cryptographic method used by developers to prove that a piece of software is authentic. By digitally signing apps, software, or embedded firmware with a private key, the proof is provided to end-users that the code originates from a trusted and legitimate source and that it hasn’t been tampered with since it was published.[33]

**Why Code Signing Security Matters**

Code signing without securing your private keys can expose you to more risk than no code signing at all. Attackers seek to compromise these keys to sign and distribute malicious code to your customers – masked as legitimate software or firmware.

**Key Theft**

If the private keys linked to your code signing certificates are compromised, it’s game over. Stolen code signing keys are the top prizes for hackers – either sold or used to create signed malware that appears be to published by your developers.

**Signing Breach**

Hackers don’t need your keys to sign malware. If build servers or developer workstations with unhindered access to code signing systems are breached, an attacker can simply submit malware to be signed and distributed without detection.[33]

**Internal Misuse**

Developers specialize in code, not security. Code signing keys and certificates can easily be misused or misplaced by developers, making it much easier for would-be attackers to undermine the integrity of your code signing operations.

**Sandboxing**

Sandboxing is a security practice in which you use an isolated environment, or a “sandbox,” for testing. Within the sandbox you run code, analyze the code in a safe, isolated environment without affecting the application, system or platform.

Sandboxing is very effective when mounting a defense against zero-day threats, which are threats that have not been seen before or match any known malware on file. Even though regular email filters can scan emails to detect malicious senders, file types, and URLs, zero-day threats pop up all the time, and they can be missed by traditional filtration.

Sandboxing provides a greater level of protection, particularly when a malicious email slips by the filters put in place by your provider.

When sandboxing is used for testing, it creates a safe place to install and execute a program, particularly a suspicious one, without exposing the rest of your system. If the application contains malicious code, it can run within the sandbox without impacting any other components of your network. [35]

**Benefits of Sandboxing**

Sandboxing comes with several benefits that can enhance the safety of your network, as well as offer new options for accomplishing your company's objectives—IT and otherwise.

Create and deploy environments: If you use sandboxes, it is easy to create and deploy environments at scale. A sandbox gives you the flexibility to test different versions and new lines of code.

Gain access to advanced networking and support: With the right kind of sandbox architecture, you can use advanced networking features and test them out to see how they may fit in with, or improve, your current system.[19]

Enhance collaboration: With a sandbox environment, you can deploy an application and grant access to people from a variety of departments. They can then use the sandbox and "play” with the application. They can leave feedback for the IT team, management, or stakeholders in other departments. If teams are allowed to use an application and take notes on their experiences for an extended time, their findings can be used to better inform the next iteration.

Save your company money: Instead of sourcing, purchasing, staffing, and maintaining your own in-house development labs, you can use cloud-based sandboxing instead. The money you would have spent on procuring, running, and maintaining the equipment can be invested in other projects to support company objectives.

Prepare for future attacks: When a threat is contained within the sandbox environment, it is quarantined and available for study by the in-house IT team or external cybersecurity experts. A careful study of the threat may reveal patterns that can be used to identify and stop future attacks. You can also use the knowledge gained from dissecting the threat to identify vulnerabilities in the network.[43]

**Web Application Firewall (WAF)**

A web application firewall (WAF) protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others. Attacks to apps are the leading cause of breaches—they are the gateway to your valuable data. With the right WAF in place, you can block the array of attacks that aim to exfiltrate that data by compromising your systems.[21]

**How does a web application firewall (WAF) work?**

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe. Just as a proxy server acts as an intermediary to protect the identity of a client, a WAF operates in similar fashion but in the reverse—called a reverse proxy—acting as an intermediary that protects the web app server from a potentially malicious client.

WAFs can come in the form of software, an appliance, or delivered as-a-service. Policies can be customized to meet the unique needs of your web application or set of web applications. Although many WAFs require you update the policies regularly to address new vulnerabilities, advances in machine learning enable some WAFs to update automatically.

This automation is becoming more critical as the threat landscape continues to grow in complexity and ambiguity. [43, 45]

**Runtime Application Self-Protection (RASP)**

Runtime Application Self Protection (RASP) is a security solution designed to provide personalized protection to applications. It takes advantage of insight into an application’s internal data and state to enable it to identify threats at runtime that may have otherwise been overlooked by other security solutions.

**How RASP Works**

RASP wraps around and protects a particular application, rather than a general network-level or endpoint-level defensive solution. This more targeted deployment location enables RASP to monitor the inputs, outputs, and internal state of the application that it is protecting. By deploying RASP, developers can identify vulnerabilities within their applications. Additionally, the RASP solution can block attempts to exploit existing vulnerabilities in deployed applications.

RASP’s focused monitoring makes it capable of detecting a wide range of threats, including zero-day attacks. Since RASP has insight into the internals of an application, it can detect behavioral changes that may have been caused by a novel attack. This enables it to respond to even zero-day attacks based upon how they affect the target application.[18, 45]

**Benefits of Runtime Application Self-Protection (RASP)**

RASP differs from other cybersecurity solutions in its level of focus on a single application. This focus enables it to provide a number of security benefits:

Contextual Awareness: When a RASP solution identifies a potential threat, it has additional contextual information about the current state of the application and what data and code is affected. This context can be invaluable for investigating, triaging, and remediating potential vulnerabilities since it indicates where the vulnerability is located in the code and exactly how it can be exploited.

Visibility into Application-Layer Attacks: RASP has deep visibility into the application layer because it is integrated with a particular application. This application-layer visibility, insight, and knowledge can help to detect a wider range of potential attacks and vulnerabilities.

Zero-Day Protection: While RASP can use signatures to identify attacks, it is not limited to signature-based detection. By identifying and responding to anomalous behaviors within the protected application, RASP can detect and block even zero-day attacks. [1, 8]

Lower False Positives: RASP has deep insight into an application’s internals, including the ability to see how a potential attack affects the application’s execution. This dramatically increases RASP’s ability to differentiate true attacks (which have a true negative impact on application performance and security) from false positives (such as SQL injection attempts that are never included in an SQL query). This reduction in false positives decreases load on security teams and enables them to focus on true threats.

Lower CapEx and OpEx: RASP is designed to be easy to deploy yet is able to make a significant difference in an application’s vulnerability to attack and rate of false positive alerts. This combination reduces both up-front expenses (CapEx) and the cost of effectively protecting the application (OpEx) compared to manual patching and web application firewalls (WAFs).[14]

Easy Maintenance: RASP works based upon insight into an application, not traffic rules, learning, or blacklists. SOC teams love this reliability and CISOs appreciate the resource savings. Applications become self-protected and remain protected wherever they go.

Flexible Deployment: While RASP is typically based upon HTML standards, it is easy to adapt its API to work with different standards and application architectures. This enables it to protect even non-web applications using standards like XML and RPC.

Cloud Support: RASP is designed to integrate with and be deployed as part of the application that it protects. This enables it to be deployed in any location where the protected applications can run, including in the cloud.

DevSecOps Support: RASP solutions are designed to be integrated into a DevOps continuous integration and deployment (CI/CD) pipeline. This makes RASP easy to deploy and supports DevSecOps operations.[22]

**Software Composition Analysis (SCA)**

Software composition analysis (SCA) provides a deep analysis of open source packages in use by an application. SCA highlights vulnerabilities and licenses in dependencies for risk and compliance assessments, and it can generate a software bill of materials (SBOM) of all resources to share with internal stakeholders and external customers.

Software composition analysis (SCA) provides a deep analysis of open source packages in use by an application. SCA highlights vulnerabilities and licenses in dependencies for risk and compliance assessments, and it can generate a software bill of materials (SBOM) of all resources to share with internal stakeholders and external customers.

Software Composition Analysis Identifies Risks in Open Source Packages

SCA tools identify all open source packages in an application and all the known vulnerabilities of those packages. This knowledge can be used to notify developers of the issues in their code to fix them before they are exploited. A good software composition analysis process will look beyond package managers into infrastructure as code (IaC) and Kubernetes manifests, pulling images to identify vulnerabilities in those images.

SCA tools with connections to IaC templates and limitless dependency scanning ensure vulnerabilities don’t go undetected or unresolved.

Software composition analysis tools can also be used to generate a software bill of materials (SBOM or software BOM) that includes all the open source components used by an application. The SBOM lists details about the package version as well as known vulnerabilities and licenses for each component in use. For example, for Python, the BOM will include all the packages in import statements, such as httplib2, along with the version number, discovered vulnerabilities and licenses for each package.[30]

SCA programs should enable collaboration among stakeholders such as engineering, DevOps, security and compliance teams. Many organizations will use these programs to create alerts and/or block code from merging into repositories if said code includes open source components that violate the organization’s compliance mandates for controlling exposure. Determining an acceptable severity level for vulnerabilities and license types should involve the relevant stakeholders.

**Static Application Security Testing (SAST)**

Static application security testing (SAST), or static analysis, is a testing methodology that analyzes source code to find security vulnerabilities that make your organization’s applications susceptible to attack. SAST scans an application before the code is compiled. It’s also known as white box testing.

**What problems does SAST solve?**

SAST takes place very early in the software development life cycle (SDLC) as it does not require a working application and can take place without code being executed. It helps developers identify vulnerabilities in the initial stages of development and quickly resolve issues without breaking builds or passing on vulnerabilities to the final release of the application.

SAST tools give developers real-time feedback as they code, helping them fix issues before they pass the code to the next phase of the SDLC. This prevents security-related issues from being considered an afterthought. SAST tools also provide graphical representations of the issues found, from source to sink. These help you navigate the code easier. Some tools point out the exact location of vulnerabilities and highlight the risky code. Tools can also provide in-depth guidance on how to fix issues and the best place in the code to fix them, without requiring deep security domain expertise.

**Why is SAST an important security activity?**

Developers dramatically outnumber security staff. It can be challenging for an organization to find the resources to perform code reviews on even a fraction of its applications. A key strength of SAST tools is the ability to analyze 100% of the codebase. Additionally, they are much faster than manual secure code reviews performed by humans. These tools can scan millions of lines of code in a matter of minutes. SAST tools automatically identify critical vulnerabilities—such as buffer overflows, SQL injection, cross-site scripting, and others—with high confidence. Thus, integrating static analysis into the SDLC can yield dramatic results in the overall quality of the code developed.

**Dynamic Application Security Testing (DAST)**

Dynamic application security testing (DAST) is a method of AppSec testing in which testers examine an application while it’s running, but have no knowledge of the application’s internal interactions or designs at the system level, and no access or visibility into the source program. This “black box” testing looks at an application from the outside in, examines its running state, and observes its responses to simulated attacks made by a testing tool. An application’s responses to these simulations help determine whether the application is vulnerable and could be susceptible to a real malicious attack.

**How does DAST work?**

DAST works by simulating automated attacks on an application, mimicking a malicious attacker. The goal is to find outcomes or results that were not expected and could therefore be used by attackers to compromise an application. Since DAST tools don’t have internal information about the application or the source code, they attack just as an external hacker would—with the same limited knowledge and information about the application.

**What problems does DAST solve?**

Applications run the world economy and organizations are under tremendous pressure to stay ahead of the curve as our digital world accelerates. Businesses must continually innovate in an environment where sophisticated, relentless threat actors are ready to exploit any opportunity to disrupt, threaten critical data, and do damage. To successfully navigate this new world, it is vital to develop and execute a plan to ensure their applications are secure.

DAST works by simulating automated attacks on an application, mimicking a malicious attacker. The goal is to find outcomes or results that were not expected and could therefore be used by attackers to compromise an application. Since DAST tools don’t have internal information about the application or the source code, they attack just as an external threat actor would—with the same limited knowledge and information about the application. [31]

**Why is DAST vital to application security?**

As more businesses rely on web and mobile applications for success, application security vulnerabilities have rapidly become the most prevalent cause of data breaches. Thus, it is more important than ever for organizations to protect their applications and code.

**Challenges that organizations are currently facing**

The shift to the cloud and cloud-native application technologies is making applications more complex.

Massively distributed microservices and serverless functions mean that developers are focused solely on their own services, and no one has a complete grasp of the entire codebase.

As the sheer number of applications increases, the overall lines of software code deployed to the cloud expands the potential attack surface.

With more organizations focused on digital transformation, knowledge of the legacy code is waning as developers retire or change roles.

The prevalence of third-party and open source software make applications more composite in nature. As a result, a significant amount of the application code is developed outside the purview of the organization.[36]

DevOps methodologies help development teams move faster but leave little time for manual or outdated security checks.

The velocity of code change is increasing, the underlying architecture where applications are hosted is changing, and the number of attacks against applications is growing. These three shifts capture the need for lightweight but comprehensive and highly usable application security solutions that serve the needs of both information security and application development teams working in concert. This is achieved by application security tools running efficiently, in the context of projects being worked on, reporting vulnerabilities and an application’s security state accurately. They must also support developer education by providing expert consultation for particularly difficult problems, and a solution that can be easily integrated into SDLCs.

Implementing DAST is not only necessary to determine the security posture of applications running in production and how they will likely interact with end users—it has now become essential for teams to keep up with the changing nature of applications and the knowledge of adversaries. Effective DevSecOps starts with taking feedback produced from DAST and integrating it into SecOps and DevOps tools. After all, DAST finds the actual vulnerabilities that put an organization and its end users at risk. [37]

Protect your applications and your code

Identify inherited and new vulnerabilities

Provide quality vulnerability assessment reports to expedite the remediation process

**Interactive Application Security Testing (IAST)**

IAST (interactive application security testing) analyzes code for security vulnerabilities while the app is run by an automated test, human tester, or any activity “interacting” with the application functionality. This technology reports vulnerabilities in real-time, which means it does not add any extra time to your CI/CD pipeline.

IAST works inside the application, which makes it different from both static analysis (SAST) and dynamic analysis (DAST). This type of testing also doesn’t test the entire application or codebase, but only whatever is exercised by the functional test.

IAST works best when deployed in a QA environment with automated functional tests running.

**IAST advantages**

Speed of results: IAST reports findings in real-time for the scope of the app being “exercised.”

API testing: Many functional API tests are automated, making IAST a good fit for teams building in microservices, etc.

Promotes re-use of existing test cases: IAST avoids the need to re-create scripts for security testing.

IAST is best used in conjunction with other testing technologies. Most organizations need both security assurance and developer-centric solutions. Security assurance solutions, including static analysis, dynamic analysis, and software composition analysis, provide security teams, executives, and application owners comprehensive assessments that support risk-based decision-making. Developer-centric solutions, like Veracode Static Analysis IDE Scan, software composition analysis, and IAST, help developers fix and find security-related flaws early and often, helping them learn to code more securely and lessen the number of defects later in the development lifecycle.[39]

**Conclusions**

Application security became very critical since applications run the world economy and organisations, which are under tremendous pressure to stay ahead of the curve as our digital world accelerates. Organisations\Businesses must continually innovate in an environment where sophisticated, relentless threat actors are ready to exploit any opportunity to disrupt, threaten critical data, and do damage. To successfully navigate this new world, it is vital to develop and execute a plan to ensure that their applications are secure. Therefore, application of security solutions are quite critical components of secure world, which’s importance will continue as accelerated each year.

**4.3 Secure Network Design**

**VPN**

While many network protocols have encryption built in, this is not true for all Internet traffic. This means that an attacker could potentially eavesdrop upon and modify data as it flows over the network. A virtual private network (VPN) is designed to fix this problem. It provides a secure, private connection between two points communicating over a public network.

**How does a VPN work?**

A VPN provides a secure, encrypted connection between two points. Before setting up the VPN connection, the two endpoints of the connection create a shared encryption key. This can be accomplished by providing a user with a password or using a key sharing algorithm.

Once the key has been shared, it can be used to encrypt all traffic flowing over the VPN link. For example, a client machine will encrypt data and send it to the other VPN endpoint. At this location, the data will be decrypted and forwarded on to its destination. When the destination server sends a response, the entire process will be completed in reverse.[11]

**Types of VPNs**

VPNs are designed to provide a private, encrypted connection between two points – but does not specify what these points should be. This makes it possible to use VPNs in a few different contexts:

Site-to-Site VPN: A site-to-site VPN is designed to securely connect two geographically-distributed sites. VPN functionality is included in most security gateways today. For instance a next-generation firewall (NGFW) deployed at the perimeter of a network protects the corporate network and also serves as a VPN gateway. All traffic flowing from one site to the other passes through this gateway, which encrypts the traffic sent to the gateway at the other site. This gateway decrypts the data and forwards it on to its destination.[11, 19]

Remote Access VPN: A remote access VPN is designed to link remote users securely to a corporate network. For instance when the COVID-19 pandemic emerged in 2020, many organizations transitioned to a remote workforce, and set up secure remote access VPNs from the remote clients to connect to critical business operations at the corporate site.

VPN as a Service: VPN as a Service or a cloud VPN is a VPN hosted in cloud-based infrastructure where packets from the client enter the Internet from that cloud infrastructure instead of the client’s local address. Consumer VPNs commonly use this model, enabling users to protect themselves while connecting to the Internet via insecure public Wi-Fi and provide some anonymity while accessing the Internet.

**Benefits of a VPN**

VPNs can provide users and companies with a number of benefits, such as:

Secure Connectivity: A VPN’s encrypted connection makes it impossible for a third party to eavesdrop on the connection without knowledge of the secret keys used for encryption and securing the data while in transit.

Simplified Distributed Networks: Any computers accessible from the public Internet need to have public IP addresses – either directly or via Network Address Translation (NAT). A site-to-site VPN simulates a direct connection between the two networks, enabling them to use private IP addresses for internal traffic.

Access Control: Every organization has systems and resources that are designed to only be accessible to internal users. A VPN provides a remote user or site with “internal” access – since the VPN endpoint is inside the network firewall – making it possible to allow access to these resources to authorized remote users without making these resources publicly accessible.

**Is a VPN Secure?**

A VPN uses cryptography to provide its security and privacy guarantees. In this way, VPNs can meet the three criteria of information security:

Confidentiality: Data privacy is ensured by encrypting all data flowing over the public network.

Message Integrity: Message authentication codes (MACs) ensure that any modifications or errors in transmitted data are detectable. In short, this detects when a message is tampered with or interfered with in some way, either intentionally or unintentionally.

Authentication: The initial authentication and key sharing process proves the identity of both endpoints of the VPN connection, preventing unauthorized use of the VPN.

By providing all of the features of the “CIA triad”, VPNs ensure a secure and private connection for their users.[11]

**Limitations and Security Risks of VPNs**

While VPNs are designed to fill a vital role for the modern business, they are not a perfect solution. VPNs have several limitations that impact their usability and corporate cybersecurity, including:

Fragmented Visibility: VPNs are designed to provide secure point to point connectivity with every VPN user on their own link. This makes it difficult for an organization’s security team to maintain the full network visibility required for effective threat detection and response.

No Integrated Security: An organization must deploy additional security solutions behind the VPN to identify and block malicious content and to implement additional access controls.

Inefficient Routing: VPNs can be used in a “hub and spoke” model to ensure that all traffic flows through the organization’s centralized security stack for inspection. As remote work and cloud applications become more common, this detour may not be the optimal path between the client and the cloud application or the Internet. Learn more about the SD-WAN vs VPN debate.

Poor Scalability: As a point-to-point security solution, VPNs scale poorly. For example, the number of site-to-site VPN connections in a fully-connected network grows exponentially with the number of sites. This creates a complex network infrastructure that is difficult to deploy, monitor and secure.

Endpoint Vulnerabilities: Endpoints who have legitimate access to the VPN can sometimes be compromised via phishing and other cyber attacks. Since the endpoint has full access to the VPN resources, so does the threat actor who has compromised the endpoint.

Many organizations require secure remote access solutions, and these VPN limitations make the search for VPN alternatives a priority. To learn about how to deploy secure remote access in your network, contact us. And don’t hesitate to request a free trial of Check Point’s remote workforce security solutions to learn how they can help to improve the productivity and security of your organization’s teleworkers.[29]

**Network Segmentation**

Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. This allows network administrators to control the flow of network traffic between subnets based on granular policies. Organizations use segmentation to improve monitoring, boost performance, localize technical issues and – most importantly – enhance security.

With network segmentation, network security personnel have a powerful tool with which to prevent unauthorized users and protect static IP addresses, whether curious insiders or malicious attackers, from gaining access to valuable assets, such as customers’ personal information, corporate financial records and highly confidential intellectual property, the so-called “crown jewels” of the enterprise. As a result of the rise of software-defined networking (SDN), these assets are frequently found spread across hybrid and multicloud environments – public clouds, private clouds and software-defined networks (SDNs) – all of which need to be secured against attacks and data breaches. To understand the security usage of network segmentation, it’s first necessary to consider the concept of trust in network security.[20]

**Use Cases**

Organizations can use network segmentation for a variety of applications, including:

Guest wireless network: Using network segmentation, a company can offer Wi-Fi service to visitors and contractors at relatively little risk. When someone logs in with guest credentials, they enter a microsegment that provides access to the internet and nothing else.

User group access: To guard against insider breaches, many enterprises segment individual internal departments into separate subnets consisting of the authorized group members and the DAAS they need to do their jobs. Access between subnets is rigorously controlled. For example, someone in engineering attempting to access the human resources subnet would trigger an alert and an investigation.

Public cloud security: Cloud service providers are typically responsible for security in the cloud infrastructure, but the customer is responsible for the security of the operating systems, platforms, access control, data, intellectual property, source code and customer-facing content that typically sit atop the infrastructure. Segmentation is an effective method for isolating applications in public and hybrid cloud environments.

PCI DSS compliance: Network administrators can use segmentation to isolate all credit card information into a security zone – essentially a protect surface – and create rules to allow only the absolute minimum, legitimate traffic in the zone while automatically denying everything else. These isolated zones are frequently virtualized SDNs in which PCI DSS compliance and segmentation can be achieved via virtual firewalls.[32]

**Access Control**

Access control is a fundamental component of data security that dictates who’s allowed to access and use company information and resources. Through authentication and authorization, access control policies make sure users are who they say they are and that they have appropriate access to company data. Access control can also be applied to limit physical access to campuses, buildings, rooms, and datacenters.

**How does access control work?**

Access control identifies users by verifying various login credentials, which can include usernames and passwords, PINs, biometric scans, and security tokens. Many access control systems also include multifactor authentication (MFA), a method that requires multiple authentication methods to verify a user’s identity.

Once a user is authenticated, access control then authorizes the appropriate level of access and allowed actions associated with that user’s credentials and IP address.

There are four main types of access control. Organizations typically choose the method that makes the most sense based on their unique security and compliance requirements. The four access control models are:

Discretionary access control (DAC): In this method, the owner or administrator of the protected system, data, or resource sets the policies for who is allowed access.

Mandatory access control (MAC): In this nondiscretionary model, people are granted access based on an information clearance. A central authority regulates access rights based on different security levels. This model is common in government and military environments.

Role-based access control (RBAC): RBAC grants access based on defined business functions rather than the individual user’s identity. The goal is to provide users with access only to data that’s been deemed necessary for their roles within the organization. This widely used method is based on a complex combination of role assignments, authorizations, and permissions.

Attribute-based access control (ABAC): In this dynamic method, access is based on a set of attributes and environmental conditions, such as time of day and location, assigned to both users and resources. [37]

**Data loss prevent (DLP)**

Data loss prevention (DLP) is a part of a company’s overall security strategy that focuses on detecting and preventing the loss, leakage or misuse of data through breaches, ex-filtration transmissions and unauthorized use.

A comprehensive DLP solution provides the information security team with complete visibility into all data on the network, including:

Data in use: Securing data being used by an application or endpoint through user authentication and access control

Data in motion: Ensuring the safe transmission of sensitive, confidential or proprietary data while it moves across the network through encryption and/or other e-mail and messaging security measures

Data at rest: Protecting data that is being stored on any network location, including the cloud, through access restrictions and user authentication

DLP is also a way for companies to classify business critical information and ensure the company’s data policies comply with relevant regulations, such as HIPAA, GDPR and PCI-DSS. A properly designed and configured DLP solution streamlines reporting to meet these compliance and auditing requirements.

Finally, some DLP solutions can also provide alerts, enable encryption and isolate data when a breach or other security incident is detected. In doing so, the DLP solution can expedite incident response by identifying areas of weakness and anomalous activity during routine networking monitoring.

**3 Types: Network vs. Endpoint vs. Cloud**

**There are three types of DLP:**

Network DLP: monitors and protects all data in use, in motion or at rest on the company’s network, including the cloud

Endpoint DLP: monitors all endpoints, including servers, computers, laptops, mobile phones and any other device on which data is used, moved or saved

Cloud DLP: a subset of Network DLP that is specifically designed to protect those organizations that leverage cloud repositories for data storage

Network DLP

Tracks and analyzes the organization’s network activity and traffic, across a traditional network and the cloud; this includes monitoring e-mail, messaging and file transfers, to detect when business critical data is being sent in violation of the organization’s information security policies

Establishes a database that records when sensitive or confidential data is accessed, who accesses it, and, if applicable, where the data moves on the network

Provides the infosec team with complete visibility into all data on the network, including data that is in use, in motion or at rest

**Endpoint DLP**

Monitors all network endpoints, including servers, cloud repositories, computers, laptops, mobile phones and any other device on which data is used, moved or saved in order to prevent data leakage, loss or misuse

Assists in the classification of regulatory, confidential, proprietary or business-critical data in order to streamline reporting and compliance requirements

Tracks data stored on endpoints both on and off the network

**Cloud DLP**

Scans and audits data in the cloud to automatically detect and encrypt sensitive information before it is admitted to and stored in the cloud

Maintains a list of authorized cloud applications and users that can access sensitive data

Alerts the infosec team to policy violations or anomalous activity

Maintains a log of when confidential, cloud-based data is accessed and the user’s identify

Establishes end-to-end visibility for all data in the cloud

**Why Is DLP Important for Organizations?**

As companies move to a more remote and dispersed workforce and rely more heavily on cloud-based infrastructure, protecting sensitive data has become more challenging.

According to CrowdStrike Intelligence, ransomware related data leaks saw an 82% increase from 2020 to 2021. 2,686 data leak events happened in 2021 (compared to 1,474 in 2020) and were felt across sectors and industries, with the engineering and manufacturing sectors suffering most and the technology sector trailing behind them.

Anomaly detection

Anomaly detection, the “identification of rare occurrences, items, or events of concern due to their differing characteristics from the majority of the processed data,” allows organizations to track “security errors, structural defects and even bank fraud,” according to DeepAI and described in three main forms of anomaly detection as: unsupervised, supervised and semi-supervised. Security Operations Center (SOC) analysts use each of these approaches to varying degrees of effectiveness in Cybersecurity applications.

Often, Cybersecurity vendors make bold claims about artificial intelligence (AI) and its role in their anomaly detection products. Though these vendors imply that their AI enhancements can identify anomalies on their own, the reality often falls short. Even when these systems can identify anomalies (with or without AI tools), anomaly identification is a far cry from actually swatting down threats.

AI in Cybersecurity has become a marketing tool. Systems that rely on machine learning or supervised/unsupervised learning may be using “AI” but the technology is dated. So-called first- and second-wave AI can be taught to recognize anomalies that deviate from an expected norm (a baseline established by human operators), but true, self-learning AI is far less common among the options available in the Cybersecurity marketplace. Most available systems are limited by human interaction.

There’s no doubt that anomaly detection is helpful and necessary as a key component of Cybersecurity. Tools like User Behavioral Analytics (UBA) and Network Traffic Analysis (NTA) are based around anomaly detection. The key difference between Cybersecurity solutions that use these tools lies in what happens once an anomaly is detected.

**Endpoint security**

Endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats. Endpoint security has evolved from traditional antivirus software to providing comprehensive protection from sophisticated malware and evolving zero-day threats.

Organizations of all sizes are at risk from nation-states, hacktivists, organized crime, and malicious and accidental insider threats. Endpoint security is often seen as cybersecurity's frontline, and represents one of the first places organizations look to secure their enterprise networks.

As the volume and sophistication of cybersecurity threats have steadily grown, so has the need for more advanced endpoint security solutions. Today’s endpoint protection systems are designed to quickly detect, analyze, block, and contain attacks in progress. To do this, they need to collaborate with each other and with other security technologies to give administrators visibility into advanced threats to speed detection and remediation response times. [28]

**Why endpoint security is important**

An endpoint protection platform is a vital part of enterprise cybersecurity for several reasons. First of all, in today’s business world, data is the most valuable asset of a company —and to lose that data, or access to that data, could put the entire business at risk of insolvency. Businesses have also had to contend with not only a growing number of endpoints, but also a rise in the number of types of endpoints. These factors make enterprise endpoint security more difficult on their own, but they’re compounded by remote work and BYOD policies—which make perimeter security increasingly insufficient and create vulnerabilities. The threat landscape is becoming more complicated, as well: Hackers are always coming up with new ways to gain access, steal information or manipulate employees into giving out sensitive information. Add in the opportunity, cost of reallocating resources from business goals to addressing threats, the reputational cost of a large-scale breach, and the actual financial cost of compliance violations, and it’s easy to see why endpoint protection platforms have become regarded as must-haves in terms of securing modern enterprises. [8]

**How endpoint protection works**

Endpoint security is the practice of safeguarding the data and workflows associated with the individual devices that connect to your network. Endpoint protection platforms (EPP) work by examining files as they enter the network. Modern EPPs harness the power of the cloud to hold an ever-growing database of threat information, freeing endpoints of the bloat associated with storing all this information locally and the maintenance required to keep these databases up to date. Accessing this data in the cloud also allows for greater speed and scalability.

The EPP provides system administrators a centralized console, which is installed on a network gateway or server and allows cybersecurity professionals to control security for each device remotely. The client software is then assigned to each endpoint—it can either be delivered as a SaaS and managed remotely, or it can be installed directly on the device.

Once the endpoint has been set up, the client software can push updates to the endpoints when necessary, authenticate log-in attempts from each device, and administer corporate policies from one location. EPPs secure endpoints through application control—which blocks the use of applications that are unsafe or unauthorized—and through encryption, which helps prevent data loss.

When the EPP is set up, it can quickly detect malware and other threats. Some solutions also include an Endpoint Detection and Response (EDR) component. EDR capabilities allow for the detection of more advanced threats, such as polymorphic attacks, fileless malware, and zero-day attacks. By employing continuous monitoring, the EDR solution can offer better visibility and a variety of response options.

EPP solutions are available in on-premises or cloud based models. While cloud- based products are more scalable and can more easily integrate with your current architecture, certain regulatory/compliance rules may require on-premises security.[8, 21]

**Intrusion prevention systems**

In short, an Intrusion Prevention System (IPS), also known as intrusion detection prevention system (IDPS), is a technology that keeps an eye on a network for any malicious activities attempting to exploit a known vulnerability.

An Intrusion Prevention System’s main function is to identify any suspicious activity and either detect and allow (IDS) or prevent (IPS) the threat. The attempt is logged and reported to the network managers or Security Operations Center (SOC) staff.

**Why should Intrusion Prevention Systems be used?**

IPS technologies can detect or prevent network security attacks such as brute force attacks, Denial of Service (DoS) attacks and vulnerability exploits. A vulnerability is a weakness in a software system and an exploit is an attack that leverages that vulnerability to gain control of a system. When an exploit is announced, there is often a window of opportunity for attackers to exploit that vulnerability before the security patch is applied. An Intrusion Prevention System can be used in these cases to quickly block these attacks.

Because IPS technologies watch packet flows, they can also be used to enforce the use of secure protocols and deny the use of insecure protocols such as earlier versions of SSL or protocols using weak ciphers.[36]

**How do Intrusion Prevention Systems work?**

IPS technologies have access to packets where they are deployed, either as Network intrusion detection systems (NIDS), or as Host intrusion detection systems (HIDS). Network IPS has a larger view of the entire network and can either deployed inline in the network or offline to the network as a passive sensor that receives packets from a network TAP or SPAN port.

The detection method employed may be signature or anomaly-based. Predefined signatures are patterns of well-known network attacks. The IPS compares packet flows with the signature to see if there is a pattern match. Anomaly-based intrusion detection systems uses heuristics to identify threats, for instance comparing a sample of traffic against a known baseline.[13]

**What's the difference between IDS and IPS?**

Early implementations of the technology were deployed in detect mode on dedicated security appliances. As the technology has matured and moved into integrated Next Generation Firewall or UTM devices, the default action is set to prevent the malicious traffic.

In some cases, the decision to detect and accept or prevent the traffic is based upon confidence in the specific IPS protection. When there is lower confidence in an IPS protection, then there is a higher likelihood of false positives. A false positive is when the IDS identifies an activity as an attack but the activity is acceptable behavior. For this reason, many IPS technologies also have the ability to capture packet sequences from the attack event. These can then be analyzed to determine if there was an actual threat and to further improve the IPS protection.[13]

**Conclusions**

Secure network design including networks, data, tools and systems with an endpoint protection platform is a vital part of organisations’ cybersecurity for several reasons where in today’s business world, data is the most valuable asset of a company\organisation —and to lose that data, or access to that data, could put the entire organisation\business at risk of insolvency. They have also had to contend with not only a growing number of secure network implementations, but also a rise in the number of types of more specific tools and applications (such as endpoints).

**4**[**.4**](https://docs.google.com/document/d/1r9tAENn4JvJzvoSJP-L_gPrG4BwmCnxY/edit#heading=h.7pii0khen2cd) **Secure Cloud Controls and Solutions**

**Cloud Security Controls**

Cloud security controls are a set of security controls that protect cloud environments against vulnerabilities and mitigate the effects of malicious attacks.

A broad term, cloud security control includes all best practices, procedures, and guidelines that must be followed to secure cloud environments. Cloud security controls assist businesses in addressing, evaluating, and implementing cloud security.

A cloud service provider hosts a company’s applications on its servers and makes them available via the internet in cloud computing. At the same time, on-premises software is deployed in-house on a company’s servers.

Because cloud computing is different from on-premises deployment, it is reasonable to expect cloud security to be further as well. Before migrating to the cloud, organizations must understand how cloud security differs from data center security. It’s also essential for companies to implement cloud security controls after completing the migration.

While cloud service providers offer a range of cloud security tools and services to secure customers’ networks and applications, organizations must implement the necessary security controls. [33]

Also, when companies move their sensitive data and applications to the cloud, user access happens remotely. As a result, administrators must also implement cloud-based user access controls.

**What Does Cloud Security Controls Mean?**

A cloud security control is a collection of controls that enable the cloud architecture to protect against vulnerabilities and mitigate the impact of a malicious attack. It is a broad term encompassing all of the precautions, practices, and guidelines that must be put in place to safeguard a cloud computing environment.

Cloud security control primarily helps to consider, evaluate and implement security in the cloud. The Cloud Security Alliance (CSA) has created a Cloud Control Matrix (CCM) designed to help prospective cloud buyers assess the overall security of a cloud solution.

Although there are unlimited cloud security controls, they are similar to standard information security controls and can be categorized in different domains, including:

Deterrent Controls: Do not protect the cloud environment but serve as a warning to a potential attacker.

Preventive Controls: Used to manage, strengthen and protect vulnerabilities within a cloud.

Corrective Controls: Helps reduce the after-effects of an attack.

Detective Checks: Used to identify or detect an attack.

**What Kinds of Cloud Computing Security Controls Exist?**

Your organization and the cloud service providers with whom you do business share responsibility for enforcing cloud security controls that protect applications and data stored or distributed in the cloud.

These controls include security controls such as establishing data recovery and business continuity plans, encrypting data, and controlling cloud access to reduce, mitigate or eliminate various types of risk.

While there are numerous types of cloud computing security audits available, they are typically classified into the four categories listed below:

Deterrent Controls – Deterrent controls are intended to keep malicious actors away from a cloud system. Deterrent controls inform attackers that there will be negative consequences if they continue to steal data or engage in any suspicious activity. They work more like a warning system. Insider attacks pose a risk to cloud service providers, so one deterrent control would be for a cloud service provider to conduct criminal background checks on employees. These checks can warn that an attack will face the consequences. [40]

Preventive Controls – Preventive controls strengthen the cloud’s resilience to attacks by removing security flaws. A preventative measure would be to write code that disables inactive ports, ensuring that hackers have no suitable entry points. Another way to reduce vulnerability to attack is to maintain a robust user authentication system. Preventive controls are critical to system strengthening. Strong authentication of the cloud user, for example, ensures that only authorized personnel can access the data.

Detective Controls – Detective controls are designed to detect and respond to security threats and events. Detective controls are designed to detect and appropriately respond to any event that may appear on the online platform where you place your data. Detective controls include intrusion detection software and network security monitoring tools. Also, monitoring the network to determine when an attack might occur is an example of detective control. In an attack, detective controls trigger security protocols and appeal to the attacker and the owner of the data, which is something suspicious. System and network security monitoring, intrusion detection systems, and prevention arrangements are part of detection controls.[38]

Corrective Controls – In a security breach, corrective controls are activated. The task of corrective controls is to limit the damage caused by the event. A software developer can write a code to disconnect data servers from the network when a specific type of threat is detected to prevent data theft. Corrective controls usually come into play during or after the event, limiting the damage of attacks. An example of this is backing up the system in case of an attack.

**What Are the Applicable Cloud Computing Security Controls?**

Cloud computing security generally refers to various policies, technologies and controls deployed to protect cloud data, applications, and related cloud computing infrastructure. Cloud security architecture is only effective when you have an appropriate security and defense system and process.

Security concerns related to cloud computing fall into two main categories:

Security issues faced by cloud security providers

Security issues faced by customers using cloud security software

Responsibility for securing data is divided between cloud service providers and customers. The cloud service provider must always ensure that the infrastructure is secure and that its client’s information is protected.

On the other hand, users should strictly control their cloud security practices and prevent security protocols such as strong passwords and authentication methods so that only authorized personnel can access the data.

Physical availability decreases when an organization decides to bring its data online with a cloud security software or application. Therefore, it is necessary to keep an eye on employees who have access to this information, as insider attacks are a massive threat to organizations and businesses. In addition, data centers often need to be under surveillance.

Below are the useful vital features that need to be addressed when deploying cloud security controls. By implementing these controls, you can take advantage of the agility and customer focus of the cloud without sacrificing the security or compliance you need:

**Data Protection in Cloud Environments**

If you choose to host sensitive data with a cloud service provider, you lose control of physical access to the server. This creates additional security vulnerabilities as you can no longer play a role in determining who has physical access to servers.

An employee of the cloud service provider can illegally access, modify or copy data and even distribute it to others. To prevent insider attacks, cloud service providers must perform detailed employee background checks and maintain strict and transparent access to servers and IT infrastructure.

Also, knowing what your users and systems are doing requires reviewing log files. In the cloud, you will likely need to rely on your vendor to provide log files, and you probably won’t be able to review the logs of the underlying shared infrastructure.

You should ensure that logs are aggregated and flowing into your event management tool despite potentially limited information.

**Centralized visibility of cloud infrastructure**

One of the most challenging challenges in cloud computing security is the lack of visibility into cloud-deployed applications and services. Lack of visibility means you cannot efficiently gather information about the security state of applications and infrastructure deployed in the cloud.

This may be because many different systems are working together in the cloud, or there is no transparency between the business and the cloud service provider.

Cloud security control fundamentals include centralized visibility into security policies, configuration settings, and user activity, as well as risks that may be stored in online data stores. This makes it less likely for your security team to overlook a vulnerability in cloud security due to misconfiguration or a lack of abnormal activity that could indicate an attack.

The problem is that different clouds provide different configuration options, and developers frequently select these options without security expertise. It is not easy to gain visibility across instances and clouds.

Security teams require centralized visibility into their cloud infrastructure to reduce such risks. Cloud workload protection (CWP) tools, tightly integrated into cloud management and security systems, can assist with this task.

Cloud workload protection (CWP) tools give security teams the ability to monitor and evaluate existing services’ configuration status and the overall security posture of the cloud environment. Automatic configuration monitoring allows IT teams to quickly identify and respond to security misconfigurations, reducing the time it takes to implement fixes while

increasing security.

Critical capabilities of adequate workload protection and platform security tools include:

Traffic analysis

Examination of data stored in the cloud for sensitive or malicious content

Regular configuration monitoring and evaluations

Recommendations on how to improve vulnerable areas of the cloud environment

Warnings for configuration issues

Identifying compatibility issues due to misconfiguration

Integration with cloud management and security systems on a native level

In legacy IT systems deployed and managed on-premises, IT organizations, maintain complete control over every piece of IT infrastructure across the entire technology stack. Delegating some of your IT infrastructure to a cloud service provider, on the other hand, entails giving up some control over how that infrastructure is deployed, managed, and configured.

As a result, IT organizations must increasingly rely on cloud service providers to make administrative decisions that enforce a high level of security.

Unlike traditional data centers, cloud computing relies on a shared responsibility model where the customer and others control some security settings by the public cloud vendor.

Visibility of your security posture across clouds requires close coordination between your solution and the underlying cloud environment. This means API-level integration with tools such as Amazon Inspector and VPC Flow logs and GuardDuty for AWS, Stack Event, Security Center for Azure, and Stream Drivers for Google Cloud Platform.

A cloud access security broker (CASB) solution that integrates deeply with the SaaS service may be required to identify risks and configuration issues.[41]

**Cloud Security Through User Authentication and Access Management**

Cloud services should be protected by a username and password. Still, a malicious actor always risks stealing login credentials, gaining unauthorized access to cloud services, and stealing or modifying data.

An attacker can also install malicious code on the system. Cloud service providers must implement a secure authentication and access management system to protect customers from such attacks.

Controlling who can access your data and managing their privileges is critical to information security. For your data in the cloud, you must understand the cloud provider’s controls over their employees’ access to your systems.

You should extend your identity and access management to the cloud using federated security with single sign-on and role-based privileges to reduce the number of identities and privileges to manage. Root privileges, which should always be minimized, must be even more tightly managed in the cloud.[32]

**Additional web application layer protections**

Additional vulnerabilities arise when it is unclear who is responsible for protecting the cloud infrastructure. Your company is in charge of the security of cloud-based applications and data. Cloud service providers take responsibility for infrastructure only.

To best fulfill their role in the shared responsibility model, your organizations should use web application firewalls to secure web applications. App threat detection differs when apps run in the cloud rather than on-premises because controlling access to specific IP addresses does not work with cloud-deployed apps.

Here, threat detection should occur in the application content, not traffic. This requires constant granular adjustments that you cannot handle manually.

Only an approach that takes advantage of AI’s computing power and speed will be able to protect today’s cloud-based applications. Machine learning can assist in detecting the type of user or application behavior that indicates a problem and implementing safeguards that no human-assisted approach can match in terms of speed or accuracy.

**Threat intelligence feeds**

The more complex your cloud environment, the more vulnerable it is to threats. Maximum cloud security is provided by a comprehensive solution that brings all of your company’s cloud services under one roof.

A good solution should include dynamic threat intelligence feeds with extensive global and local security event intelligence. When selecting cloud security controls, look for providers whose solutions are informed by data collected across all of their deployed sensors.

**Cloud security automation**

The cybersecurity field is insufficient to meet all corporate needs due to the cybersecurity skills gap. Today, cybersecurity professionals are in high demand, and existing security teams have a variety of skill gaps. After all, such issues expose businesses to a wide range of threats.

Until the cybersecurity industry can keep up with enterprise needs and demands for a larger and more capable talent pool, security architects are encouraged to help organizations automate their security functions wherever possible.

One approach currently used includes plugins that provide administrators with greater visibility into multivendor ecosystems, automation, and simplified management. When application changes occur, IT and DevOps teams can stay up to date without updating security policies each time application features change.

Security configuration scripts, available for download from security providers, can also help automate security processes.

**Patch management in the cloud**

While your servers are in the cloud, the need to know about your systems’ vulnerabilities and apply patches does not disappear. For some types of cloud services, the vendor will resolve these issues, but you remain responsible for some versions of Infrastructure as a Service.

The challenge of keeping track of whether patches have been applied becomes more complex as servers in the cloud are up and down much more frequently. You will want to scan for security vulnerabilities continuously, not periodically.

**Cloud Access Security Broker**

A Cloud Access Security Broker, or CASB, is cloud-hosted software or on-premises software or hardware that act as an intermediary between users and cloud service providers. The ability of a CASB to address gaps in security extends across software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) environments. In addition to providing visibility, a CASB also allows organizations to extend the reach of their security policies from their existing on-premises infrastructure to the cloud and create new policies for cloud-specific context. CASBs have become a vital part of enterprise security, allowing businesses to safely use the cloud while protecting sensitive corporate data. The CASB serves as a policy enforcement center, consolidating multiple types of security policy enforcement and applying them to everything your business utilizes in the cloud—regardless of what sort of device is attempting to access it, including unmanaged smartphones, IoT devices, or personal laptops. With the increase in workforce mobility, the growth in BYOD and the presence of unsanctioned employee cloud usage, or Shadow IT, the ability to monitor and govern the usage of cloud applications such as Microsoft 365 has become essential to the goal of enterprise security. Rather than banning cloud services outright and potentially impacting employee productivity, a CASB enables businesses to take a granular approach to data protection and the enforcement of policies—making it possible to safely utilize time-saving, productivity-enhancing, and cost-effective cloud services. [23]

**What CASBs offer**

Many CASB security features are unique compared with those offered by other security controls such as enterprise/web application firewalls and secure web gateways, and may include:

Cloud governance and risk assessment

Data loss prevention

Control over native features of cloud services, like collaboration and sharing

Threat prevention, often user and entity behavior analytics (UEBA)

Configuration auditing

Malware detection

Data encryption and key management

SSO and IAM integration

Contextual access control

**How does a CASB work?**

The job of a cloud access security broker is to provide visibility and control over data and threats in the cloud to meet enterprise security requirements. This is done through a three-step process:

Discovery: The CASB solution uses auto-discovery to compile a list of all third-cloud services, as well as who is using them.

Classification: Once the full extent of cloud usage is revealed, the CASB then determines the risk level associated with each by determining what the application is, what sort of data is within the app, and how it is being shared.

Remediation: After the relative risk of each application is known, the CASB can use this information to set policy for the organization’s data and user access to meet their security requirements, and automatically take action when a violation occurs.

CASBs also offer additional layers of protection through malware prevention and data encryption. [29]

**Conclusions**

Cloud computing is a promising area (relatively a new area in IT) which provide effective solution for various organisations by hosting their applications and data on its servers and making them available via the internet. Cloud computing is still a developing field which also provides various career opportunities in the IT field. Since the hosting of the organisations’ data on servers, its security is such a critical subject where cloud security implementations are a must, which portrays a wide range of efforts to fulfil the security requirements. With the increasing amount of data stored online, cloud computing gains a more important role in making it possible to safely utilize time-saving, productivity-enhancing, and cost-effective cloud services.

**The Geek’s Corner**

**Data-Centric Audit and Protection (DCAP)**

Data-centric audit and protection (DCAP) is a term used by Gartner, a business research and consulting company, to describe a type of data-centric security. The goal of DCAP is to protect an organization’s data privacy and apply it to specific pieces of data, not the entire organization.

DCAP focuses on:

● Classifying data

● Storing sensitive data

● Data security governance

● Protecting data against unauthorized access

● Data monitoring and auditing

Read more about DCAP for Geeks:

<https://www.microfocus.com/en-us/what-is/data-centric-audit-protection-dcap>

<https://www.lepide.com/blog/what-is-data-centric-audit-and-protection-dcap/>

<https://www.trustradius.com/data-centric-audit-protection>

<https://www.ibm.com/docs/en/hpdc/1.2.3?topic=overview-data-centric-protection>

**Conclusions**

In this unit, we briefly covered various security controls and solutions which are parameters implemented to protect various forms of data and infrastructure important to an organization ranging from the key design, architectural and implementation solutions\choices made by organizations in satisfying specified security requirements for systems or system components. In addition, cloud computing area was covered as it provides unique services to host organisations’ data on cloud platforms, which still has a long way to advance its services and security aspects, similar with other security control and solution tools and studies.

**Quiz**

| 1. **One operation that frequently has cross-site scripting (XSS) vulnerabilities is?**
 |
| --- |
|   |  |  |  |  |
|   | 1. A user visits a site's homepage.
 |  |  |  |  |
|   | 1. A site prompts the user for their user name and password.
 |  |  |  |  |
|   | 1. **A site produces an error message for an invalid user name.**
 |  |  |  |  |
|   | 1. A user clicks on a hyperlink to visit another page in the same site.
 |  |  |  |  |
|   | 1. A user clicks on a hyperlink to visit another page in a different site.
 |  |  |  |  |

|   **2. One common strategy to prevent XSS vulnerabilities is to?** |
| --- |
|   |  |  |  |  |
|   | 1. Educate your users to recognize safe vs. unsafe web pages.
 |  |  |  |  |
|   | 1. Escape user's input is valid as soon as possible.
 |  |  |  |  |
|   | 1. **Avoid using JavaScript in your site.**
 |  |  |  |  |
|   | 1. Use an interpreted programming language such as Java or C#.
 |  |  |  |  |
|   | 1. Make sure your database is configured for strong security.
 |  |  |  |  |

|   **3. In a typical N-tier web application with a DMZ, standard security practices dictate that encryption is required when (choose 1 or more answers):** |
| --- |
|   |  |  |  |  |
|   | 1. Displaying the logon page's form.
 |  |  |  |  |
|   | 1. Credit card numbers are being transmitted to the site.
 |  |  |  |  |
|   | 1. **Credit card numbers are being transmitted between two machines within the DMZ itself.**
 |  |  |  |  |
|   | 1. Credit card numbers are being transmitted between two machines within the secure network behind the DMZ.
 |  |  |  |  |
|   | 1. Never. Encryption is always required.
 |  |  |  |  |

  **4. What is the top vulnerability leading to data breaches?**

1. **SQL Injection**
2. Cross-Site Scripting
3. Cross-Site Request Forgery
4. Sensitive Data Exposure

**References**

1. Aldhyani, T.H.; Alkahtani, H. Attacks to automatous vehicles: A deep learning algorithm for cybersecurity. Sensors 2022, 22, 360. [CrossRef]

2. Alrawi, O.; Lever, C.; Antonakakis, M.; Monrose, F. SoK: Security Evaluation of Home-Based IoT Deployments. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 1362–1380.

3. Al-Saud, M.; Eltamaly, A.M.; Mohamed, M.A.; Kavousi-Fard, A. An intelligent data-driven model to secure intravehicle communications based on machine learning. IEEE Trans. Ind. Electron. 2019, 67, 5112–5119. [CrossRef]

4. Aly, M.; Khomh, F.; Haoues, M.; Quintero, A.; Yacout, S. Enforcing security in Internet of Things frameworks: A Systematic Literature Review. Internet Things 2019, 6, 100050. [CrossRef]

5. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. J. Inf. Secur. Appl. 2018, 38, 8–27. [CrossRef]

6. Apostu, S.; Burkacky, O.; Deichmann, J.; Doll, G. Automotive Software and Electrical/Electronic Architecture: Implications for OEMs. 2019. Available online: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/automotivesoftware-andelectrical-electronic-architecture-implications-for-oems (accessed on 16 July 2022).

7. Bali, R.S.; Jaafar, F.; Zavarasky, P. Lightweight Authentication for MQTT to Improve the Security of IoT Communication. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP ’19), Kuala Lumpur, Malaysia, 19–21 January 2019; pp. 6–12.

8. Bandur, V.; Selim, G.; Pantelic, V.; Lawford, M. Making the case for centralized automotive e/e architectures. IEEE Trans. Veh. Technol. 2021, 70, 1230–1245. [CrossRef]

9. Carvajal-Roca, I.E.; Wang, J.; Du, J.; Wei, S. A Semi-Centralized Dynamic Key Management Framework for In-Vehicle Networks. IEEE Trans. Veh. Technol. 2021, 70, 10864–10879. [CrossRef]

10.Cheshire, S.; Krochmal, M. DNS-Based Service Discovery. Available online: https://tools.ietf.org/html/ rfc6763 (accessed on 15 March 2023).

11. Cheshire, S.; M.K. Multicast DNS. Available online: https://tools.ietf.org/html/rfc6762 (accessed on 15 March 2023).

12. D’Angelo, G.; Castiglione, A.; Palmieri, F. A cluster-based multidimensional approach for detecting attacks on connected vehicles. IEEE Internet Things J. 2020, 8, 12518–12527. [CrossRef]

13. Dizdarevi´c, J.; Carpio, F.; Jukan, A.; Masip, X. A Survey of Communication Protocols for Internet of Things and Related Challenges of Fog and Cloud Computing Integration. ACM Comput. Surv. 2019, 51, 116. [CrossRef]

14. Dinculean˘a, D. Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices. Appl. Sci. 2019, 9, 848. [CrossRef]

15. E. Rescorla, N.M. Datagram Transport Layer Security Version 1.2. Available online: https://tools.ietf.org/ html/rfc6347 (accessed on 15 March 2023).

16. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. Veh. Commun. 2020, 23, 100214. [CrossRef]

17. Groza, B.; Popa, L.; Murvay, P.S. Highly efficient authentication for CAN by identifier reallocation with ordered CMACs. IEEE Trans. Veh. Technol. 2020, 69, 6129–6140. [CrossRef]

18. Guo, J.; Li, X.; Liu, Z.; Ma, J.; Yang, C.; Zhang, J.; Wu, D. TROVE: A context-awareness trust model for VANETs using reinforcement learning. IEEE Internet Things J. 2020, 7, 6647–6662. [CrossRef]

19. Guan, T.; Han, Y.; Kang, N.; Tang, N.; Chen, X.; Wang, S. An overview of vehicular cybersecurity for intelligent connected vehicles. Sustainability 2022, 14, 5211. [CrossRef]

20. Hanes, D.; Salquiero, G.; Grossetete, P.; Barton, R.; Henry, J. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things; Cisco Press: Indianapolis, IN, USA, 2017.

21. He, Y.; Jia, Z.; Hu, M.; Cui, C.; Cheng, Y.; Yang, Y. The Hybrid Similar Neighborhood Robust Factorization Machine Model for Can Bus Intrusion Detection in the In-Vehicle Network. IEEE Trans. Intell. Transp. Syst. 2021, 1, 1–9. [CrossRef]

22. Hossain, M.D.; Inoue, H.; Ochiai, H.; Fall, D.; Kadobayashi, Y. LSTM-based intrusion detection system for in-vehicle can bus communications. IEEE Access 2020, 8, 185489–185502. [CrossRef]

23.Karopoulos, G.; Kambourakis, G.; Chatzoglou, E.; Hernández-Ramos, J.L.; Kouliaridis, V. Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy. Electronics 2022, 11, 1072. [CrossRef]

23. Katragadda, S.; Darby, P.J.; Roche, A.; Gottumukkala, R. Detecting low-rate replay-based injection attacks on in-vehicle networks. IEEE Access 2020, 8, 54979–54993. [CrossRef]

24. Lenard, T.; Bolboacă, R.; Genge, B.; Haller, P. MixCAN: Mixed and backward-compatible data authentication scheme for controller area networks. In Proceedings of the 2020 IFIP Networking Conference (Networking), Paris, France, 22–26 June 2020; pp. 395–403.

25.Liu, H.; Spink, T.; Patras, P. Uncovering Security Vulnerabilities in the Belkin WeMo Home Automation Ecosystem. In Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 11–15 March 2019; pp. 894–899.

26.Li, X.; Hu, Z.; Xu, M.; Wang, Y.; Ma, J. Transfer learning based intrusion detection scheme for Internet of vehicles. Inf. Sci. 2021, 547, 119–135. [CrossRef]

27. Lin, Y.; Chen, C.; Xiao, F.; Avatefipour, O.; Alsubhi, K.; Yunianta, A. An Evolutionary Deep Learning Anomaly Detection Framework for In-Vehicle Networks—CAN Bus. IEEE Trans. Ind. Appl. 2020, 1, 1–14. [CrossRef]

28.Loi, F.; Sivanathan, A.; Gharakheili, H.H.; Radford, A.; Sivaraman, V. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In Proceedings of the Workshop on Internet of Things Security and Privacy (IoTS&P), Dallas, TX, USA, 3 November 2017.

29. Lo, W.; Alqahtani, H.; Thakur, K.; Almadhor, A.; Chander, S.; Kumar, G. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Veh. Commun. 2022, 35, 100471. [CrossRef]

30. Ma, B.; Yang, S.; Zuo, Z.; Zou, B.; Cao, Y.; Yan, X.; Zhou, S.; Li, J. An Authentication and Secure Communication Scheme for In-Vehicle Networks Based on SOME/IP. Sensors 2022, 22, 647. [CrossRef]

31. Malina, L.; Srivastava, G.; Dzurenda, P.; Hajny, J.; Fujdiak, R. A Secure Publish/Subscribe Protocol for Internet of Things. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019), Canterbury, UK, 26–29 August 2019.

31. Moulahi, T.; Zidi, S.; Alabdulatif, A.; Atiquzzaman, M. Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus. IEEE Access 2021, 9, 99595–99605. [CrossRef]

32. Mun, H.; Han, K.; Lee, D.H. Ensuring safety and security in CAN-based automotive embedded systems: A combination of design optimization and secure communication. IEEE Trans. Veh. Technol. 2020, 69, 7078–7091. [CrossRef]

33. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. IEEE Commun. Surv. Tutor. 2019, 21, 2702–2733. [CrossRef]

34. Noor, M.b.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294. [CrossRef]

35. Pekaric, I.; Sauerwein, C.; Haselwanter, S.; Felderer, M. A taxonomy of attack mechanisms in the automotive domain. Comput. Stand. Interfaces 2021, 78, 103539. [CrossRef]

36. Radoglou Grammatikis, P.I.; Sarigiannidis, P.G.; Moscholios, I.D. Securing the Internet of Things: Challenges, threats and solutions. Internet Things 2019, 5, 41–70. [CrossRef]

37. Riahi Sfar, A.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. Digit. Commun. Netw. 2018, 4, 118–137. [CrossRef]

38. Saint-Andre, P. Extensible Messaging and Presence Protocol (XMPP): Core. Available online: https: //tools.ietf.org/html/rfc6120 (accessed on 15 March 2023).

39. Shelby, Z.; Hartke, K.; Bormann, C. The Constrained Application Protocol (CoAP). Available online: https://tools.ietf.org/html/rfc7252 (accessed on 15 March 2023).

40. Song, H.M.; Kim, H.K. Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data. IEEE Trans. Veh. Technol. 2021, 70, 1098–1108. [CrossRef]

41. Sun, X.; Yu, F.R.; Zhang, P. A survey on cyber-security of connected and autonomous vehicles (CAVs). IEEE Trans. Intell. Transp. Syst. 2021, 23, 6240–6259. [CrossRef]

42. Walrand, J.; Turner, M.; Myers, R. An architecture for in-vehicle networks. IEEE Trans. Veh. Technol. 2021, 70, 6335–6342. [CrossRef]

43. Xie, G.; Yang, L.T.; Liu, Y.; Luo, H.; Peng, X.; Li, R. Security enhancement for real-time independent in-vehicle CAN-FD messages in vehicular networks. IEEE Trans. Veh. Technol. 2021, 70, 5244–5253. [CrossRef]

44. Youn, T.Y.; Lee, Y.; Woo, S. Practical sender authentication scheme for in-vehicle CAN with efficient key management. IEEE Access 2020, 8, 86836–86849. [CrossRef]

45. Zhang, L.; Ma, D. A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks. IEEE Access 2022, 10, 10852–10866. [CrossRef]