**Critical infrastructure security:**

The protection of systems, networks, and assets whose continuous operation is deemed necessary to ensure the security of a given nation, its economy, and the public's health and/or safety is referred to as critical infrastructure security.

Although the components of critical infrastructure vary depending on the country, there are many similarities among nations.The Department of Homeland Security (DHS) in the United States has identified 16 critical infrastructure sectors, including energy, communications, transportation, financial services, food and agriculture.

Devices in industrial environments are increasingly connected to the internet and capable of exchanging data, thanks to ongoing trends in M2M networking and the Internet of Things (IoT). Despite the importance of these systems, security is frequently inadequate for those who are not involved in IT (information technology).

**Application security:**

Application security refers to security measures implemented at the application level to prevent data or code contained within the app from being stolen or hijacked. It includes security considerations during application development and design, as well as systems and approaches to protect apps after they are deployed.

Application security may include hardware, software, and procedures for identifying and mitigating security flaws. A router that prevents Internet users from viewing a computer's IP address is an example of hardware application security. However, application-level security measures, such as an application firewall that strictly defines what activities are allowed and prohibited, are typically built into the software. Procedures can include things like an application security routine with protocols like regular testing.

**Network security:**

Network security is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies. Every organization, regardless of size, industry or infrastructure, requires a degree of network security solutions in place to protect it from the ever-growing landscape of cyber threats in the wild today.

Today's network architecture is complex, with a constantly changing threat environment and attackers constantly looking for and exploiting vulnerabilities. These flaws can exist in a variety of contexts, including devices, data, applications, users, and locations. As a result, many network security management tools and applications are now in use to address individual threats and exploits as well as regulatory non-compliance. When a few minutes of downtime can cause widespread disruption and massive damage to an organization's bottom line and reputation, these safeguards are critical.

**Cloud security.**

Cloud security is a cyber security discipline devoted to the protection of cloud computing systems. This includes keeping data private and secure across online infrastructure, applications, and platforms. Securing these systems requires the efforts of cloud providers as well as the clients who use them, whether they are individuals, small to medium businesses, or enterprises.

Cloud providers host services on their servers via always-on internet connections. Because their business relies on customer trust, cloud security methods are used to keep client data private and secure. However, cloud security is also partly in the hands of the client. Understanding both aspects is critical for a healthy cloud security solution.

At its core, cloud security is composed of the following categories:

* Data security
* Identity and access management (IAM)
* Governance (policies on threat prevention, detection, and mitigation)
* Data retention (DR) and business continuity (BC) planning
* Legal compliance

**Internet of Things (IoT) security:**

The practice of securing Internet of Things (IoT) devices and the networks they use is known as IoT security. Its primary goals are to protect users' privacy and data confidentiality, to ensure the security of devices and other related infrastructures, and to ensure the smooth operation of the IoT ecosystem. IoT security is a broad, but necessary, topic. The Internet of Things (IoT) is a broad field in and of itself because it involves adding internet connectivity to "things" or devices with specific functions, which has proven to have a vast and ever-expanding range of applications.

Each connected device, however, broadens the attack surface and increases the possibility of cyberattacks. The Internet of Things (IoT) can be a tempting target for cybercriminals because it contains a wealth of data, is used for critical functions, and is implemented in critical industries. IoT is already plagued by vulnerabilities and attacks such as distributed denial of service (DDoS), malware infection, and data breaches. These threats highlight the importance of developing robust IoT security. IoT security strategies, practices, and tools are constantly evolving to keep up with an ever-changing technology.

**Anti-Virus:**

Software designed specifically to detect, prevent, and remove malware (malicious software).

Antivirus software is used to prevent, scan, detect, and remove viruses from a computer. Most antivirus software, once installed, runs automatically in the background to provide real-time protection against virus attacks.

Comprehensive virus protection software protects your files and hardware from malware such as worms, Trojan horses, and spyware, and may also provide additional security features such as customizable firewalls and website blocking.

**Critical infrastructure security.**

**Access Control**

Access control is a critical component of data security that governs who has access to and uses company information and resources. Access control policies ensure that users are who they say they are and have appropriate access to company data through authentication and authorization. Physical access to campuses, buildings, rooms, and datacenters can also be restricted using access control.

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:

1. **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.
2. **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.
3. **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.
4. **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.

**Application Security:**

Application security aims to protect software application code and data against cyber threats. You can and should apply application security during all phases of development, including design, development, and deployment.

Here are several ways to promote application security throughout the software development lifecycle (SDLC):

* Introduce security standards and tools during design and application development phases. For example, include vulnerability scanning during early development.
* Implement security procedures and systems to protect applications in production environments. For example, perform continuous security testing.
* Implement strong authentication for applications that contain sensitive data or are mission critical.
* Use security systems such as firewalls, web application firewalls (WAF), and intrusion prevention systems (IPS).

**Firewalls:**

A firewall is a type of network security device that monitors incoming and outgoing network traffic and allows or denies data packets based on a set of security rules. Its purpose is to create a barrier between your internal network and incoming traffic from outside sources (such as the internet) in order to prevent malicious traffic such as viruses and hackers.

But how do we know were getting attacked? To prevent attacks, firewalls carefully analyze incoming traffic based on pre-defined rules and filter traffic coming from unsecured or suspicious sources. Firewalls protect traffic at a computer's entry point, known as ports, where data is exchanged with external devices. "Source address 172.18.1.1 is permitted to reach destination 172.18.2.1 via port 22," for example.

Consider IP addresses to be houses, and port numbers to be rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on whether they're the owner, a child, or a guest.

**Application Security**

**Authentication**

* is used by a server when the server needs to know exactly who is accessing their information or site.
* Authentication is used by a client when the client needs to know that the server is system it claims to be.
* Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to.
* Authentication does not determine what tasks the individual can do or what files the individual can see. Authentication merely identifies and verifies who the person or system is.
* Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.

**Authorization**

* Authorization is a process by which a server determines if the client has permission to use a resource or access a file.
* Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.
* The type of authentication required for authorization may vary; passwords may be required in some cases but not in others.
* In some cases, there is no authorization; any user may use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

**Encryption**

* Encryption involves the process of transforming data so that it is unreadable by anyone who does not have a decryption key.
* The Secure Shell (SSH) and Socket Layer (SSL) protocols are usually used in encryption processes. The SSL drives the secure part of “https://” sites used in e-commerce sites (like E-Bay and Amazon.com.)
* All data in SSL transactions is encrypted between the client (browser) and the server (web server) before the data is transferred between the two.
* All data in SSH sessions is encrypted between the client and the server when communicating at the shell.
* By encrypting the data exchanged between the client and server, information like social security numbers, credit card numbers, and home addresses can be sent over the Internet with less risk of being intercepted during transit.

**Logging**

Most developers already use logging for debugging and diagnostic purposes. Security logging is an equally simple concept: log security information while an application is running. Monitoring is the process of reviewing application and security logs in real time using various forms of automation. For operations, debugging, and security, the same tools and patterns can be used.

## **Benefits of Security Logging**

* Security logging can be used for:
* Feeding intrusion detection systems
* Forensic analysis and investigations
* Satisfying regulatory compliance requirements

## **Security Logging Implementation**

The following is a list of security logging implementation best practices.

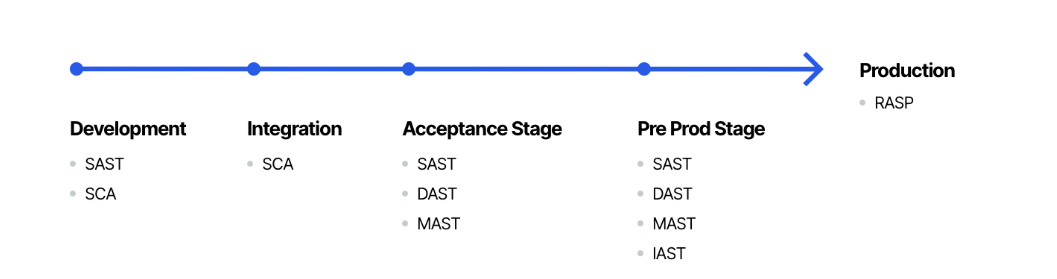
* Follow a common logging format and approach within the system and across systems of an organization. An example of a common logging framework is the Apache Logging Services which helps provide logging consistency between Java, PHP, .NET, and C++ applications.
* Do not log too much or too little. For example, make sure to always log the timestamp and identifying information including the source IP and user-id, but be careful not to log private or confidential data.
* Pay close attention to time syncing across nodes to ensure that timestamps are consistent.

https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging

**Application security testing**

The process of making applications more resistant to security threats by identifying security flaws and vulnerabilities in source code is known as application security testing (AST).

AST began as a manual process. Today, AST must be automated due to the increasing modularity of enterprise software, the large number of open source components, and the large number of known vulnerabilities and threat vectors. Most businesses use a combination of application security tools.



https://www.imperva.com/learn/application-security/application-security-testing/#:~:text=Application%20security%20testing%20(AST)%20is,and%20vulnerabilities%20in%20source%20code.

**Network Security**

**Network Segmentation**

A computer network is segmented when it is divided into smaller parts. The goal is to boost network performance and security. Network segregation, network partitioning, and network isolation are all terms that often mean the same thing.

### **How does segmentation work?** Segmentation works by controlling how traffic flows among the parts. You could choose to stop all traffic in one part from reaching another, or you can limit the flow by traffic type, source, destination, and many other options. How you decide to segment your network is called a segmentation policy.

### **What is an example of segmentation?** Imagine a large bank with several branch offices. The bank's security policy restricts branch employees from accessing its financial reporting system. Network segmentation can enforce the security policy by preventing all branch traffic from reaching the financial system. And by reducing overall network traffic, the financial system will work better for the financial analysts who use it.

### **What enforces segmentation policy?** Some traditional technologies for segmentation included internal firewalls, and Access Control List (ACL) and Virtual Local Area Network (VLAN) configurations on networking equipment. However, these approaches are costly and difficult. Today, software-defined access technology simplifies segmentation by grouping and tagging network traffic. It then uses traffic tags to enforce segmentation policy directly on the network equipment, yet without the complexity of traditional approaches.

### **What is microsegmentation?** Microsegmentation uses much more information in segmentation policies like application-layer information. It enables policies that are more granular and flexible to meet the highly-specific needs of an organization or business application.

## **Benefits of network segmentation**

### **Improve operational performance** Segmentation reduces network congestion. For example, a hospital's medical devices can be segmented from its visitor network so that medical devices are unaffected by web browsing.

### **Limit cyberattack damage** Segmentation improves cybersecurity by limiting how far an attack can spread. For example, segmentation keeps a malware outbreak in one section from affecting systems in another.

### **Protect vulnerable devices** Segmentation can stop harmful traffic from reaching devices that are unable to protect themselves from attack. For example, a hospital's connected infusion pumps may not be designed with advanced security defenses. Network segmentation can stop harmful Internet traffic from ever reaching them.

### **Reduce the scope of compliance** Segmentation reduces the costs associated with regulatory compliance by limiting the number of in-scope systems. For example, segmentation separates the systems that process payments from those that don't. That way, the expensive compliance requirements and audit processes apply only to the in-scope systems, not the entire network.

https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

**Remote Access VPN.**

A remote access virtual private network (VPN) enables users who are working remotely to securely access and use applications and data that reside in the corporate data center and headquarters, encrypting all traffic the users send and receive.

The remote access VPN does this by creating a tunnel between an organization’s network and a remote user that is “virtually private,” even though the user may be in a public location. This is because the traffic is encrypted, which makes it unintelligible to any eavesdropper. Remote users can securely access and use their organization’s network in much the same way as they would if they were physically in the office.

<https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn#:~:text=A%20remote%20access%20virtual%20private,the%20users%20send%20and%20receive>.

- Intrusion Prevention Systems

An intrusion prevention system (IPS) is a network security tool (either hardware or software) that continuously monitors a network for malicious activity and takes action to prevent it, such as reporting, blocking, or dropping it, if it does occur.

It is more sophisticated than an intrusion detection system (IDS), which detects malicious activity but does nothing more than alert an administrator. In some cases, intrusion prevention systems are included as part of a next-generation firewall (NGFW) or unified threat management (UTM) solution. They, like many other network security technologies, must be powerful enough to scan a large volume of traffic without degrading network performance.

**How does an intrusion prevention system work?**

An intrusion prevention system is placed inline, in the flow of network traffic between the source and destination, and usually sits just behind the firewall. There are several techniques that intrusion prevention systems use to identify threats:

* **Signature-based:** This method matches the activity to signatures of well-known threats. One drawback to this method is that it can only stop previously identified attacks and won’t be able to recognize new ones.
* **Anomaly-based:** This method monitors for abnormal behavior by comparing random samples of network activity against a baseline standard. It is more robust than signature-based monitoring, but it can sometimes produce false positives. Some newer and more advanced intrusion prevention systems use artificial intelligence and machine learning technology to support anomaly-based monitoring.
* **Policy-based:** This method is somewhat less common than signature-based or anomaly-based monitoring. It employs security policies defined by the enterprise and blocks activity that violates those policies. This requires an administrator to set up and configure security policies.

**Types of intrusion prevention systems**

**There are several types of IPS, each with a slightly different purpose:**

* Network intrusion prevention system (NIPS): This type of IPS is installed only at strategic points to monitor all network traffic and proactively scan for threats.
* Host intrusion prevention system (HIPS): In contrast to a NIPS, a HIPS is installed on an endpoint (such as a PC) and looks at inbound and outbound traffic from that machine only. It works best in combination with a NIPS, as it serves as a last line of defense for threats that have made it past the NIPS.
* Network behavior analysis (NBA): This analyzes network traffic to detect unusual traffic flows, such as DDoS (Distributed Denial of Service) attacks.
* Wireless intrusion prevention system (WIPS): This type of IPS simply scans a Wi-Fi network for unauthorized access and kicks unauthorized devices off the network.

<https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html>

**Sandboxing**

Sandboxing is a cybersecurity practice in which code is run, observed, and analyzed in a safe, isolated network environment that mimics end-user operating environments. Sandboxing is used to inspect untested or untrusted code and is intended to prevent threats from entering the network. Sandboxing confines the code to a test environment, preventing it from infecting or damaging the host machine or operating system.

As the name implies, this isolated test environment serves as a kind of "sandbox," in which you can experiment with various variables to see how the program works. This is also a secure environment in which anything that goes wrong cannot actively harm your host devices.

## **The Benefits of Sandboxing**

## **Using a sandbox has a number of advantages:**

* **Does not risk your host devices or operating systems.** The main advantage of sandboxing is that it prevents your host devices and operating systems from being exposed to potential threats.
* **Evaluate potentially malicious software for threats.** If you’re working with new vendors or untrusted software sources, you can test new software for threats before implementing it.
* **Test software changes before they go live.** If you’re developing new code, you can use sandboxing to evaluate it for potential vulnerabilities before it goes live.
* **Quarantine zero-day threats.** With sandboxing, you can [quarantine and eliminate zero-day threats](https://www.checkpoint.com/solutions/zero-day-protection/).

<https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/#:~:text=Sandboxing%20is%20a%20cybersecurity%20practice,inspect%20untested%20or%20untrusted%20code>.

**Hyperscale Network Security**

The ability of a technology architecture to improve and scale appropriately as more demand is added to the system is referred to as hyperscale. This includes the ability to provide and add additional resources to the system that comprise a larger distributed computing network. Hyperscale is also essential for building a robust and scalable distributed system. Furthermore, it is the integration of an infrastructure's virtualization, storage, and compute layers into a single solution architecture.

## **Hyperscale Benefits**

Hyperscale offers the best way to realize a specific business goal like big data analytics projects and cloud computing systems. The main reason why an organization might decide to adopt hyperscale computing is that many hyperscale solutions are delivering the most cost-effective approach to a demanding set of requirements. For example, a big data project might be most proficiently addressed through computing density available in hyperscale. Rapid deployment and automated management capabilities make scaling out simple and hassle free for businesses of all sizes. By tightly integrating networking and compute resources in a software-defined system, we can fully utilize all hardware resources available to us. By orchestrating your resources in an innovative way, you get much more from what you already have. It is taking what you have and giving it superpowers combined with the ability to grow on demand.

## Hyperscale Concepts

Unlike a traditional large data center architecture, hyperscale data centers are built on three important and unique concepts:

* A highly responsive and cost-effective IT infrastructure, along with distributed systems to reduce complexities and improve business operations
* Scalability to stay in line with fast changing demand for computing projects
* Security, agility and lower software/hardware costs to guarantee appropriate revenue

Implementing hyperscale computing solutions gives its users the benefit of an exceptionally low-cost investment as a system with low configuration that runs a base level of virtual machines in a chosen and private system. In addition, hyperscale computing architecture works productively in large-scale usage, where thousands of virtual machines are being used.

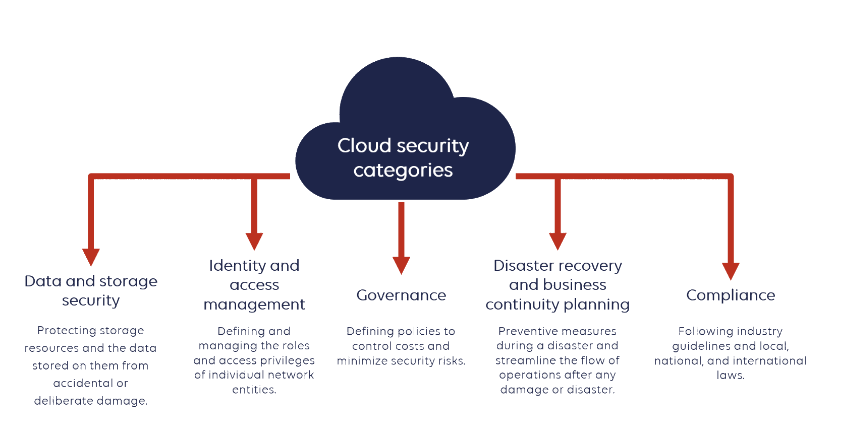
Check Point introduced [Check Point Maestro](https://blog.checkpoint.com/2019/01/22/introducing-maestro-the-industrys-first-hyperscale-network-security-solution/) to the market, the industry’s first truly Hyperscale network security solution. Check Point Maestro is a [revolutionary new architecture](https://www.checkpoint.com/downloads/products/maestro-hyperscale-network-security-infographic.pdf) that enables businesses of any size to enjoy the power of flexible cloud-level security platforms, and to seamlessly expand their existing security gateways to Hyperscale capacity.

https://www.checkpoint.com/cyber-hub/network-security/what-is-hyperscale/

**Cloud Security**

## **What is meant by cloud security?** Cloud security is a network security discipline dedicated to protecting cloud computing systems. This includes maintaining data privacy and security on online-based infrastructure, applications, and platforms. Protecting these systems involves the efforts of cloud providers and the customers who use them, whether they are used by individuals, small and medium businesses, or enterprises.

### **Cloud security can be divided into the following categories:**



## **Private cloud security**

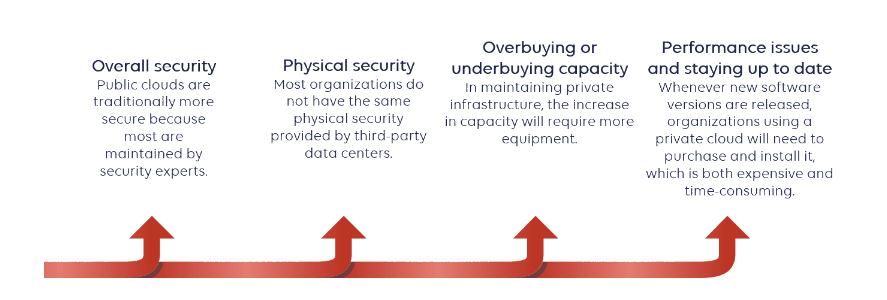
### **Advantages:**

* Security - your data and applications remain behind your firewall and are accessible only to your enterprise, making private clouds better suited to processing or storing sensitive data.
* Fully enforced compliance
* private cloud customers aren’t forced to rely on the industry and regulatory compliance offered by the cloud service provider.
* Greater visibility into security and access control - because all workloads run behind the customers’ own firewall.
* Flexibility in using hybrid cloud - ability to move non-sensitive data to a public cloud to accommodate sudden bursts of demand on your private cloud.

### **Disadvantages:**

* Higher costs at the start - increased initial charges and the need to repay the costs of the equipment you purchase.
* Responsibility - for operating and maintaining your own data center, IT hardware, and enterprise software as well as your own security and compliance.
* Less flexibility - in scaling IT resources up or down as your needs change.

**Private Cloud Security Risks:**

****

### **Overall security**

Many organizations believe that their sensitive data is more secure in a private cloud. However, the reality is that public clouds are traditionally more secure because most are maintained by security experts who understand cloud security challenges and how to mitigate them. To satisfy customers, reputable public cloud providers usually spend more time on this field than any single organization to obtain this level of reliability and security.

### **Physical security**

Most organizations do not have the same physical security (cameras, fire protection, security guards) provided by third-party data centers, which may make their data vulnerable to various threats. Many public providers also provide geographically redundant data centers, which means they have facilities throughout the state or the country.

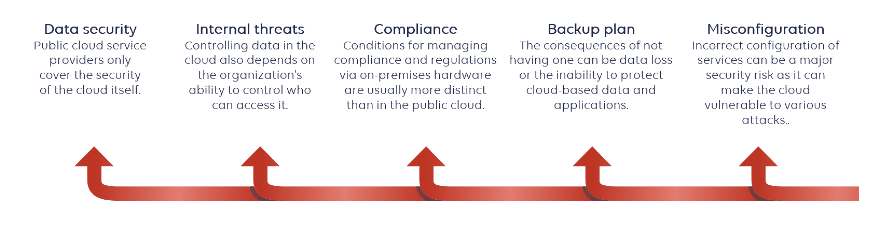
### **Overbuying or underbuying capacity**

The private cloud infrastructure is not the "cloud" as we know it. The true definition of the cloud is that it is elastic and scalable. In maintaining private infrastructure, the increase in capacity will require more equipment. If you don't buy enough capacity and your application traffic becomes too large, it could make your application very slow to load or bring it down and offline.

### **Performance issues and staying up to date**

Whenever new software versions are released, organizations using a private cloud will need to purchase and install it, which is both expensive and time-consuming. Some may continue to run on outdated software, which could then expose them to vulnerabilities. This can lead to downtime and also affects performance.

## **Public cloud security challenges and risks:**



### **Data security** Most companies that use the cloud initially believe that protecting their data is the responsibility of their cloud provider. However, this is not the case. **Cloud service providers only cover the security of the cloud** itself but do not protect customer data or the use of its infrastructure and applications by customers.

Companies are faced with the need to be responsible for their data security in the cloud, and possibly customer data security too.

### **Internal threats** Controlling data in the cloud also depends on the organization's ability to control who can access it. Most threats to data hosted in the cloud come from compromised internal accounts.

Your trusted employees, business partners, and contractors may be some of your potential security risks.

### **Compliance** Conditions for managing compliance and regulations via on-premises hardware are usually more distinct than in the public cloud. It requires a considerable amount of time to create a compliant environment. A company usually needs to hire a team or use a service that can help with compliance and regulations.

### **Backup plan** The backup plan is supposed to complement the data plan by providing security and integrity. The consequences of not having one can be data loss or the inability to protect cloud-based data and applications.

Make sure that your cloud provider offers adequate security controls, and that their backup plan is adequate.

**Services interruptions** Hardware and network problems happen. Even in high availability environments, sporadically you may encounter an interruption in the contracted cloud services.

Server failures, human errors, intrusions, or hardware/software updates can always cause collateral damage.

### **Misconfiguration** Incorrect configuration of services can be a major security risk as it can make the cloud vulnerable to various attacks. This can cause data to be publicly exposed, manipulated, or even deleted.

//https://www.stormit.cloud/blog/private-cloud-security-vs-public-cloud-security/

**Hybrid**

**What exactly is hybrid cloud security?**

Software-defined networking (SDN), virtualization, and application support at all layers of the service mesh across multiple data centers and hardware devices are all part of hybrid cloud security. Companies are increasingly looking for "single pane of glass" administration for hybrid cloud networking, which combines traditional network administration and data center management software with improved real-time data packet analytics. Hybrid cloud security must operate at all network levels and include support for new, innovative software platforms that have not been thoroughly tested in production.

**Hybrid cloud security issues and challenges**

Many senior business executives believe that the social engineering risk outweighs public cloud platform benefits and still will not sign off on transferring their most critical or sensitive data and business processes to a remote host. As the social engineering risk cannot be resolved, private cloud and on-premises data center facilities need to be managed increasingly in simultaneous integration with multiple public cloud resources and SaaS products in hybrid cloud constructs.

## **Hybrid cloud security best practice**

## Best practices in hybrid cloud security implement a multi-tiered approach to protection based upon interwoven security information and event management (SIEM) products within the service mesh. Modular hybrid cloud security systems operate at the hypervisor, operating system, web server, database, and application layers with network diagnostics based on real-time scanning, monitoring, and analysis of data packets through web traffic or other I/O transfer requests. Hybrid cloud solutions are orchestrated primarily through software platforms based on either hypervisor virtualization, container virtualization, or a combination of both.

## **Hybrid cloud security architecture**

## Hybrid cloud security begins with physical access to the web servers which house data in the form of proprietary code, databases, storage files, records, archives, or other resources. Since, by definition, the hardware available in hybrid cloud architecture is distributed globally across multiple data centers, IT administrators are forced to adopt a “zero trust” policy towards all vendors. Encryption is the primary method that security researchers adopt to keep data safe in a “zero trust” environment such as that provided in hybrid cloud architecture. Encryption strategies need to be applied at every level of the service mesh to be all inclusive. This includes the encryption of OS and software code at the web server or “bare metal” levels, as well as data in transmission, remote storage, backend processes, etc. in order to build secure hybrid cloud models on vendor-agnostic hardware. [VMware vSAN](https://www.vmware.com/products/vsan.html) Datastore is used for enterprise database encryption, while VMcrypt Encryption is applied to cloud storage resources, backups, and archives.

https://www.vmware.com/topics/glossary/content/hybrid-cloud-security.html