Data Center Security Best Practices

In the past, data centers (/cyber-hub/cyber-security/what-is-data-center/) were primarily composed of physical appliances deployed on-premises. The modern data center is a hybrid, combining on-premises systems with cloud-based infrastructure spread over multiple public and private clouds. These hybrid data centers include orchestration between the platforms that allows sharing of applications and data between the on-prem and cloud-based infrastructure. Following a data center security best practice plan will ensure their operations, applications and data are safe from threats.

Hybrid Data Center Security Best Practices

While data center security is a mix of physical security and cybersecurity, here we focus on the cybersecurity aspects of data center security. For more information about the physical security of data centers, check out our data center certifications (/cyber-hub/cyber-security/what-is-data-center/data-center-certifications/) page.

Hybrid data centers require security that is consistently applied and enforced across on-premises and cloud environments. The rapid pace of business evolution also mandates solutions that scale with the company and align with business goals.

Effective hybrid data center security provides deep visibility across environments and enforcement of zero trust security principles. Securing hybrid data centers requires following several security best practices.

#1. Identify and Control Data

When transitioning to an as-a-service model, an organization is giving up control over some parts of their infrastructure. The cloud provider may have control over the platform, operating, systems, etc. and does not provide visibility or access to these resources.

When designing security for the cloud, it is all about the data. Organizations need to develop strategies for maintaining control over their data within the constraints of the cloud service provider.

As you begin the assessment phase, ensure plans are in place for maintaining control of the data. On-prem this means designing redundancy into the plan. Have resilient, redundant systems and backup or disaster recovery plans in place. For cloud providers (/cyber-hub/cloud-

security/what-is-cloud-security/what-are-cloud-service-providers/), this means reviewing their SLAs to ensure they have what the customer expects in terms of availability (99.9999x) and access.

#2. Classify Sensitive Data

When moving to the cloud, organizations need to know what data is sensitive. This helps with designing protections for this data and ensuring that it is protected in compliance with applicable regulations.

All data should be labeled based upon its sensitivity, the type of data it is, and the business unit that owns that data. This labeling informs regulatory compliance policies and ensures that data important to certain business units meets accessibility and availability SLAs.

#3. Map Data Flows

In a hybrid data center, data will regularly flow between on-prem and cloud environments. Securing this data requires insight into these data flows so that legitimate data flows are permitted and suspicious or malicious ones are blocked.

When mapping data flows, it is important to include users, networks, systems, and applications in the map. This provides important context when implementing and enforcing granular access controls.

#4. Define Groups

Attempting to define and enforce security policies on an individual, case-by-case basis is unscalable and ineffective. A better approach is to define groups of entities that serve similar purposes and define and enforce policies on these groups.

Effective group management requires clear, consistent policies. Define systems that can be used to map which group the users, devices, VMs, and applications belong to so that the groups can then be dynamically used in policy.

#5. Segment Traffic Flows with a Scalable Security Solution

Network segmentation (/cyber-hub/network-security/what-is-network-segmentation/) is the foundation of effective network security. With segmentation, an organization can define boundaries where traffic is inspected and security policies are enforced.

When performing network segmentation in a hybrid data center, scalability and flexibility are essential. A network segmentation solution must offer support for dynamic scalability. This ensures that on-premises and cloud systems can expand and decrease natively with the ebb and flow of the business.

Network segmentation solutions should also be designed to address the unique use cases of the cloud. For example, companies are increasingly embracing serverless solutions, so hybrid data center security solutions should have support for serverless security (/cyber-hub/cloud-security/what-is-serverless-security/). This enables organizations to gain the visibility and control that they need to properly segment and secure serverless applications.

#6. Create Dynamic Access Control Policies

An organization's infrastructure can change rapidly in the cloud, and security needs to be able to deal with it. This means that a hybrid data center requires dynamic access control policies.

A cloud security solution (/solutions/cloud-security/) should be able to collect and analyze data from across the entire ecosystem – including on-prem and both public and private cloud environments – to gain necessary security context and ensure consistent security enforcement. As these environments change and evolve, security policies should change with them to provide optimal, up-to-date protection and policy enforcement.

#7. Perform Periodic Audits and Reviews

Misconfigured security settings are some of the most common causes of cloud security incidents. The wide array of cloud-based services that companies use – each with their own unique security settings – means that cloud deployments are often improperly secured.

As cloud deployments become a growing part of corporate IT infrastructure, cloud security posture management (CSPM) (/cyber-hub/cloud-security/what-is-cspm-cloud-security-posture-management/) solutions are essential to securing hybrid data centers. A CSPM solution should offer unified security management across multi-cloud environments and provide security teams with the centralized visibility and management required to respond quickly and effectively to potential security incidents.

#8. Integrate DevSecOps

DevSecOps (/cyber-hub/cloud-security/what-is-devsecops/) is intended to integrate security into modern development processes. This includes automating processes like vulnerability scanning and security policy updates as part of continuous integration and deployment (CI/CD) processes.

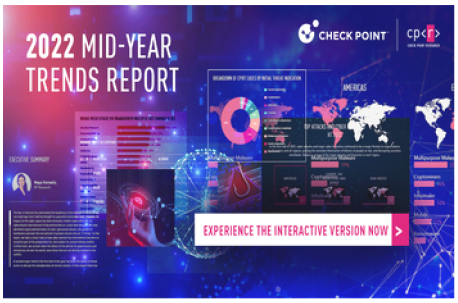
With hybrid data centers, companies can take advantage of the speed and agility of the cloud. Doing so securely requires integrating security into development and infrastructure management processes.

Implement Hybrid Data Center Security

As organizations transition to using more cloud-based services, security is a vital consideration. When implementing cloud-based infrastructure, companies require a hyperscale security solution that can scale with the business.

Check Point Maestro (/products/maestro-hyperscale-network-security/) is a hyperscale network security solution built to address the needs and challenges of cloud security. To learn more about Maestro's capabilities, check out this whitepaper (https://pages.checkpoint.com/maestro-esg-whitepaper.html). You're also welcome to request a demo (https://pages.checkpoint.com/maestro-hyperscale-network-security-demo.html) of Maestro's hyperscale network security and request for a demo (/demos/#cloud) of cloud workload protections.

Recommended Resources



Cyber-Attacks Trends: 2023 Mid-Year

https://pages.checkpoint.com/2023-mid-year-cyber-security-report.html?utm_term=cyber-hub&utm_content=td)

Security CheckUp

(https://pages.checkpoint.com/security-checkup.html?utm_term=cyber-hub&utm_content=td)

Cyber Security Report 2023

(https://pages.checkpoint.com/cyb security-report-2023.html?utm_term=cyber-hub&utm_content=td)

Get Started

Cloud Security (/cloudguard/)

Workload Protection (/cloudguard/workload-protection/)

DevSecOps (/cyber-hub/cloud-security/what-is-devsecops/)

Related Topics

Data Center Architecture (/cyber-hub/cyber-security/what-is-data-center/data-center-architecture/)

Data Center vs Cloud (/cyber-hub/cyber-security/what-is-data-center/data-center-vs-cloud/)

Data Center Management (/cyber-hub/cyber-security/what-is-data-center/data-center-management/)

Data Center Security (/cyber-hub/cyber-security/what-is-data-center/what-is-data-center-security/)