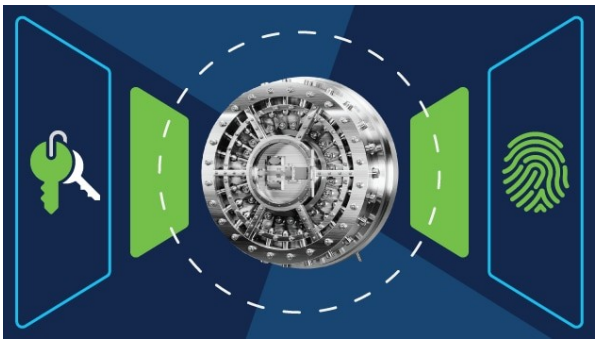
What Is Data Center Security?



Data center security is the practice of applying security controls to the data center. The goal is to protect it from threats that could compromise the confidentiality, integrity, or availability of business information assets or intellectual property.

At its simplest, a data center is a physical facility that organizations use to house their critical applications and data. A data center's design is based on a network of computing and storage resources that enable the delivery of shared applications and data. The key components of a data center design include routers, switches, firewalls, storage systems, servers, and application-delivery controllers.

Data center security follows the workload across physical data centers and multicloud environments to protect applications, infrastructure, data, and users. The practice applies from traditional data centers based on physical servers to more modern data centers based on virtualized servers. It also applies to data centers in the public cloud.

Data centers contain the majority of information assets and intellectual property. These are the primary focus of all targeted attacks, and therefore require a high level of security. Data centers contain hundreds to thousands of physical and virtual servers that are segmented by application type, data classification zone, and other methods. Creating and managing proper security rules to control access to (north/ south) and between (east/west) resources can be exceptionally difficult.

Three critical needs in data center security

Visibility

When securing the data center, there needs to be visibility of users, devices, networks, applications, workloads, and processes. Visibility makes it easier to detect performance bottlenecks, which informs capacity planning. It can speed attack-detection and make it easier to identify malicious insiders who are attempting to steal sensitive data or disrupt operations.

Visibility also improves post-incident response times and forensics, which can uncover the extent to which critical systems were breached and determine what information was stolen.

Segmentation

Segmentation reduces the scope of an attack by limiting its ability to spread through the data center from one resource to another. For servers on delayed patch cycles, segmentation is an important tool. It reduces the possibility that a vulnerability will be exploited before adequate patch qualification and deployment into production is complete.

For legacy systemsworkload, segmentation is critical to protect resources that don't receive maintenance releases or patch updates.

Many attacks focus on having direct access to a system to compromise it through application vulnerabilities, unsecured ports, or denial-of-service (DoS) attacks. DoS attacks crash the system and allow the attacker to gain admin control and install malicious code to continue the breach. If the hacker can't gain access to a high-value asset in the data center, many attacks can be prevented rather than continue until detection or system compromise.

For some industries, like utilities, advanced persistent threats are a way of life. It is almost impossible to defend against this type of attack 100 percent of the time, but segmentation is a valuable tool to slow down the hacker and give security teams time to identify the problem, limit exposure, and respond to the attack.

Threat protection

All data centers need to protect their applications and data from an increasing number of sophisticated threats and global attacks. All organizations are under threat of attack, and many have been breached but are unaware of it.
Protecting the modern data center is a challenge for security teams. Workloads are constantly moving across physical data centers and multicloud environments. That's why the underlying security policies must dynamically change to help enable real-time policy enforcement and security orchestration that follows the workload everywhere. In a data center with multiple customers, such as a public cloud environment, one customer may attempt to compromise another's server to steal proprietary information or tamper with records.

Mobile and web applications can strengthen customer loyalty, but they increase the attack surface and create another avenue for exploitation. Employees may unwittingly compromise the business and contribute to a data breach. Hackers often begin by gaining access to an employee's authentication credentials. They do this by infecting an endpoint device with malware or using phishing or other social engineering techniques to trick users into supplying their credentials. The hacker can now gain "authorized" access to a server or servers within the data center, access more user accounts, and continue toward the target server where the data theft occurs.

You can mitigate the business disruption and impact from a breach by deploying comprehensive, integrated security products that work together in an automated process. This streamlines threat protection, detection, and mitigation.

Data center tiers and levels of security

ANSI/TIA-942 defines data center standards and breaks them into four tiers based on level of complexity. More complex data centers require increased redundancy and fault tolerance. Ensuring the integrity of the data center is a form of security, and the more complex data centers in the higher tiers have more security requirements.

Tier 1: Basic site infrastructure
Provides limited protection from physical events. Consists of single-capacity components and a single, nonredundant distribution path.

Tier 2: Redundant-capacity component site infrastructure

Offers better protection from physical events. Includes redundant capacity components and, like Tier 1, a single, nonredundant distribution path.

Tier 3: Concurrently maintainable site infrastructure

Protects from almost all physical events. Includes redundant-capacity components and various independent distribution paths. All components can be removed or replaced without disrupting end-user services.

Tier 4: Fault-tolerant site infrastructure

Provides the top level of fault tolerance and redundancy. Contains redundant-capacity components and various independent distribution paths that enable concurrent maintainability. One fault in the installation will not cause downtime.