
ZONES™

Data center security

The threat landscape that affects your network constantly evolves and changes. With public cloud, private cloud, and hybrid cloud creating an intersection of physical and virtual infrastructure, there is an expanding set of elements for data center administrators to consider. On top of that, cyberattacks are becoming increasingly sophisticated.

Quality data center security is an essential defense against denial of service attacks and data breaches.

The worst time to consider your data center's security is after a breach or data loss has taken place. Depending on your regulatory environment, this might mean serious consequences, hefty fines, or a serious impact on your operations and profit margin.

To stay ahead of threats and keep your data center protected, it's essential that you regularly evaluate and update the security infrastructure that you have in place to protect your data center. When is the last time that you revisited your data center security? Consider both the physical and the virtual protections that you have in place.

The most essential considerations for data center security are the virtual and physical security you have in place around your servers – as well as how carefully you create physical and logical separation in your data center access.

Your security policies create the essential division between physical and logical data center access. At no point should people with logical access and administrator control have physical access to your servers; and anyone with physical server access should have no administrator rights. In smaller companies, this may present challenges. Cloud infrastructure helps ensure the separation of administrators and physical server access; in hybrid environments and with on-premises data centers, strict security policies should be created and enforced.

Intelligent facilities: IoT and data center protection

The Internet of Things (IoT) also has great applications for data center security.

A major trend with the IoT is intelligent facilities. Sensors, triggers, and location tracking of people and equipment are some of the most replicable aspects of IoT. Using an IoT solution in your data center can help you provide leading physical security.

Cloud providers: Advantages for data center security

Cloud providers have to create rigorous security in order to offer their customers a cloud platform consistent with regulatory requirements across industries. Select a cloud provider after reviewing their internal security management standards – the security controls and best practices that they have in place internally to ensure comprehensive security control. Industry standards, such as the ISO 27001 certification, demonstrate that a cloud provider has passed third-party audits to ensure that they maintain and manage rigorous security controls.

Where is the threat originating? The role of next-generation firewalls

Firewalls are physical or virtual appliances that protect your data center – and they exist on the network, server, or web application level. They help mitigate inbound attacks and create additional authentication and access control capabilities; as well as allowing you to monitor and discover workloads to ensure security policy compliance.

If you have expanded your workloads and web-application hosting in the cloud, you may want to consider a web application-level firewall, which blocks attacks that originate within cloud hosted web-applications and helps fill gaps in cloud infrastructure security.

In the event of an application-based breach, your cloud provider will shut down your servers as part of their overall security protocol. These same protections secure your data if a threat arises from another organization using the same cloud platform; although useful, if you are the source of a breach, you could face downtime or disrupted operations on your end. Placing web-application level firewalls helps you ensure business continuity as you expand into the cloud.

If you are interested in a review and assessment of your data center security, contact your Zones account executive or call 800.408.ZONES.