Modern Data Centers Need a New Approach to Security

Virtualization, cloud, and Software-Defined Networking (SDN) are changing the scope and function of the modern data center. Workloads are dynamic and constantly moving across multi-cloud and physical data centers. DevOps teams are utilizing Continuous Integration and Continuous Deployment (CICD), rolling out new applications and services quickly to keep up with the rapid speed of business. New technologies like microservices, containers, and APIs, are transforming the design of applications.

There is a huge influx of data from big data analytics and new types of applications. Employees, contractors, business partners, and customers are interacting with resources in the data center in an ever-expanding way. This boosts the value of the data center, but alternatively can increase data theft opportunities.

Data center teams must now rethink their approach to security. The IT organization is overwhelmed, spending 76 percent of its attention focused on securing the data center[1].

The answer is an integrated security architecture, with best-in-class products that together address three critical needs of the data center.

Visibility

See everything with complete visibility of users, devices, networks, applications, workloads, and processes.

With complete visibility, you can better detect performance bottlenecks and improve capacity planning. It makes it easier to identify malicious insiders attempting to steal sensitive data or disrupt operations. You can also speed attack-detection and post-incident response time and forensics. This helps you determine if and to what extent critical systems were breached and what information was stolen.

The Cisco® approach gives customers far greater insight into workloads and application behavior. It helps you identify who users are, where they are connecting from, and what hosts and application resources they are accessing. We make it easier for you quickly discover hard-to-see threats with security analytics that analyze network flows for malicious network activity.

Segmentation

Reduce the attack surface by preventing attackers from moving laterally within the data center with consistent security policy enforcement, application allow-listing, and microsegmentation.

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, reducing the potential for vulnerability exploitation until adequate patch qualification and deployment into production is complete. For legacy systems, 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. The 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 a number of industries, like utilities, advanced persistent threats are a way of life. This type of attack is almost impossible to keep out 100 percent of the time. Segmentation is a valuable tool to slow down the hacker and provide security team's time to identify the problem, limit the exposure, and respond to the attack.

Segmentation plays an important role in audit and compliance scenarios. For industry requirements such as the Payment Card Industry Data Security Standard (PCI DSS) and regulations like the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA), segmentation can be used to help reduce the number of systems that require controls, as well as the scope of an audit.

Cisco provides multilayer segmentation. We help you consolidate policies and automate the enforcement at the perimeter, on the data-center fabric, on the host, and even in the application process.

[1] Cisco Annual Cybersecurity Report

Threat Protection

Stop the breach by deploying multilayered threat sensors strategically in the data center. They can quickly and dynamically detect, block, and respond to threats, preventing hackers from stealing data or disrupting operations.

All data centers have something in common: the need to protect their applications and data from an increasing number of sophisticated threats and global attacks. All organizations are under threat of attack; 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 multi-cloud 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 in order to steal proprietary information or tamper with records.

The attack surface has increased with the use of mobile and web applications, which can strengthen customer loyalty but create another avenue for exploitation. Employees may unwillingly 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 a phishing attack or other social engineering technique 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 towards the target server where the data theft occurs.

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

Cisco customers can deploy threat sensors strategically across north-south and east-west traffic flows to quickly detect, block, and respond to attacks before hackers can steal data or disrupt operations. We can see applications, operating systems, virtual machine communications, and network devices. At the same time, we can detect the latest and most advanced forms of malware backed by Cisco Talos™, the industry-leading threat intelligence team.

Why Cisco?

Cisco helps data center teams consistently protect the workload everywhere through complete visibility and comprehensive multilayered segmentation. Our solutions provide integrated threat protection capabilities that keep your business more secure and your data center team more productive.

For more information on Cisco's data center security capabilities, visit us at: https://www.cisco.com/go/securedc

C96-740102-00 07/20