illumio

Best Practices to Contain Cyberattacks

The damaging cyberattacks of the last few years have given business leaders reason to pause and rethink their IT security strategies. In its first *State of Dynamic Data Center and Cloud Security in the Modern Enterprise* survey and research report, the SANS Institute identified a shift to a new normal for enterprise security—one that involves redefining how to contain and handle attacks. Here, we outline seven best practices IT and security professionals must take to gain control over the enterprise security posture in their dynamic data centers and to contain attacks immediately when they do occur.

Gain full visibility inside your data center and cloud

58 percent of enterprises have no visibility into the East-West traffic inside their data center or cloud environments—or don't know if they do.

Given the constantly changing nature of computing in today's data centers—where application workloads are dynamically instantiated, migrated, and decommissioned—full visibility into all applications and interactions behind the perimeter is a prerequisite to setting up the right policies and monitoring compliance.

Substantially reduce your attack surface

More than 75 percent of enterprises rely only on traditional perimeter security, leaving East-West connections—inside the data center—unsecured.

When a malicious actor gets past a perimeter, it is difficult to prevent the attack from spreading. Many enterprises extend chokepoint security by using network firewalls inside the data centers, but this strategy results in more management for only a small reduction in attack surface. A better approach to substantially reducing the attack surface is to microsegment applications and enforce policies at the most granular location—individual application workloads.

Implement a network-neutral security strategy

Most security policies rely on network-dependent polices to control access to high-value assets inside data centers and clouds like VLANs, subnets, IP addresses, and zones.

This results in policies that are not portable between environments and need constant manual modifications when application workloads move or change. A network-neutral security strategy eliminates this static, point-in-time approach with policies that rely on application behavior—not network settings.

Adapt automatically to application changes

More than 1/3 of the enterprises said it takes more than two weeks to implement security changes.

Manual adjustments to policies in response to application changes are slowing down businesses and causing errors. Many large enterprises with distributed and hybrid computing environments are opting for adaptive approaches to policy management where security is automatically and continuously computed using up-to-date application state information collected from every compute instance.

Automate encryption of application traffic

In distributed environments, data may travel over untrusted networks as application workloads communicate.

Encryption of data in motion is necessary to prevent compromises or loss of sensitive data. IPsec offers convenient network layer encryption of all application traffic. But, traditionally IPsec has required specialized hardware and software and configurations on both ends of the encrypted communications. Consider IPsec implementations that can be baked into security policies to automate encryption of traffic between specific tiers of applications.

Contain first, ask questions later

Traditional detection and response strategies to cyberattacks do not identify system compromises in time, allowing the attacker to spread laterally inside the data center.

To handle today's advanced attacks, enterprises must adopt a "contain first" strategy to ensure that any suspicious activity inside the data center or cloud is immediately stopped in its tracks, giving security teams time to research and remediate.

Fuse security into DevOps practices

Of SANS survey respondents who were compromised, 50 percent blame the exploits of app vulnerabilities.

Outdated security policies and manual errors are a significant source of vulnerabilities. Security must mirror the speed of application development to keep up with the rapid change and movements of applications and their environment in dynamic data centers and clouds. Building in application security through API-driven integration with DevOps tools, and enabling enforcement rules to adapt automatically, in concert with applications, minimizes the possibility of attacks that exploit application vulnerabilities.

ABOUT ILLUMIO

Illumio delivers *adaptive security* for every computing environment, protecting the 80 percent of data center and cloud traffic missed by the perimeter. The company's Adaptive Security Platform™ visualizes application traffic and delivers continuous, scalable, and dynamic policy and enforcement to every bare-metal server, VM, and container in data centers and public clouds. Using Illumio, enterprises such as Morgan Stanley, Plantronics, NTT, and Creative Artists Agency have achieved secure application and cloud migration, environmental segmentation, high-value application protection from breaches and threats, and compliance with no changes to applications or infrastructure. For more information, visit www.illumio.com or follow us on Twitter @Illumio.