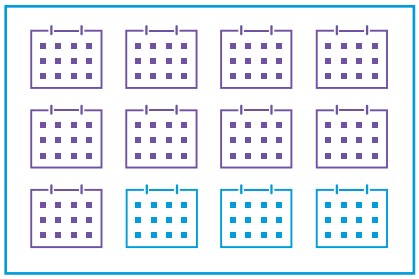
Lateral Security is the New Cybersecurity Battleground



277 days

The average time to detect and contain a breach inside the network[1]

It's time to face the stark reality that the bad guys are likely already inside the network. While perimeter and endpoint cyber defenses are essential, advanced threats still can find a way in. With expanding attack surfaces and new vulnerabilities being reported faster than organizations can patch them, even well-resourced security teams and practices can be compromised. We need look no further than recent breaches that leveraged compromised software supply chains or popular open-source software to serve as cautionary tales.

What is the lateral movement?

An initial breach into the network often is not the intended target. After the initial compromise through stolen credentials or hacked endpoints, attackers then can move laterally through the network to more valuable targets.

Once attackers get inside, they aim to stay in, remain undetected and continue to "live off the land". The average time to detect and contain a breach inside the network is 277 days (207 to detect and another 70 to contain)[1]. According to VMware Contexa data, 44% of intrusions move from the initial attack laterally throughout the data center, looking for more valuable assets to ransom or exfiltrate. Once an attacker breaches the network, and is using lateral movement inside the network, also called "east-west" traffic, they often have an easier time as perimeter-based security controls are ineffective in stopping them.

1. IBM Security, Cost of a Data Breach Report, 2022.

You can't stop what you can't see

Existing network controls can't see what they are missing. Deployed at the network edge, in-line or with a span tap, these controls can't effectively inspect virtualized network traffic that never touches the physical network.

Protecting the inner workings of applications

So how can we find and evict these threat actors — even those using trusted ports and protocols — before they do serious damage? The first step is to have a baseline understanding of the inner workings of all applications. This requires deep visibility into the applications, flows, related services, connections and data patterns. Adding even more complexity is the need to have this visibility for both traditional applications that are predominantly virtualized and for modern applications that are largely containerized.

Micro-segmentation can be effective for stopping obviously malicious traffic by establishing security barriers to stop attackers from traversing across defined network segments within the data center. However, attackers are stealthy and have evolved their techniques to exploit trusted processes, protocols and software modules to move laterally. These movements often look like legitimate traffic, taking advantage of common services, such as Samba, RDP and PowerShell or use passwords captured over the network (pass the hash). Without additional context and applied threat intelligence, it is hard to distinguish between friend and foe.

You can't stop what you can't see

To detect threats in a virtualized data center, environments where the virtual machine (VM) to VM traffic may not traverse the physical network, security controls must include deep visibility. Traditional appliance-based firewalls rely on network taps, being in-line or hair-pinning the traffic. They are impractical to implement within virtualized networks because they require disruptive changes to the network configuration. Additionally, the data collected can be incomplete. Traditional appliance-based network taps are limited to only data that traverse the physical network, missing the intra-host VM to VM traffic entirely. With today's high-performance servers that can run hundreds of VMs, this leaves many blind spots that bad actors can use to move laterally unchecked.

With VMware, see all connections and conversations

Where physical network-based security and visibility controls are blind to virtualized network traffic, the virtualization layer itself becomes the security professional's best tool.

VMware NSX® security is instrumented in the virtualization layer and uses distributed advanced intrusion detection and prevention (IDS/IPS), along with network traffic analysis (NTA) for deep visibility into application environments. This enables users to see and understand what is happening on all connections, including the process that initiated the traffic, even if it is encrypted. It is the industry's only full emulation network sandbox that uses baseline context to distinguish anomalies — identifying friend from foe — even on trusted systems and protocols. These capabilities are delivered as an advanced threat software solution. This is the first and only solution to get the AAA rating from SE Labs for network detection and response.

VMware NSX security detects the threat and evicts the attacker from the network. Learn more

Let's get started

Stop malicious lateral movement with strong distributed security that includes micro-segmentation and AI/ML-powered NDR for enterprise-wide visibility and consistent policy.

VMware NSX Distributed Firewall
Advanced Threat Prevention
Customer Case Studies

The same security needs and principles apply to modern applications and workloads; however, the insertion mechanisms are different. Modern application architectures include microservices and APIs and can have hundreds or even thousands of endpoints talking to each other. Like in a traditional virtualized environment, defending against laterally moving threats requires understanding and visibility of these services and their APIs. And, just like the hypervisor layer in virtualized environments, VMware offers visibility and controls for modern application environments. The VMware service mesh enables observation and analysis of APIs to understand their schemas, data flows and normal traffic baselines. If an attack is attempted, for example, an anomalous request for data, VMware NSX security detects the threat and evicts the attacker from the network.

Consistent security demands automation

The cloud radically changed how VMs and containers are instrumented. The "Cloud Operating Model" has provided push-button automation and efficiency to deploy new workloads and their supporting infrastructure, including switching, routing and load balancing. Security for both traditional and modern applications must be consistent with the cloud operating model.

VMware's cloud operating model integrates into existing automation processes — automating distributed firewalling (for segmentation and micro-segmentation), IDS/IPS, NDR, NTA and network sandboxing — for the optimal level of operational efficiency and consistent security.

Workloads are more secure on VMware clouds

VMware lateral security protections for multi-cloud environments provide a full suite of lateral security tools to help organizations achieve strong security against sophisticated threats. Only VMware sees every process running in an endpoint, every packet crossing the network, and every access point, as well as the inner workings of traditional and modern apps, to identify and stop threats others cannot.