APP SECURITY: FIRST LINE OF DEFENSE

A renewed security mindset and robust app security can ensure protection.

MATTHEW SCHNEIDER
SENIOR DIRECTOR OF GOVERNMENT, EDUCATION AND HEALTHCARE, VMWARE

IT'S NO LONGER safe to assume that applications, data, and traffic within the network perimeter are secure. Think of it like a building—even if you have guards at the front door, attackers will simply find a way in through a window or a back door.

The unfortunate reality of today's networks is we must assume our defenses have not kept the bad actors out and we are in fact compromised. Yet in most cases, government data centers weren't built to fully secure assets inside a data center from other inside applications. In fact, 70-80 percent of the traffic inside a typical data center today never touches a firewall.

So, how do you ensure that applications running within your network are secure? Before diving into technology, it's important to first change your mindset. Today's realities demand that agencies adopt the "zero trust" model. This means you have to assume your network has already been compromised and act accordingly.

Securing the data center from within usually involves starting with the applications themselves. Modern applications are no longer built to remain static. They are dynamic—constantly on the move within the data center, across data centers, in and out of clouds. With the growth of containers, this trend is only going to add complexity. This type of dynamic movement leaves a lot of potential "open windows" for hackers to exploit.

The first step in securing your applications is to know what you have, know if and how they're secured, and map out which applications communicate with other applications and users. The best way to do this is with a combination of automated, intelligent application discovery, and human interaction.

Start with your most critical applications. Observe how they behave and what they interact with for several days. Armed with that information, you can apply the most appropriate security rules and parameters. Instead of protecting applications based on IP addresses—a haphazard and volatile method at best—you can spell out in common language which applications have permission to talk to other applications and users. You can even specify ports and protocols.

Automating the process to the greatest extent possible helps boost security. If you can automate how you deploy new applications and define rule sets, policies, and configurations, you are removing a lot of potential human risk. Automation also helps network administrators quickly quarantine, segment, or remediate applications in high-alert situations instead of doing it manually.

Another important tactic to ensure application security is micro-segmentation. This breaks the data center into logical elements based on application and common language rules and manages them with automated security policies. It's a way to bring firewall, advanced security, and other traditionally perimeter-level defenses to the application level. Even if bad actors enter the network and try to move laterally through your applications, by employing micro-segmentation, you can be confident your applications will be protected.

Moving to a zero-trust model and focusing on security as close to the application layer as possible can go a long way toward improving cybersecurity. That's not enough on its own though. It's essential to change the entire mindset of how your cybersecurity defenses work and how you deploy them. Security is no longer a point-in-time or project-based initiative. Modern cybersecurity is a continuum. That means implementing security within the fabric of the data center in a way that helps your agency be reactive, dynamic, and proactive.

__Matthew Schneider__ is senior director of government, education and healthcare at VMware.

IN A CULTURE OF POSSIBILITY

SECURITY UNSHACKLES INNOVATION.

Learn how our customers are shaping the future.
vmware.com/possible

vmware®

REALIZE WHAT'S POSSIBLE.™