VMware on VMware: A Customer One Story

Industry

Cloud computing and enterprise networking

Location

Palo Alto, California

Goal

Eliminate the castle-and-moat approach to enterprise security by implementing Zero Trust everywhere

Key challenges

- Build and implement a comprehensive Zero Trust architecture that can protect the entire enterprise infrastructure.
- Endpoints are difficult to secure since they can be found in a variety of environments throughout the organization.
- All users—remote or on-site—must enjoy the same seamless yet secure experience

How VMware IT Built a Zero Trust Architecture to Protect the Entire Enterprise

VMware IT implemented Zero Trust to Successfully replace the legacy security architecture.

The traditional castle-and-moat approach was ideal for enterprise security. Its foundations were based around on-premises data centers and default trusted authorization. Now, many of the advantages these legacy systems used to offer are proving to be vulnerabilities in the cloud era thanks to remote workers, modern apps, a proliferation of mobile devices, and other factors.

Realizing this issue, VMware implemented Zero Trust architecture throughout the entire VMware ecosystem.

Zero Trust takes off—airport style

The VMware approach is to replace the castle-and-moat paradigm with one akin to an airport. When travelers arrive at an airport, the 'system' treats them as unauthenticated, unauthorized, and thus untrusted until proven otherwise. Similarly, Zero Trust architecture assumes every interaction—whether it's logging in, downloading a new app, accessing the system via a new device, or any similar scenario—is not to be trusted.

Zero Trust at VMware involves four teams—End-User Services, InfoSec, Networking, and Cloud Operations. Together, these teams can fully secure the entire VMware global ecosystem, including all aspects of clouds, networking, access, endpoints, and workloads. This is all accomplished via automation, orchestration, and all-new levels of visibility, and analytics.

Solution

VMware NSX®, VMware Carbon Black®, VMware Workspace ONE®, VMware Aria Automation™, VMware Aria Cost™ powered by CloudHealth®.

- Enable more efficient security measures and controls across multiple domains for better security posture.
- Allow for more agile security operations when it comes to a cloud operating model.
- Provide visibility and automation in current ecosystem state and configuration.
- Identify current risks and help detect and respond to future threats.

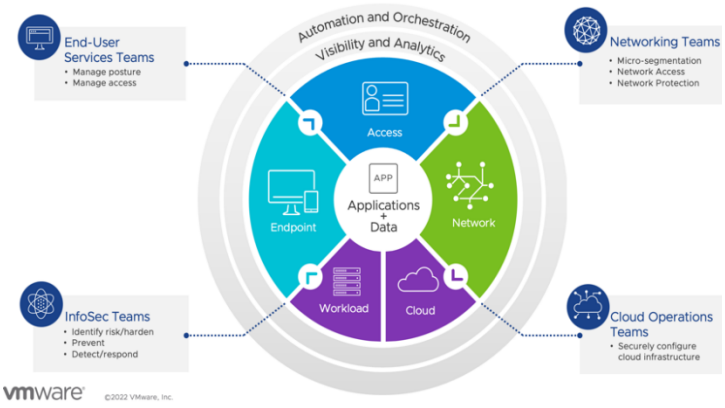

Figure 1. VMware IT comprehensive vision of Zero Trust.

The seven pillars of Zero Trust architecture

1. **Core network services (CNS)—**These are scaled out to include all ancillary services, micro-segmented by default, and are closely monitored by both humans and artificial intelligence. Examples include NSX security and secure cloud connections.
2. **Endpoints**—Manageable devices must be managed, yet unmanageable devices are denied access to core services. Multifactor authentication (MFA) is standard, and reliance on passwords is dramatically decreased if not eliminated altogether.
3. **Office networks**—Wi-Fi by default in order to ensure high transfer speeds and reliability. Ethernet ports are disabled, negating the need for laptop dongles. In addition, there is no longer a need for expensive network access control (NAC) administrative overhead.
4. **Internet-only access**—Remove 'default trusted' end-user-accessible networks and switch to location-based managed Wi-Fi internet access. Peer-to-peer connectivity is enabled, and endpoints now reside off the main network in trusted locations.
5. **VPN and network policies**—'Default trusted' paths to the network are removed. VPN are allowed, but the defaults are set to 'off.' There is an increased use of identity-defined policies for access. Users in high-risk countries (HRC) still maintain full-tunnel VPN security.
6. **Blast chambers**—These provide secure and contained network segments for R&D. Features include manageable, segmented network pod architecture and easy issue isolation. They also make it simple to significantly increase productivity without violating corporate policies.
7. **Admin VDI access**—Admin-level access for non-API-level activities is only available via virtual desktop infrastructure (VDI) sessions (Windows and Linux). Any CLI/UI-level admin tasks must be conducted via a VDI jump box. Overall, these stateless desktops substantially reduce threat actor risk.

Looking Ahead

Combined, these elements enable the various teams to deliver unprecedented experiences that are virtually transparent to the user. That means users are more productive than ever, without having to worry about passwords and other legacy security measures. Whatever the task, whatever device is used, wherever it's accessed, Zero Trust ensures the VMware ecosystem is always safe and secure.

VMware is also constantly looking at evolving beyond Zero Trust. Internally, there are over 40 major initiatives across many cross-functional teams that are shaping the future of zero trust to provide better agility and efficiency.

Learn more, schedule a briefing

To learn more, contact your sales representative or vmwonvmw@vmware.com to schedule a 1:1 Schedule a briefing on this topic with a VMware IT subject matter expert.

More information or purchase VMware products

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit vmware.com/products, or search online for an authorized reseller.

vmware®
ON VMWARE