WHITE PAPER–AUGUST 2021

Securing Workload Access as Part of an End-to-End Zero Trust Architecture

vmware®

Introduction

As enterprises accelerate digital transformation—adopting multi-cloud strategies, modernizing applications, and adapting to changing workforce models—the traditional trust boundaries using perimeter security have been obliterated and many are exposed to new security risks through larger, more complex attack surfaces. This creates friction and conflict between the teams tasked with innovation and those responsible for managing risk.

Which is why organizations are also accelerating their adoption of Zero Trust strategies, a security model based on the principle of "never trusting, always verifying" before allowing access to applications and resources. Removing the assumption of trust, limiting access, and authenticating based on identity and context creates a far more robust security posture that supports digital transformation instead of hindering it.

However, too often Zero Trust is associated only with securing user access to the enterprise network. Until now, enterprises haven't been as focused on the growing security risks and expanding attack surface resulting from applications and the workloads that constitute the applications, communicating with each other.

This white paper discusses the need for a Zero Trust approach that embraces securing workload access. You'll learn how VMware can help cloud and application security leaders, enterprise IT leaders, and security teams use Zero Trust principles to protect workloads running in private and public environments as part of a Zero Trust strategy.

Threats to modern workloads are on the rise

The move from monolithic applications to a highly distributed modern application architecture is creating enormous growth in number of workloads and communications within and across clouds. The predominant approach to modern application development is a microservices architecture, with each element of functionality developed as an independent service and running in its own process (typically in a container). Microservices communicate with other services upstream and downstream to deliver the business functionality needed within the distributed application.

Microservices adoption is rapidly growing. Almost one-third of organizations say they are migrating or implementing more than 50% of their systems using microservices. More than three-fifths (61%) of organizations have been using microservices for at least one year, with 28% using microservices for at least three years.[1]

The ensuing shift in traffic patterns has not gone unnoticed by cybercriminals, who have more recently taken their attacks to workloads. Attackers attempt to exploit security policy and control gaps to compromise applications and move laterally from one application environment to others.

The growing application attack surface is why Zero Trust is more important than ever—and why enterprises need to implement Zero Trust principles for more than securing user access to the network. To be effective and improve protection, Zero Trust must also encompass security for workloads.

1. "Microservices Adoption in 2020," O'Reilly, July 2020.

The three legs of a Zero Trust architecture

The National Institute of Standards and Technology (NIST) defines a Zero Trust architecture (ZTA) as "an enterprise cybersecurity architecture that is based on Zero Trust principles and designed to prevent data breaches and limit internal lateral movement."[2]

To improve protection across an increasingly complex application environment, enterprises need to take a Zero Trust approach to user and workload access and provide robust controls to the security team:

1. **Secure user access:** Applying Zero Trust principles to users accessing the enterprise network (or any service on the network). Zero Trust Network Access (ZTNA) helps organizations achieve this.
2. **Secure workload access:** Applying Zero Trust principles to applications and associated workloads and data (that may run in the private or public cloud).
3. **Security Operations Center (SOC) controls:** To operationalize a Zero Trust strategy, enterprises need a common set of core capabilities that support the entire ZTA environment. These capabilities include visibility into and risk analysis of all users, devices, and resources and orchestration to automatically respond to security events.

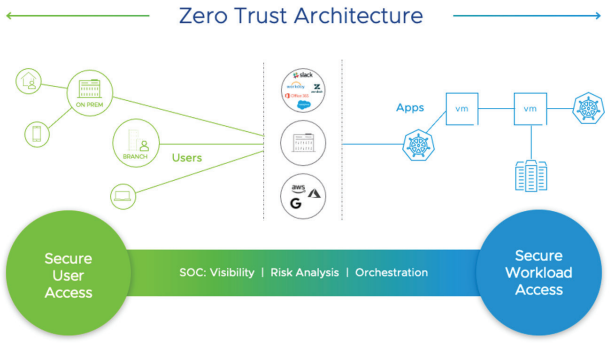

FIGURE 1: ZTA components

How secure workload access protects workloads

To support the principles of Zero Trust for application communication, secure workload access requires components that deliver east-west and edge controls plus authoritative context based on workload identity.

All these components work together to deliver the protection modern workloads need against advanced cyberthreats.

2. NIST Special Publication 800-207, Zero Trust Architecture, August 2020.

MAPPING SECURE WORKLOAD ACCESS TO NIST ZTA GUIDANCE

In its special publication, 800-27 Zero Trust Architecture, NIST defines Zero Trust and ZTA, describes general deployment models/approaches, and discusses use cases where Zero Trust can improve an organization's IT security posture.

NIST describes in section 3.1 the three approaches to implementing a ZTA as:

1. ZTA using enhanced identity governance
2. ZTA using logical micro segmentation
3. ZTA using network infrastructure and software-defined perimeters

Not only is the concept of secure workload access as described in this white paper compatible with all three of the NIST approaches, but it also extends the concepts within each to support the protection of workloads:

- The identity-driven approach is extended to include workload identity
- The micro-segmentation approach is extended to include threat prevention at the workload level
- The network infrastructure approach is extended to include protection within the workload as well as protection at the boundary of a private or public cloud

Secure workload access functionality for implementing controls

- East-west controls, which include:
  - Layer-7 micro-segmentation to apply access controls to communications into and out of workloads associated with an application
  - Workload security to protect the components inside the workload by scanning for vulnerabilities, configuration errors, and malware
  - API security to protect access to APIs exposed by workloads to the rest of the application
  - Advanced threat prevention for in-band detection and prevention of threats attempting to move laterally between workloads and applications
- Edge controls, which include:
  - Edge security to protect access to the clouds hosting workloads
  - Secure cloud-to-cloud connectivity for workloads running in different cloud environments
  - Web application and API security to protect individual applications from incoming threats
  - Advanced threat prevention to inspect incoming traffic at the cloud edge for threats using signature and behavior-based techniques

Authoritative context for secure workload access

- Workload identity involves having a complete inventory of all workloads to be secured using identifiers such as Internet Protocol (IP) address, Domain Name System (DNS), labels, and certificates. It is important to have a single source for all workload inventory with metadata and business relationship information from existing systems.

In addition to workload identity, authoritative context may include information on the workload such as the operating system, workload type, software version, known vulnerabilities and misconfigurations, and anomalous workload behavior.

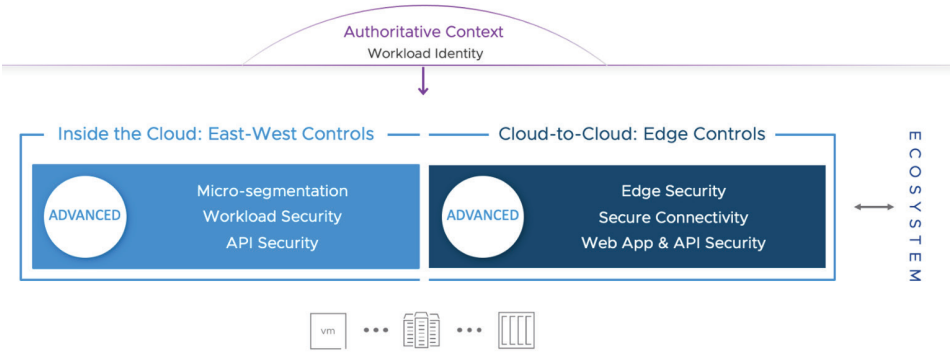

FIGURE 2: Secure workload access components

VMware enables full deployment of secure workload access

With solutions from VMware, enterprises can improve their security posture by implementing Zero Trust strategies that support secure workload access.

Adopting VMware solutions enables enterprises to more easily protect application and workload communication that accelerates adoption of Zero Trust principles, reduces the attack surface, mitigates lateral movement by attackers, and prevents advanced threats against applications. Using VMware security products, organizations can protect workloads from inside the cloud with east-west controls and add a layer of security between clouds with edge controls.

Here's how the VMware security portfolio supports the essential components needed to implement secure workload access.

East-west controls

- **Layer 7 micro-segmentation: VMware Distributed Firewall** – VMware NSX® Distributed Firewall[3] is distributed at each workload, requires no network changes, automates policy, and eliminates blind spots. With NSX Distributed Firewall, enterprises can easily create, enforce, and manage micro-segmentation policies with deep visibility into east-west traffic and comprehensive security policy controls.
- **Advanced threat prevention: NSX Advanced Threat Prevention for the NSX Distributed Firewall** – NSX Advanced Threat Prevention protects workloads and prevents lateral movement of threats by delivering network traffic analysis, intrusion detection and prevention, and advanced malware analysis with comprehensive network detection and response capabilities.
- **Workload security: VMware Carbon Black Cloud™ Workload, VMware Carbon Black Cloud Containers** – VMware Carbon Black Cloud Workload provides advanced security that is purpose-built for workloads. It secures workloads against modern attacks, blocking both known and unknown threats—including malware, fileless, and living-off-the-land attacks. VMware Carbon Black Cloud Container enables enterprise-grade container security at the speed of DevOps by providing continuous visibility, security, and compliance for containerized applications from development to production—in any private or public cloud environment.
- **API security: VMware Tanzu Service Mesh** – VMware Tanzu™ Service Mesh™, built on VMware NSX, is an enterprise-class service mesh solution that provides consistent control and security for microservices/APIs, end users, and data—across all clusters and clouds in the most demanding multi-cluster and multi-cloud environments. Enterprises can secure applications and data by defining attribute-based authorization policies for service-to-service access control.

Edge controls

- **Edge security and advanced threat protection: VMware NSX Gateway Firewall[4]** – VMware NSX Gateway Firewall is a standalone, software-only Layer-7 firewall that offers application and user access control along with advanced threat protection (including signature-based detection, behavior-based detection, network sandboxing, and URL filtering) and Transport Layer Security (TLS) decryption.
- **Secure cloud-to-cloud connectivity: NSX Gateway Firewall** – VMware NSX Gateway Firewall inspects all incoming and outgoing traffic at the cloud edge to provide comprehensive protection against threats.

3. Previously called NSX Service-defined Firewall

4. The information presented here is for informational purposes only and may not be incorporated into any contract. There is no commitment or obligation to deliver any items presented herein.

- **Web applications and API security: NSX Advanced Load Balancer with WAF** – When deployed together, NSX Gateway Firewall and NSX Advanced Load Balancer provide multi-cloud load balancing, web application firewall (WAF) functionality, application analytics, and container ingress services. They enable enterprises to erect defenses at the boundary of each cloud deployment (private or public cloud using a gateway/edge firewall) and the boundary of each complex application (for example, at the ingress of a modern application with a WAF).

Workload identity: VMware Global Network Identities

VMware Global Network Identities is a network services platform that provides unified visibility, control, and governance of network identifiers to simplify management of network identities and provide a framework to implement secure workload access. It offers connectors to orchestrate DNS, Dynamic Host Configuration Protocol (DHCP), and IP address management (IPAM) capabilities in existing enterprise, public cloud, and managed solutions.

Scalability and manageability of secure workload access is critical

While enterprises need the controls enabled by the core elements of secure workload access to protect workload communications, it's also imperative to use solutions that collectively deliver optimal manageability, adaptability, and scalability of the ZTA environment. That's where VMware's approach to Zero Trust differs from the rest.

VMware takes an intrinsic approach that makes it easier to secure workload communications (and the rest of the digital footprint) across distributed environments, with less operational overhead and greater speed, scalability, and accuracy. This means that solutions from VMware that support secure workload access also provide:

- **A distributed architecture:** Security policies are fully distributed for scalable and ubiquitous traffic protection, ensuring there are no blind spots, avoiding traffic and inspection bottlenecks, and reducing architectural complexity.
- **Workload-awareness:** Security policies are specific to the workload, ensuring that policies can be specified at the granularity of workloads and that the lifecycle of the policy follows the lifecycle of the workload.
- **Elastic scale:** As the number of workloads and the volume of workload communications continue to grow, VMware solutions can scale easily and effectively by dynamically changing capacity based on workload traffic.
- **Policy automation:** For easy, simplified, and centralized management of security policies, VMware automates policy recommendations and generation, driven by unique visibility into network traffic and authoritative context.

Conclusion

For digital transformation success, enterprises must change their approach to security to reflect the realities of the modern application environment. The Zero Trust security model delivers what traditional perimeter defenses cannot: protection of digital assets no matter where they live.

Secure workload access extends Zero Trust principles to enable secure workloads and workload-to-workload communications across multi-cloud environments—private and public. VMware is leading the industry with solutions that fully support the requirements of secure workload access as a core part of a Zero Trust strategy.

For Further Reference

NIST Zero Trust Architecture NIST Special Publication 800-207, Zero Trust Architecture

VMware secure workload access implementation:

- VMware NSX Distributed Firewall
- VMware NSX Advanced Threat Prevention
- VMware Tanzu Service Mesh
- VMware NSX Gateway Firewall
- VMware NSX Advanced Load Balancer
- VMware Global Network Identities
- VMware Carbon Black Cloud Workload
- VMware Carbon Black Cloud Container

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: vmw-wp-securing-workload-access_v2 8/21