ADAPTIVE MICRO-SEGMENTATION: BUILT-IN APPLICATION SECURITY TO ENABLE ZERO-TRUST

Application Security Built into Your Environment, Not on Top of It

Gain home court advantage by 'ensuring good' rather than 'chasing bad'. Security is traditionally an asymmetric battle; attackers can try an infinite number of attack methods but only need to be right once, while defenders have to build a defense that must withstand an infinite quantity and variety of attacks every single time. Most security technologies are focused on identifying attack methods in order to stop them, resulting in an arms race that puts defenders at a major disadvantage.

But no one knows your applications and environment better than you. With Adaptive Micro-segmentation, you can use your existing virtualization infrastructure as the built-in visibility and control point needed to harness that knowledge and put it to use to shrink your application attack surface, giving you home court advantage over attackers.

Modern Apps are Distributed and Dynamic, Making 'Ensuring Good' Hard

Ensuring good. Zero-trust. Least privilege. Whitelisting. These concepts are not new to the industry. However, operationalizing these security models is hard because IT and InfoSec teams lack the comprehensive visibility and consistent control points needed to be successful.

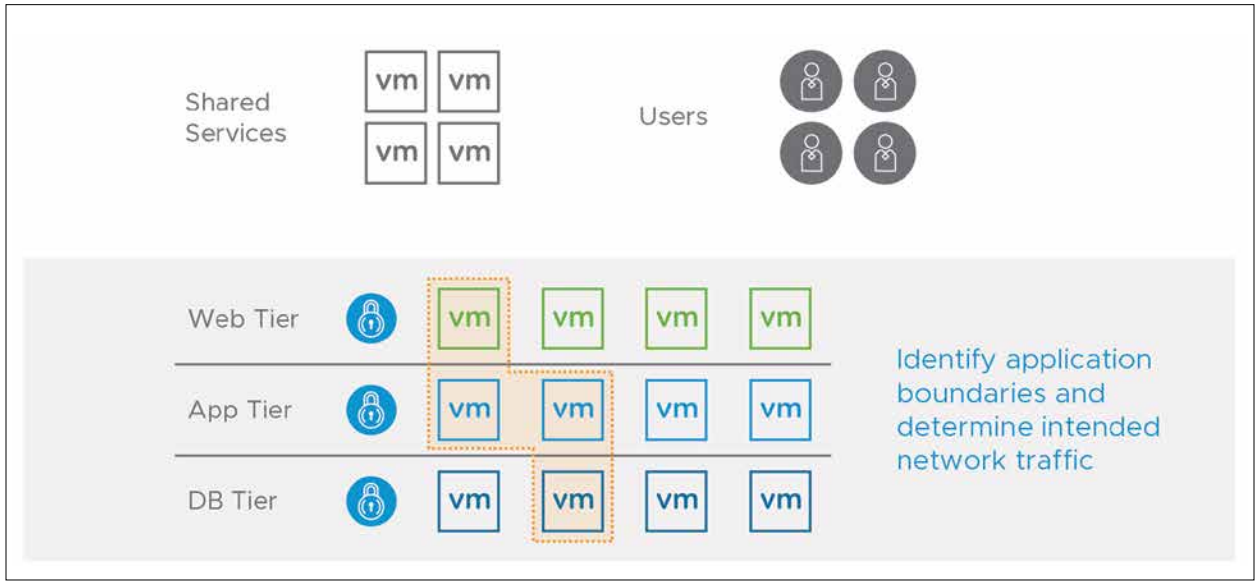
Applications are too widely distributed across data centers, private, and public clouds and they change too frequently for IT and InfoSec teams to determine their intended state and behavior, design and deploy adequate security policies and maintain these policies over time. Even if IT and InfoSec teams had all of the necessary insight, they lack consistent control points to effectively enforce security policies, regardless of where the application resides.

Built-in Application Visibility and Control with VMware

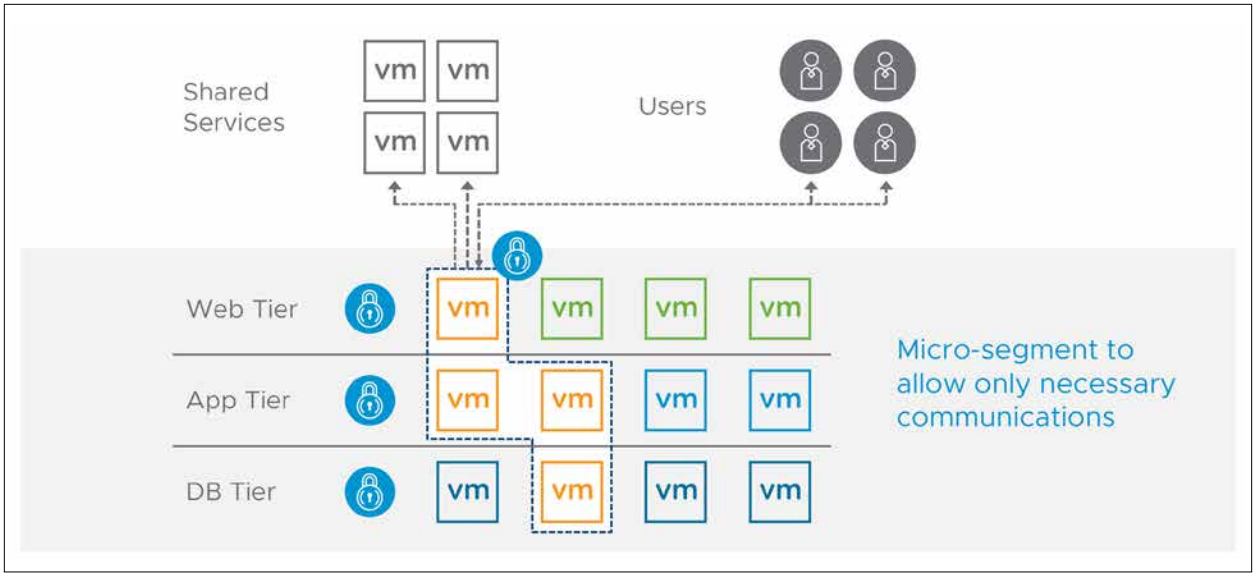
Adaptive Micro-segmentation gives you home court advantage by harnessing the knowledge of your applications' intended state and behavior and giving you built-in network- and workload-level controls to shrink the application attack surface based on that knowledge.

Enable zero-trust and Adaptive Micro-segmentation for your applications with VMware NSX® in three steps:

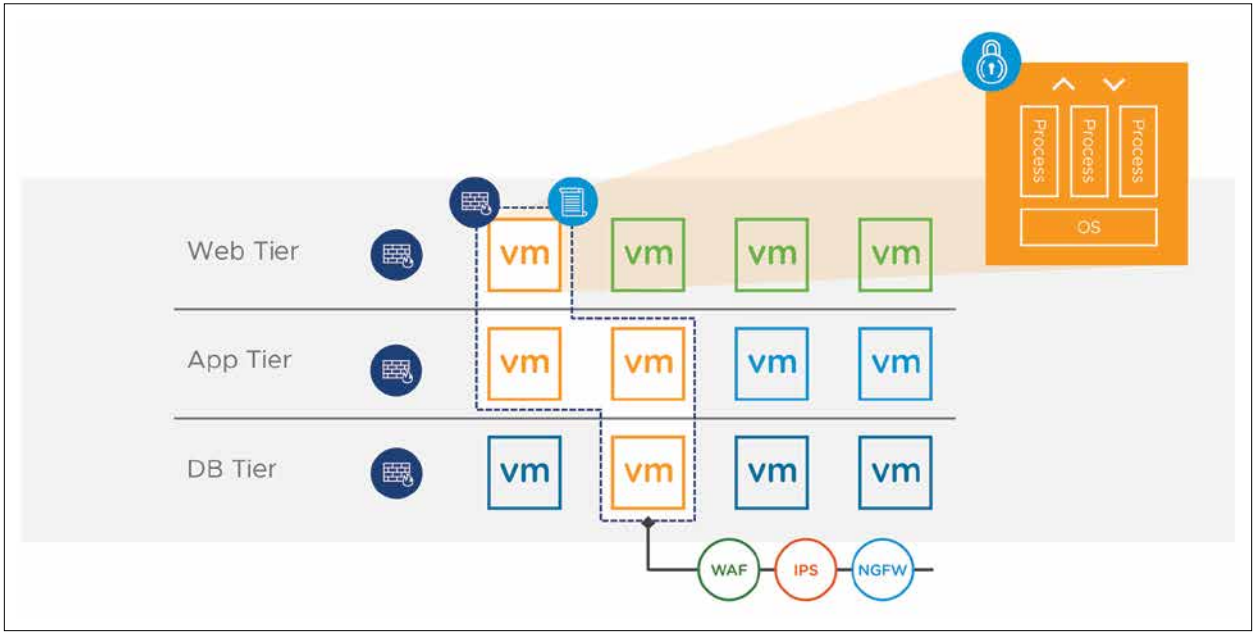
1. Determine Application Composition – Automatically identify the workloads and network traffic that make up a given application.



2. Micro-segment the Application – Determine all superfluous inter- and intra-application network traffic and create micro-segmentation policies to eliminate unnecessary traffic and reduce the application attack surface within the environment.



3. Enforce Workload Intended State and Behavior – Identify and enforce the individual workload intended state and behavior within the context of an application to protect against workload compromise through legitimate network communication paths and direct workload access.



By automatically turning application visibility and insights into security policies and enforcing those policies at both the network and workload layers of the application, VMware is able to reduce the attack surface of the entire application.

GET STARTED

Learn More About Adaptive Micro-segmentation Today

VISIT THE SITE >

Join Us Online:

VMware Difference – The Advantage of Built-in Security

By architecting security controls directly into the virtualization infrastructure on top of which applications live, VMware shifts security from a reactive afterthought to a proactive part of the application development lifecycle.

Holistic Application Visibility – VMware has unique visibility into application composition—from network communications to process-level behavior on individual workloads—due to its built-in position in the hypervisor and other native control points on top of which applications are built. This insight allows InfoSec and IT teams to design application-centric security policies without the need for a lengthy, arduous security review process.

Consistent, Automatic Enforcement of Security Policies – VMware enables the extension and enforcement of security policies across multi-data center and hybrid cloud environments and grants ubiquitous control over VM-based and container-based applications, from network- to workload- and process-level enforcement. Because the virtualization infrastructure is built into the software, automating the deployment and enforcement of security policies on both the network and the workload is easy.

Security Policy Lifecycle – VMware facilitates security as part of the application development lifecycle. InfoSec and IT teams have visibility into how applications they are responsible for protecting change over time. Newly provisioned workloads automatically inherit security policies that stay with them throughout their lifecycle. As the application changes, their security policies dynamically adapt to account for the changes. When workloads are eventually deprecated so are their security policies, decreasing policy bloat over time and simplifying management.

Summary

With VMware built-in application security, you can finally take advantage of home court advantage to protect your critical applications and get the most out of the VMware infrastructure you've already invested in. Learn more at www.vmware.com/nsx and www.vmware.com/appdefense.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com