Securing Applications in Virtualized and Cloud Environments with VMware AppDefense

While worldwide spending on IT security continues to climb, the odds of an organization falling victim to a data breach have risen to 1 in 4.[1] Despite thousands of security products on the market and massive budgets to purchase them, data isn't any safer. This creates a significant challenge for Chief Information Security Officers (CISOs), who are faced with securing applications and data living in increasingly dynamic, distributed IT environments. As more organizations embrace modern, agile models of application development, the problem of implementing security at the speed of the business is exacerbated – security is often seen as an obstacle to progress.

CISOs and their teams face two main challenges while trying to secure their data and applications:

Undetected threats and false alarms

Existing endpoint security solutions trigger numerous false alarms, resulting in Security Operations teams wasting time manually investigating non-existent threats. Worse yet, the can miss threats entirely.

Fast-paced, dynamic environments

Existing security solutions are not designed to accommodate the speed at which modern application development and deployment occurs, which means that as new applications are launched and updated, security cannot keep pace.

Transforming Security through Virtualization

VMware AppDefense is uniquely positioned to tackle both of these challenges. AppDefense is a data center endpoint security product that embeds threat detection and response into the virtualization layer on which applications and data live. Leveraging VMware vSphere®, AppDefense delivers three key advantages over existing endpoint security solutions:

Authoritative knowledge of application intended state – when you know what's good, you can detect what's bad

From inside the vSphere hypervisor, AppDefense has an authoritative understanding of how data center endpoints are meant to behave and is the first to know when changes are made. This contextual intelligence removes the guess work involved in determining which changes are legitimate and which are real threats.

Automated, precise threat response – the right response at the right time

When a threat is detected, AppDefense can trigger vSphere and VMware NSX® to orchestrate the correct response to the threat, without the need for manual intervention. For example, AppDefense can automatically:

- Block process communication
- Snapshot an endpoint for forensic analysis
- Suspend an endpoint
- Shut down an endpoint

AT A GLANCE

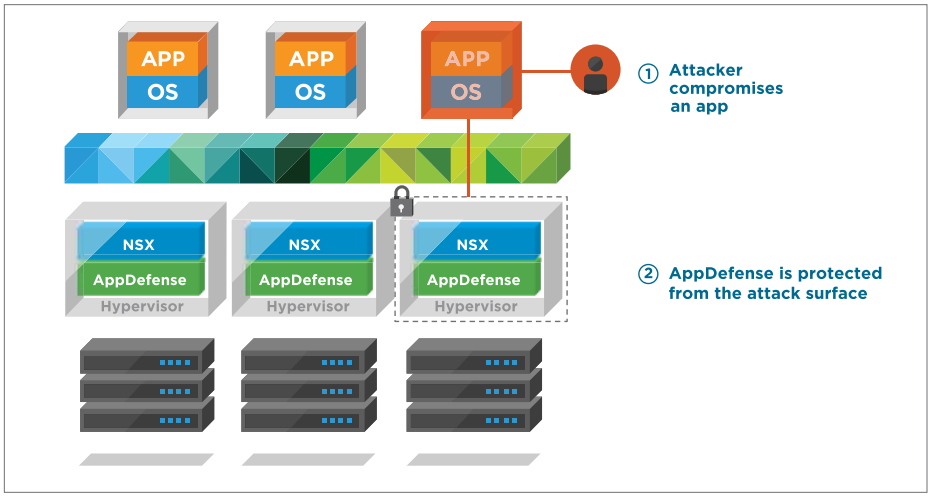
VMware AppDefense™ is a data center endpoint security product that protects applications running in virtualized environments. Unlike existing endpoint security solutions that chase threats, AppDefense focuses on monitoring applications against their intended state – what they're supposed to do – and automatically responding when they deviate from that intended state, indicating a threat. This maximizes Security Operations efficiency and effectiveness and streamlines the application security readiness review process.

KEY HIGHLIGHTS

- Simplify data center endpoint security
- Improve threat detection in SOC
- Automate incident responses
- Streamline application security reviews

Isolation from the attack surface – protect the protector

The first thing that most malware variants do when they reach an endpoint is disable antivirus and other agent-based endpoint security solutions. The hypervisor provides a protected location from which AppDefense can operate, ensuring that even if an endpoint is compromised AppDefense itself is protected.



AppDefense in Action

AppDefense is a foundational security product that has a wide-reaching impact on an organization's security strategy.

Application-centric alerting for the Security Operations Center (SOC)

AppDefense doesn't produce a lot of alerts, but when it raises the alarm it's smart to listen. The authoritative alerts generated by AppDefense coupled with automated response capabilities allow security administrators to focus on catching and eradicating threats from their environment, rather than sifting through noisy data and investigating threats that aren't there.

Transforming application security readiness reviews

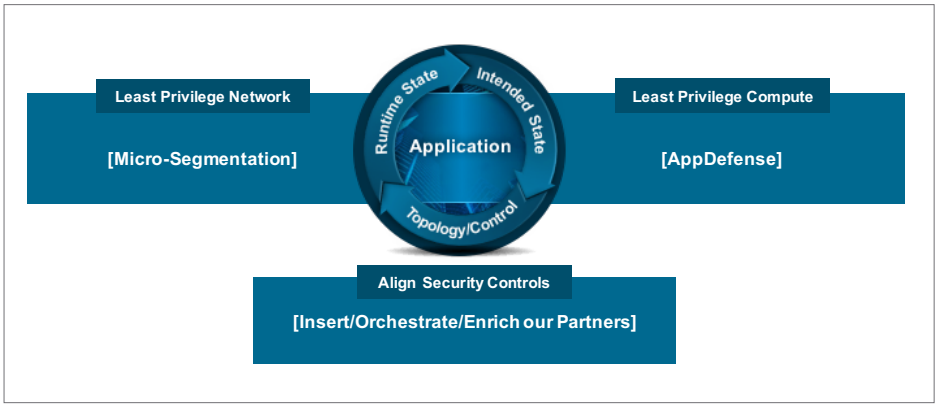
In the world of modern application development, applications are launched, changed, and decommissioned rapidly. By the time a security team learns of the existence of a new application, it has often already changed. AppDefense creates a common source of truth between application team and the security teams, streamlining the security review process.

Application-Centric Security with VMware

VMware has changed the face of network security with our network virtualization platform, VMware NSX, and its ability to enable micro-segmentation across the data center. NSX architects network and security services – such as firewalling – directly into the hypervisor, enabling a least privilege model for the network. The net outcome is that network security teams can prevent threats from moving laterally within their environments.

LEARN MORE

For more information or to purchase VMware AppDefense, visit http://www.vmware.com/appdefense and test drive the product in our Hands-on Lab.



AppDefense layers in threat detection and response capabilities into another core area of the infrastructure, enabling a least privilege model for data center endpoints. Should a threat make it onto an endpoint, AppDefense will immediately detect the threat and automatically respond with precision. Together, NSX and AppDefense offer a robust solution for securing the application infrastructure and thus, the applications and data that live there.

---

[1]Ponemon Institute, June 2017, "2017 Cost of a Data Breach Study: Global Overview"

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