VMWARE APPDEFENSE

Comprehensive Security for Your Applications

vmware®

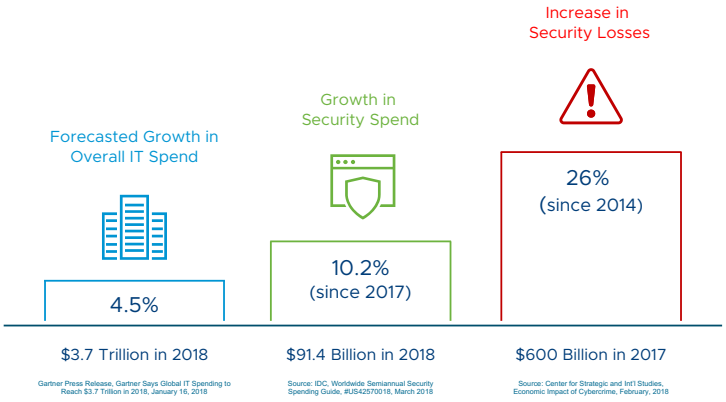
Table of Contents

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

Introduction

Despite cybersecurity being a top priority, organizations continue to fall short protecting against threats.

Security-related losses are increasing at a rate more than double that being spent on security. The amount of funds and effort being spent on security is simply not producing the expected results as seen in the graphic below.



Attackers are winning on a more frequent basis, and when they do, they cause more damage than ever before. Research reveals a hacker strikes every 39 seconds - and the cost of a breach is rising.[1] The average financial loss from a cyberattack is now estimated at $3.6 million, up 62 percent in the last five years. This is largely due to “dwell time”, or the number of days attackers can gain a foothold in your data center before intrusions can be identified and resolved.[2] In addition to managing the financial downside of a breach, businesses must also invest time and funds to reassure customers that their data is secure. The onus is on organizations to ensure comprehensive protection across their IT infrastructure and applications.

These statistics show an alarming trend in that many of the past security efforts have proven ineffective. Dozens of security products are being deployed, often with limited integration with one another, resulting in increased operational complexity. Attackers are taking advantage of this complexity to gain access into an organization and to remain in place for months at a time – undetected.

The fact is, we need better security - not more standalone security products. Instead of only focusing on attempting to hunt threats, we need to change the way we approach securing our applications and data. We need to evolve our thinking and focus on reducing the overall attack surface, which is a critical protection strategy that is often overlooked.

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

Rethinking Our Approach to Cybersecurity

Security tools are often completely unaware of the applications or infrastructure they are designed to protect. Instead – they spend most of their time focused on detecting threats, which is an extremely difficult proposition. One reason for this is that security is bolted on rather than architected into the infrastructure. We design infrastructure in advance of understanding all the applications that will run on it, then we build applications and tell security to go "secure it". The controls themselves are even bolted on to the infrastructure - as agents on endpoints or boxes on the network.

This model results in more and more specialized security products being used in an attempt to stay ahead of the never-ending threats against organizations. Unfortunately, it only increases complexity and creates challenges with the alignment of security controls. Each control has its own policy, its own telemetry, and its own source of truth. It's left up to the security team to reconcile these solutions. The result is greater cost and complexity -- but not greater security.

Unfortunately, this can result in IT organizations foregoing some security requirements in order to simply meet agile initiatives for the business.

This approach is simply not working. How do we fix it?

VMware Integrated Security

At VMware, we believe the answer to more effective cyber security won't be achieved by simply bolting on more security products to chase more threats. The answers are to architect security into the infrastructure rather than bolting it on, and to take a proactive approach that reduces the overall attack surface by continuously validating intended state behavior. This type of approach has been inherently difficult for organizations to achieve, but new capabilities provided by cloud and machine learning now make it feasible.

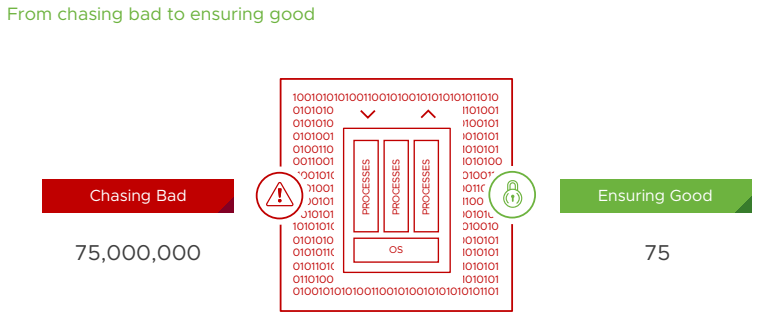
Security that is architected in to the infrastructure can provide a significant advantage in the ability to reduce the attack surface by having a unique understanding of:

1. Distributed applications (including their components and the infrastructure that serves them)
2. Expected (intended state) behavior of the application
3. Verified behavior from population analysis

With this understanding, VMware is uniquely able to leverage the virtual infrastructure to provide visibility into critical applications and data, and to create least privilege / zero trust environments around those applications and data. The end result is a dramatically smaller attack surface, and greater context to control to surgically respond to threats. This shifts the security model from solely focusing on chasing bad, to helping customers understand

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

what should be occurring across the environment. This process establishes a known-good state of behaviors that can then be monitored or enforced. Anything outside of the known-good is detected and can be responded to appropriately.



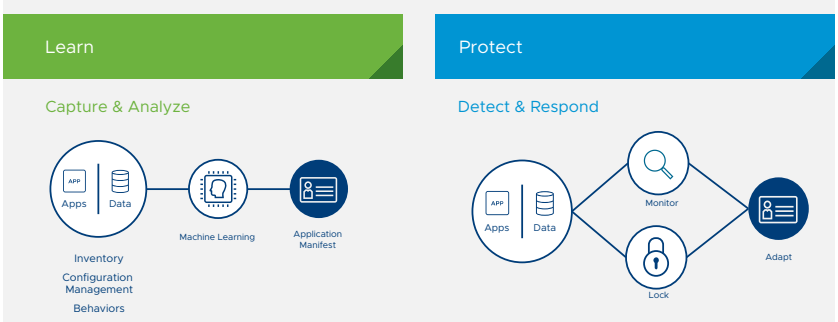
This simplified approach reduces the attack surface across compute and network, severely limiting the ability for an attacker to gain access or perform malicious activity. It not only cripples an attacker's ability to move laterally within the organization, it gives the security teams much better visibility and context around anomalous behavior that is occurring. Any behavior that deviates from the applications known intended state is recognized, resulting in faster detection, faster response, and if necessary, remediation of the threat.

VMware AppDefense

Leveraging the Hypervisor to Run Secure Applications

In contrast to traditional security solutions which focus on chasing threats, VMware AppDefense leverages its position in the hypervisor to learn and verify the intended state of an application and respond immediately to deviations from that state. The result is a common source of truth for IT and security teams, making it easy for them to collaborate around compliance, security incident investigation and incident response.

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



AppDefense enables enterprises to

- Learn: Understand, visualize, and verify the composition and intended state for the applications in your environment.
- Protect: Monitor your running applications against their intended state to know instantly when something or someone is manipulating your applications, and have greater context. You can also lock down applications so the only things that run are what you intended to run and respond to any deviations.

How AppDefense Works

Intrinsic

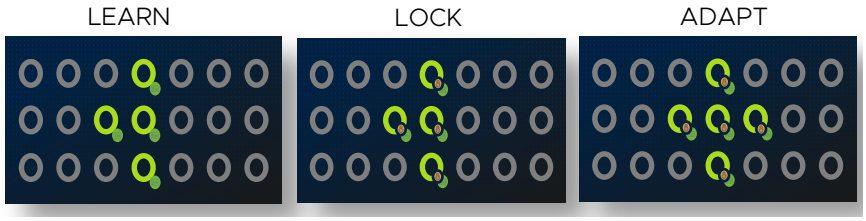
AppDefense is delivered natively through the virtual infrastructure, solving both operational and security challenges that are typically associated with application and endpoint security. Because AppDefense leverages VMtools for behavioral introspection, you get the benefit of deep OS-level and application inspection and control without the need for any add-on security agents. Reducing the need for agents on servers has tremendous operational advantages for organizations, including reducing lifecycle management requirements and easing performance challenges on critical machines. Additionally, AppDefense performs its inspection and control through a protected position offered by the ESXi hypervisor, providing a higher degree of confidence in its ability to control attacker behavior without being manipulated or disabled.

Learn

AppDefense uses a unique Intended State Engine to understand the composition and behaviors of an application. It correlates details from inventory, provisioning, automation, software catalogs, process reputation, as well as run time observation to build a “Manifest” of expected behavior. This contextual information is then analyzed using machine learning and

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

consensus to **verify** the intended state, which vastly reduces the manual burden of maintaining security policy. This baseline for how the application should be functioning and communicating (the Application Manifest) can then be used as a governing ruleset for detection and control.



Lock

Once the application manifest is established, AppDefense then monitors for any changes in the runtime behavior of the application. The continuous detection and prevention of any deviations from the intended state ensures the integrity of applications, infrastructure, and operating system. AppDefense has the capability of responding directly, such as blocking the attempted behavior immediately or sending an alert to your SIEM system. It also has the capability of kicking off more a more complex remediation like Snapshotting a VM for forensic analysis or adjusting the security policy of a VM through NSX service composer.

Adapt

Applications are in a constant state of change with software patching and system updates, etc., often occurring monthly, weekly, and daily. AppDefense continuously adapts its manifest by sending each behavior it sees back through its Intended State Engine to determine if it potentially was a false positive. This technique leverages machine learning and consensus models focused on verifying known good intended state. This vastly reduces the operational burden of zero trust security – and provides higher fidelity alerts for security operations. In addition, it allows AppDefense to work with modern applications that are more ephemeral in nature and have much more frequent updates. Through integrations with the CI/CD pipeline, the moment the application team make changes the AppDefense manifests are updated, therefore instantly updating the security team and the security policy.

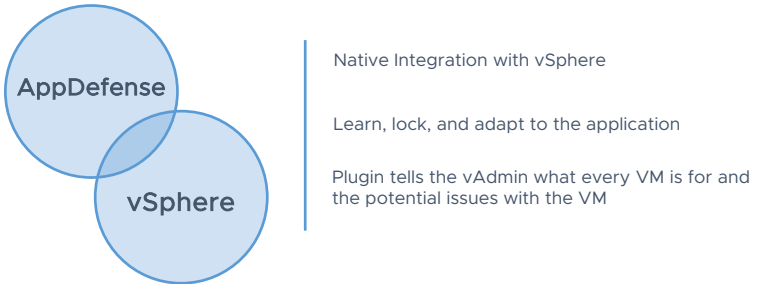
vSphere Platinum

The Most Secure Place to Run Apps

AppDefense can be added to vSphere version 6.5 and above. In addition, our flagship vSphere offering "vSphere Platinum" has AppDefense built right

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

in. vSphere Platinum includes an AppDefense plug-in for vCenter that enables rapid enablement across the infrastructure and provides virtualization teams detailed visibility and classification of their workloads. The plugin provides visibility into the behaviors of each workload and also calls into the AppDefense Intended State Engine to classify all learned behaviors. This also provides a single source of truth, allowing virtualization teams to collaborate far more effectively with security teams.



The benefits of vSphere Platinum include:

- Understanding the purpose, composition, and behavior of each of your virtual machines with application layer visibility
- Classifying behaviors from each VM through the AppDefense Intended State Engine and providing that detail within vCenter
- Alignment with the AppDefense console to allow virtualization teams to collaborate more effectively with security and compliance teams.

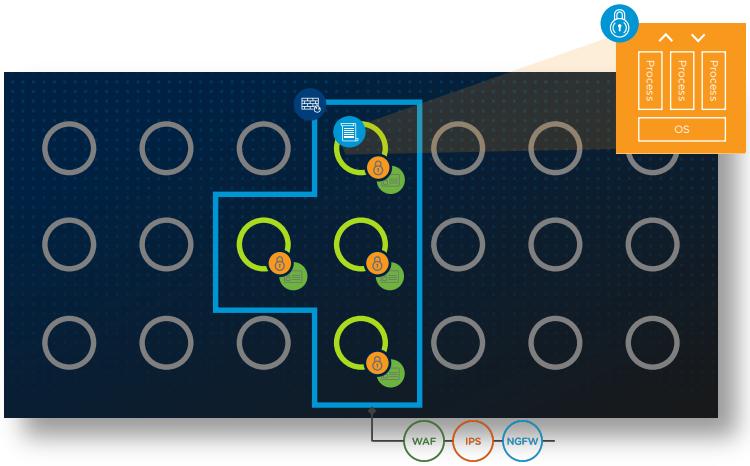
As a result, vSphere Platinum empowers virtualization teams to help shrink the attack surface and reduce the risk of security incidents from compromised applications in the enterprise.

Adaptive Micro-segmentation

Securing Network and Compute

Customers leverage VMware NSX to provide zero trust networks through micro-segmentation. AppDefense now integrates with NSX to provide Adaptive Micro-segmentation - a comprehensive, built-in zero trust model to secure applications and networks deployed in private or public cloud environments.

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



To achieve this level of visibility and control, NSX Data Center and VMware AppDefense work together to:

- Leverage the Intended State Engine to automatically determine the intended state and behavior of the workloads that comprise applications - including process behavior, operating system configuration, and necessary network traffic.
- Enforce security policies at both the network and application level. AppDefense programs the NSX distributed firewall directly, aligning the zero-trust network and zero trust workload to the application.
- Adapt to change by classifying unknown behavior and then adjusting rules (or increasing the severity of alerts) where necessary

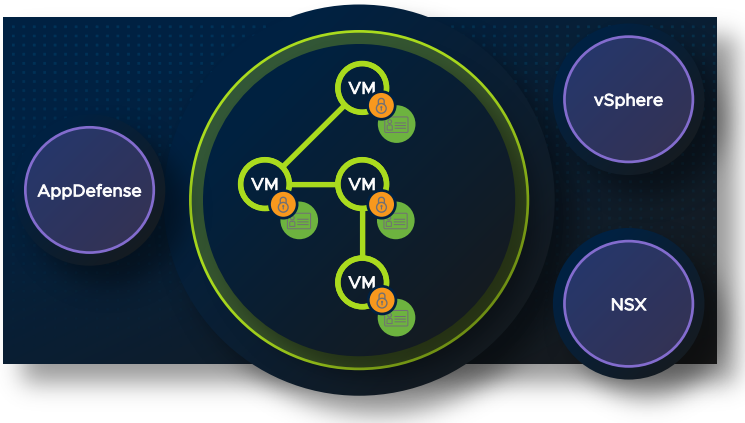
With Adaptive Micro-segmentation, InfoSec and IT teams can automatically determine the intended state and behavior of the workloads that comprise applications - including process behavior, operating system configuration, and necessary network traffic – resulting in a holistic picture of their applications without the need for lengthy application security reviews.

Summary

At VMware, we take an application-based approach to security, one that architects security in to the infrastructure, rather than bolting it on as an afterthought. Our unique capabilities across the network, compute, and mobile environments allow us to deliver granular visibility into the applications and data you are trying to protect and reduce the attack surface by creating least privilege / zero trust environments around those applications and data at

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

a network, workload, device and user level. The result is radically more secure and securable environment.



AppDefense is a ground-breaking product that leverages the unique capabilities of the hypervisor to enforce the known good state of applications and create automated and orchestrated response capabilities.

The combination of AppDefense with NSX Data Center delivers Adaptive Micro-segmentation to secure both network and compute environments.

vSphere Platinum bridges the gap between IT and security teams to offer a single source of truth that creates better awareness within IT teams while delivering alerts with application-based context to the security operations team and offering granular response capabilities.

[1] University of Maryland. "Clark School Study by Michel Cukier," February 10, 2017.

[2] Ponemon Institute. "2017 Cost of Data Breach Study," June 13, 2017.

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