IBM QRadar® + VMware AppDefense®

Protect Applications Running in Virtualized and Cloud Environments

Highlights

- Reduce the time to detect, remediate and respond to advanced threats across virtualized workloads with high fidelity application context.
- Understand the scope and veracity of advanced attacks through a single pane of glass versus pivoting on disparate tools and interfaces, streamlining the security review and readiness process.
- Limit attack surface by enforcing 'known good' application behavior.
- Focus on real threats and avoid alert fatigue with the potential of missing alerts in the noise of event data.

For years, the cybersecurity industry has been fragmented, disjointed and frustratingly complicated. Many enterprises have as many as 85 security tools from 45 different vendors. These siloed technologies often lack deep integrations resulting in ineffective security. At the same time, sophisticated threats continue to rise in numbers and scale, generating more security alerts than organizations can feasibly respond to with their limited time and resources. With the rapid adoption of hybrid cloud solutions there are now even more gaps in end-to-end visibility and control of the network.

To combat this complexity, IBM Security and VMware have joined forces to break down these siloed barriers by building an integrated solution that delivers actionable insights - accelerating threat protection and response for hybrid, on-premise and cloud environments.

Understand and Identify Threats Faster

VMware AppDefense integrates with IBM's QRadar Security Intelligence platform, enabling security analysts to understand threats and respond faster across their virtualized workloads. Downloadable via the IBM Security App Exchange, this powerful app provides enrichment to give SOC analysts the application context of devices in their virtualized and cloud environments.

AppDefense app understands how applications running in virtualized environments are meant to behave, monitors changes to that intended state, and sends actionable alerts when applications deviate from their intended behavior. This intelligence helps assess which application

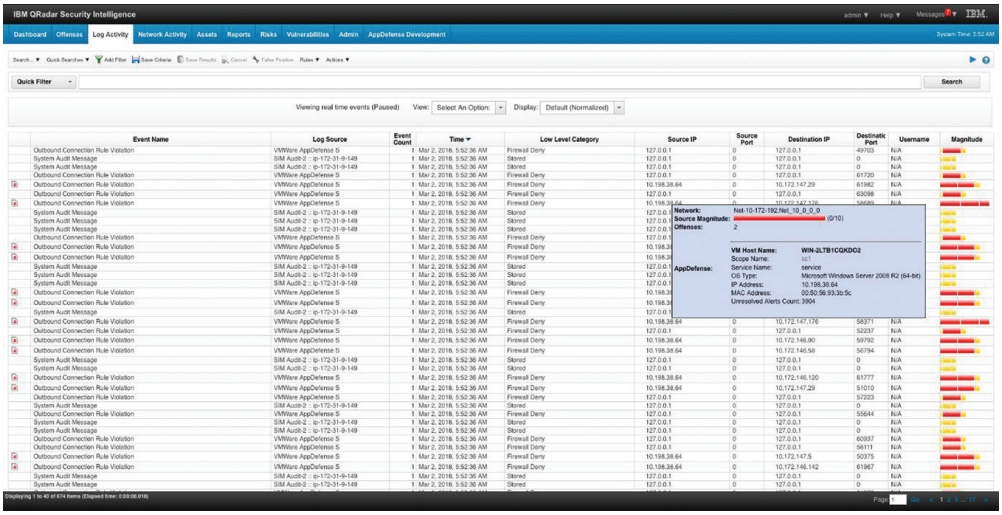
IBM Security vmware®

changes and network traffic anomalies associated with processes, executables and operating systems are legitimate and which are real threats. The analyst can get additional context from the myriad of information in QRadar, including IBM X-Force® threat intelligence and QRadar Watson Advisor, to gain better insight into the overall threat. The analyst can then quickly drill down into AppDefense for immediate actions, such as quarantining the endpoint, blocking process communication or shutting down the endpoint, to remediate threats quickly. This powerful integration enables the analyst to thoroughly understand the scope and veracity of advanced attacks on a single pane of glass, without having to rely on disparate security tools and interfaces.

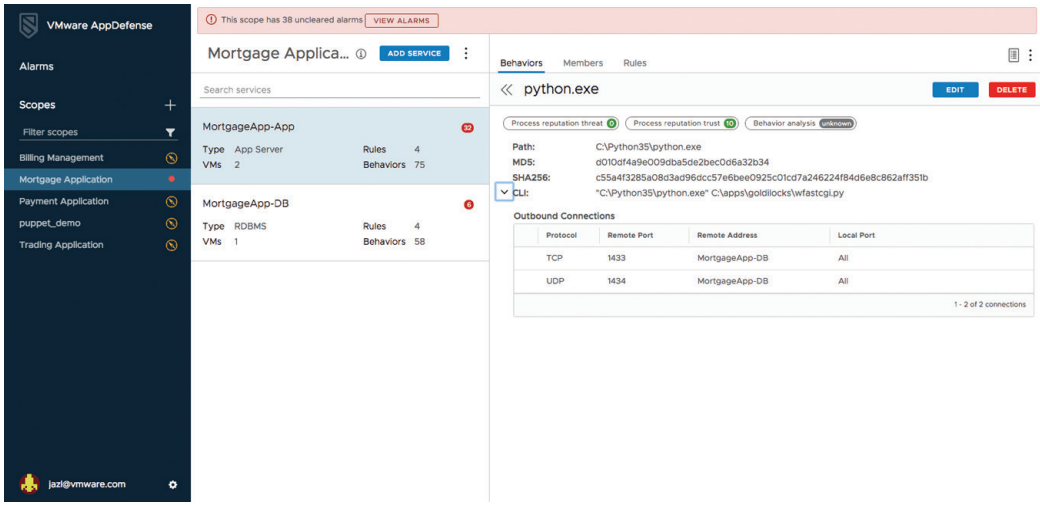
AppDefense layers in threat detection and response capabilities into the virtualization layer, thereby reducing the attack surface and enabling a least privilege model for data center endpoints.

By leveraging the power of QRadar combined with VMware AppDefense analysts can limit attack surface by securing the application infrastructure and data that live there.

View from QRadar's Log Activity screen, where a mouse-over can see details of the alert raised by AppDefense quickly and easily. The pop up alert will appear on any IP that is assigned to a VM that AppDefense tracks. This extra contextual informa-tion is valuable not only to investigate alerts from AppDefense but also events and flows from other devices in QRadar.



The analyst can then directly jump to the AppDefense UI to take action on the affected machine.



Why IBM and VMware?

IBM operates the world's broadest security research, development and delivery organization. This comprises 10 security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM solutions empower organizations to reduce their security vulnerabilities and focus more on the success of their strategic initiatives. These products build on the threat intelligence expertise of the IBM X-Force research and development team to provide a preemptive approach to security. As a trusted partner in security, IBM delivers the solutions to keep the entire enterprise infrastructure, including the cloud, protected from the latest security risks.

VMware AppDefense is a data center endpoint security product that protects applications running in virtualized environments. 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.

The ongoing collaboration between IBM Security and VMware is helping organizations to strengthen their posture against increasingly sophisticated cyberattacks. These two leading security providers are collaborating to build solutions and share threat information that will empower clients to act at extreme speed and scale, to see a threat once—and protect everywhere.

QRadar currently supports several additional VMware product families including VMWare vShield and VMWare vCenter.

IBM Security vmware®

For more information

To download the app, visit the IBM Security App Exchange:
ibm.com/security/engage/app-exchange

To learn more, contact your VMware or IBM representative:

VMware Partner Locator:
https://www.vmware.com/partners/siso/ibm-software-solutions.html

IBM Partner Locator:
https://www-356.ibm.com/partnerworld/wps/bplocator/#!/landin

Email: IBM4Me@Vmware.com

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
May 2018

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

Please Recycle