RELEASE NOTES

APPDEFENSE

What's New, July 2018

What's New, July 2018

This release of the AppDefense service focuses on improving ease of operation as well as addressing net-new security use cases with the GA of partner native container support. With this release, AppDefense improves the alarm remediation workflow by automatically de-classifying benign alarms. We also improved allowed behavior creation by introducing shared services and global services that better reflect the true network patterns of an application. Finally, the Aqua Security integration extends the AppDefense vision to container workloads. These improvements and others expand the addressable customer use cases and makes it easier for our customers to operationalize AppDefense at scale.

VMware Tools Embedded Release for Windows

The AppDefense Guest Module for Windows is now packaged with the 10.3.0 VMware Tools release. For customers that are already deploying VMware Tools on their VMs, AppDefense features can be delivered without any additional agents. This integration with the VMware ecosystem reduces the operation burden of security on IT.

Partner Native Container Support

AppDefense adds containers workloads as a supported use case with the GA of its partner native container support integration with Aqua Security. Working in combination with the Aqua Security manager, AppDefense customers can now have visibility into the inventory, behavior, and security profile of container workloads in their environment, side-by-side with their VMs.

Social Assurance

AppDefense has added the ability to leverage anonymized process data from other organizations in order to de-classify alarms. In practice, this means if a particular process is marked as anomalous for one organization, but is well-known within the ecosystem, AppDefense uses that information to lower the criticality of that alarm. This feature utilizes the unique qualities of the SaaS offering to significantly increase efficacy for organizations utilizing the service.

Alarm Classification

AppDefense has added severity levels for all security alarms, increasing operational efficiency by allowing customers to focus on the alarms that matter most. Alarms are classified in four severities: Critical, Serious, Minor, and Info. AppDefense automatically classifies alarms into different severities based on a number of factors, including 3rd party reputation, behavior analysis via machine learning (ML), and prevalence across the global population. Automatically classifying alerts reduces the operational burden on security teams.

Behavior Analysis in Protected Mode

AppDefense adds the ability to analyze behaviors with its machine learning (ML) algorithms at any point in the application lifecycle. This increased capability, backed by a significant infrastructure investment, greatly increases the runtime protections for an organization's applications.

Global Services

AppDefense add the ability to logically group IP addresses as an allowed group. For example, there are a number of "Windows update" IPs that are learned by a variety of applications in Discovery Mode. Sharing the aggregate list of those IPs as an allowed behavior reduces false positives and increases visibility.

vmware®

APPDEFENSE

What’s New, July 2018

Process Blacklist/Whitelist

AppDefense adds the ability to whitelist or blacklist processes across the entire organization. Processes in the blacklist will never be added to allowed behaviors. Alarms for processes added to the whitelist will be de-classified.

New SaaS Hosting Location (London)

AppDefense adds an additional hosting location for its SaaS service in London (AWS eu-west-2). Now, customers can choose where they want to access and store their data for GDPR and/or performance reasons.