DATA SHEET

AlienVault® AlienApps™

Extending USM Anywhere™ through Security Orchestration & Incident Response Automation

Today's constantly evolving threat landscape traps organizations in a "threat cycle." As new threats emerge, new security technologies are needed to address them. Another threat emerges, another technology follows.

Stuck in this continuous threat cycle, organizations tend to amass disparate security point solutions. This leads to an IT security environment that is siloed, complex to integrate, and difficult to manage.

AlienVault AlienApps break the threat cycle by extending the threat detection and security orchestration capabilities of the USM Anywhere platform to other security and productivity tools that your IT team uses.

With AlienApps, you can monitor more of your security posture directly within USM Anywhere, including your cloud services like Office 365 and G Suite. AlienApps also enable you to automate and orchestrate response actions when threats are detected by USM Anywhere, greatly simplifying and accelerating the threat detection and incident response processes.

AlienApps' highly extensible architecture allows AlienVault to seamlessly add new security and IT technologies to the platform as they become available, so enterprises can keep pace with the ever-changing threat landscape.

What You Can Do with AlienApps

CENTRALIZE YOUR DATA

AlienApps collect critical data from your on-premises and cloud infrastructure as well as cloud services, centralizing threat detection and incident response within USM Anywhere.

A centralized approach to security monitoring makes it easier and more efficient to investigate and respond to threats.

VISUALIZE YOUR THREAT POSTURE

AlienApps enrich your data and analyze it using the latest AlienVault Threat Intelligence. Pre-built, interactive dashboards in USM Anywhere visualize your threat posture, making it easier to gain insights into trends and identify anomalies worth investigation.

ORCHESTRATE & AUTOMATE

With AlienApps, USM Anywhere serves as a powerful security orchestration and automation platform. Whenever threats are detected in USM Anywhere, you can orchestrate your incident investigation and response activities, both by creating automated actions and by manually triggering actions.

RESPOND TO THREATS FASTER

When you automate or manually trigger action responses in USM Anywhere, you can communicate important security information back to your other IT and security tools, creating a closed loop threat detection and response process. For example, if USM Anywhere detects a malicious IP, it can notify your Palo Alto Networks firewall to block the IP address.