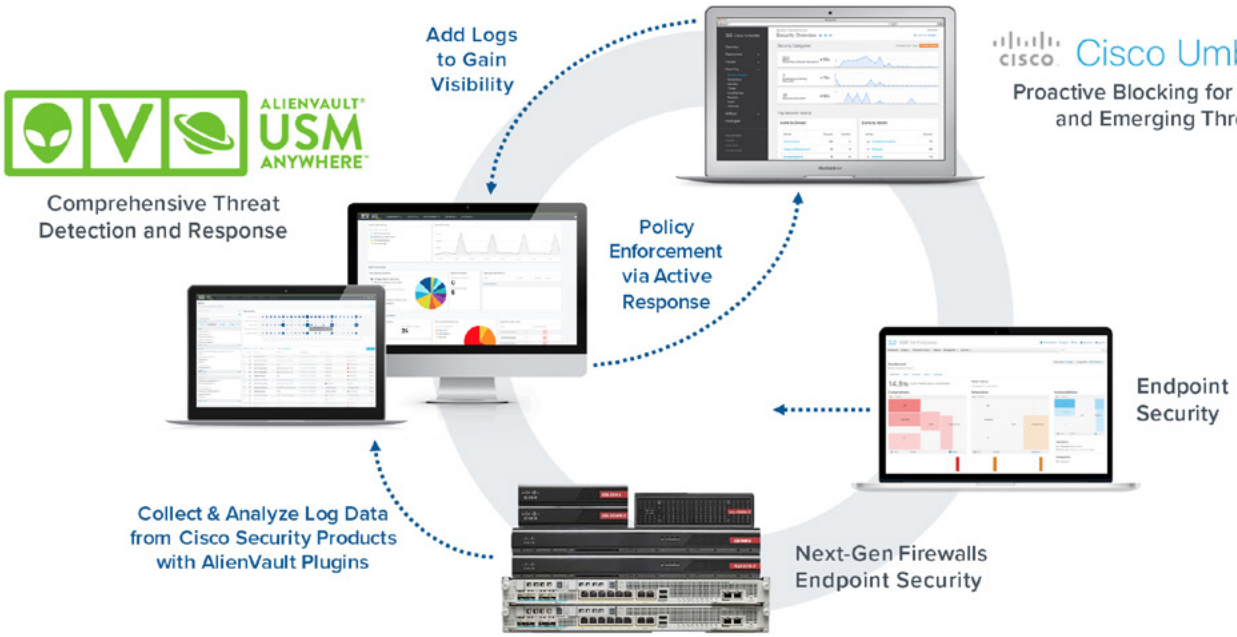
DATA SHEET

AlienVault® USM Anywhere™ and Cisco Umbrella

Powerful Threat Detection in the Cloud

The disconnected nature of today's security solutions demands innovation. As threats continue to evolve, organizations acquire more and more point solutions to maintain their security and mitigate their risk. Unfortunately, these point solutions are typically disconnected from each other, delivering sub-optimal protection that requires additional management effort along with often-complex inter-product orchestrations to be developed. This demands time, money, and resources that most organizations simply don't have.

Find a new way with AlienVault USM Anywhere and Cisco Umbrella. Together these solutions deliver a full package of security essentials for threat detection, taking your threat detection and response capabilities to new levels. With the integration of these products, you can add Umbrella logs to USM Anywhere to gain visibility into all internet activity and automated alerting, and you can send malicious domains detected within USM Anywhere to Umbrella for automated blocking.



A Unified Approach for Enhanced Protection

The AlienVault USM Anywhere platform is built with an architecture that delivers modularity and extensibility through AlienApps™. AlienApps are modular software components tightly integrated into the USM Anywhere platform that deliver technology quickly through the platform to extend, orchestrate, and automate functionality between the built-in security controls in USM Anywhere and the other tools that IT security teams need, including Cisco Umbrella. With the AlienApp for Cisco Umbrella, malicious domains identified by USM Anywhere can be passed instantly to Umbrella, ensuring the most current protection possible.

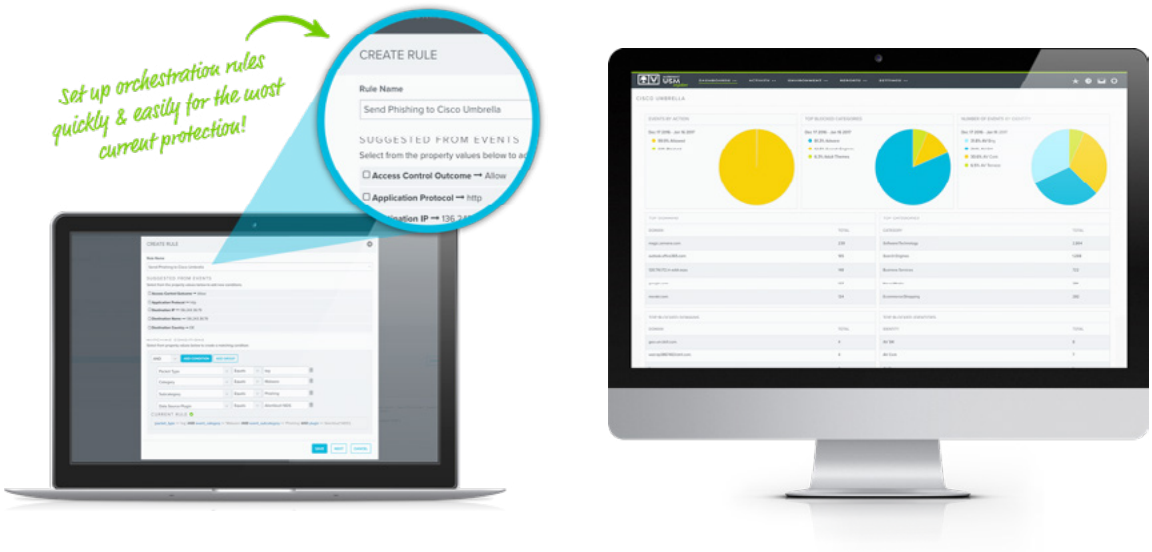
With the AlienApp for Cisco Umbrella, malicious domains identified by USM Anywhere can be passed instantly to Umbrella, ensuring the most current protection possible.

Through the combined solutions, customers receive the benefit of best-in-class threat intelligence delivered via the Cisco Talos research organization backbone and via the AlienVault Open Threat Exchange® (OTX™).

Orchestrate & Automate

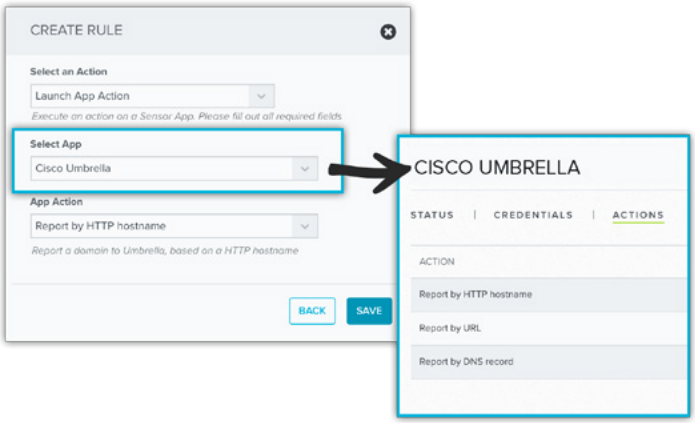
Threats identified by USM Anywhere can be sent to Cisco Umbrella – either through a user-executed action, or automatically based on a predefined rule – coordinating threat detection and response in a single, active response action.

The bidirectional capabilities of the AlienApp for Cisco Umbrella enable USM Anywhere to incorporate data from Cisco Umbrella into its threat analysis and orchestrate response actions by passing malicious domains identified by USM Anywhere instantly to Cisco Umbrella.



How it Works

- USM Anywhere detects communication from a phishing site
- USM Anywhere (either through a user-executed action, or automatically) sends the phishing data to Cisco Umbrella
- Cisco Umbrella will start to block upcoming requests to the domain name added



Benefits of the Combined Solution

SAVE TIME & MONEY	REDUCE TIME TO DETECTION & RESPONSE
• SaaS-delivered threat detection eliminates hidden costs and saves time • Affordable subscription-based pricing for USM Anywhere and Cisco Umbrella; buy what you need, add as you need • Unify visibility across cloud and on-premises environments, reducing time and expense of integrating and managing multiple products • Focus on threat response and not writing complex security analytics rules	• Get prioritized, contextual alarms with AlienVault OTX and the Cisco Talos backbone for robust threat intelligence • Automate policy enforcement between the platforms for rapid response • Enhance threat visibility and reduced mean time to detection & response

Unified Threat Detection and Automated Response

The combination of AlienVault's and Cisco's cloud security solutions deliver better outcomes to customers – specifically, shortening the time to protection/detection and response.

About USM Anywhere

AlienVault USM Anywhere is a cloud-based security management solution that accelerates and centralizes threat detection, incident response, and compliance management for your cloud, hybrid cloud, and on-premises environments. Unlike any other security solution on the market today, USM Anywhere delivers five essential security capabilities in a unified SaaS solution, giving you everything you need to keep your business secure in a single pane of glass.

About Cisco Umbrella

Cisco Umbrella, a secure internet gateway, is a cloud-delivered security platform that provides the first line of defense against internet threats to protect employees both on and off the corporate network. Umbrella stops current and emergent threats over all ports and protocols for the most comprehensive coverage.

Additional AlienVault USM Anywhere Resources

Analyst Report: 451 Research Report: AlienVault USM Anywhere

Webcast: Get Powerful Threat Detection for the Cloud, In the Cloud with USM Anywhere

White Paper: AlienVault USM Anywhere for AWS Environments