ALIENVAULT USM ANYWHERE

Organisations that want their threat detection, incident response, and compliance management centralised in one place need look no further than AlienVault, an AT&T company. Deployed as a SaaS (software as a service) solution, its USM Anywhere delivers everything they could possibly need, all easily accessible from a single web portal.

USM Anywhere provides a wealth of security measures, including automatic asset discovery, IDS, vulnerability assessment, event correlation, endpoint detection and response (EDR), compliance reporting and much more. Its scalable, distributed architecture is built around on-premises and cloud sensors, so no network is beyond its reach and it can continuously monitor Amazon Web Services (AWS) and Microsoft Azure cloud environments.

AlienVault provides purpose-built sensors for Hyper-V, VMware, AWS and Azure. These collect data from on-premises and cloud environments and securely pass it to the USM Anywhere cloud-hosted service, which provides a centralised collection and management point.

Deployment is simple, as we tested the Hyper-V version and had our sensor VM ready for action inside 30 minutes. The VM requires five virtual network interfaces, with the first used for management and internet access, while the other four are assigned to dedicated vSwitches, so they can passively monitor network traffic from mirrored switch ports to perform IDS.

An installation wizard quickly sorted out the sensor connection to our secure cloud account, created our first network scan for asset discovery and offered to scan our Active Directory server. It presented a status view of the VM network ports to confirm they were operational and provided details for Syslog-enabled devices to send logs to the sensor.

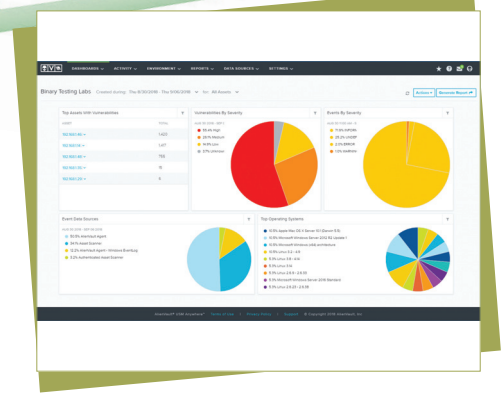
In under an hour, we were logged in to our cloud portal and viewing all discovered assets. Identification is accurate, as the scans correctly surmised we were running Windows Server 2012 R2 and Server 2016 hosts, had HPE ProCurve networking switches and multiple storage devices running various flavours of Linux.

USM Anywhere's dashboard puts everything at your fingertips with a default set of graphs and charts organised neatly into sections for SIEM alarms and events, asset discovery and vulnerability assessment. These team up to provide an instant readout on your security posture and you can create multiple custom dashboards from a big list of widgets.

The service runs scheduled standard and authenticated asset scans where the former probes network services, looking for vulnerabilities. Authenticated scans require administrative access to assets and provide more accurate information about running software and its configuration.

The AlienVault Agent can be deployed on selected assets to gather more detail and we used the predefined PowerShell script to download the Windows agent to our Server 2016 hosts. This also enabled the EDR feature for continuous asset security monitoring and compliance, plus file integrity monitoring.

Alert fatigue is avoided as rules analyse all events for behavioural patterns and issue alarms when the correlation engine has established patterns, such as cyber-attacks.



Alarms provide a wealth of information about associated events and the portal also offers sage advice on remedial action.

USM Anywhere's correlation rules are written and updated by AlienVault Labs Security Research Team; through the crowd-sourced Open Threat Exchange (OTX) community according to emerging and evolving threats they see in the wild and they use machine learning and human intelligence to analyse and expand threat scenarios. Along with extensive alerting facilities, USM Anywhere provides great reporting features including templates for the PCI, HIPAA, NIST and ISO 27001 security standards.

AlienVault's USM Anywhere is one of the most complete security solutions on the market, which we found surprisingly easy to deploy and use. This all-in-one SaaS platform presents all the information you need to pinpoint cyber-threats or asset vulnerabilities and it represents excellent value for businesses of all sizes.

Product: USM Anywhere
Supplier: AlienVault
Telephone: 353 21 206 3716
Web site: www.alienvault.com
Price: From £832 per month (ex VAT)