ALIEN VAULT

SOLUTION BRIEF

Delivering Security and Compliance for Higher Education with AlienVault USM

Higher education institutions are increasingly in the crosshairs of malicious hackers, with security breaches rising dramatically in recent years. Universities and colleges are an enticing target for attacks, given the open nature of campus IT systems, their limited IT resources, the high numbers of users bringing their own devices to campus networks, and the presence of valuable intellectual property at these institutions.

The Security Challenge

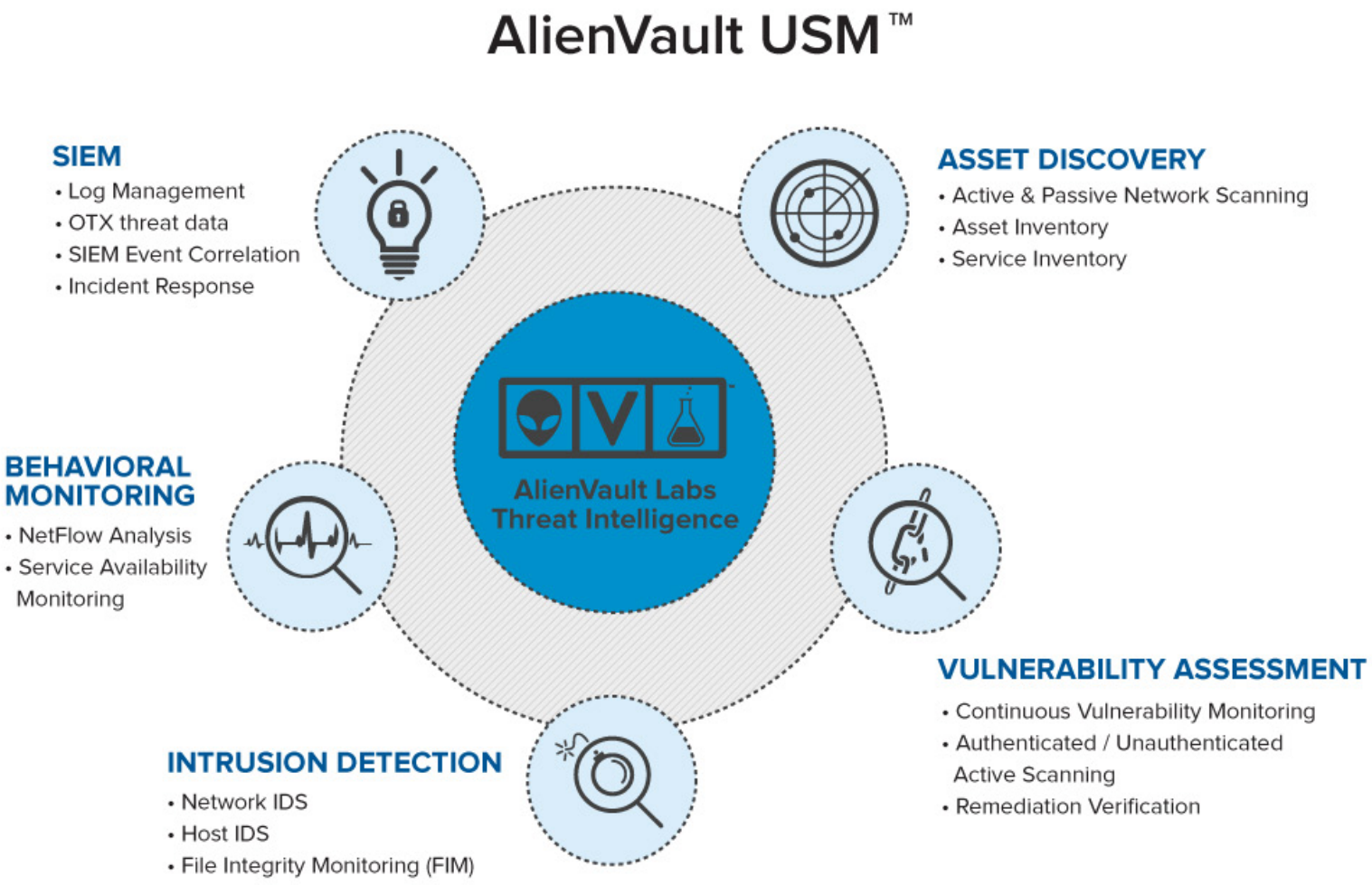
For these reasons and more, university information security and compliance presents a difficult challenge for IT security operators. You need to adeptly manage a range of issues, including securing your open networks from the latest threats, addressing the privacy concerns of your users, as well as managing your particular compliance requirements (such as FERPA, HIPAA, and PCI compliance).

You need a comprehensive threat detection and compliance solution that:

- Detects threats quickly
- Gives you complete visibility into your campus network
- Deploys quickly for fast insights
- Delivers critical compliance capabilities

Unified Security with AlienVault

AlienVault Unified Security Management (USM) is the comprehensive security solution ideally suited for higher education institutions. USM delivers five essential security capabilities in one platform, giving you everything you need to detect threats, prioritize response, and manage compliance. With built-in Threat Intelligence delivered by the AlienVault Labs team, USM enables you to detect the latest threats because AlienVault Labs acts as an extension of your IT team.



USM's 5 Features

USM Feature 1 - Asset Discovery:
Combines three core discovery and inventory technologies to give you full visibility into the devices that are on your campus network:

› Active & Passive Network Scanning

› Asset Inventory

Software Inventory Asset discovery and inventory are the first essential steps to knowing what systems and devices are on your university network, and which of these systems are in scope. AlienVault USM combines three core discovery and inventory technologies to give you full visibility into the devices that show up on your university network.

USM Feature 2 - Vulnerability Assessment: Identifies assets and devices with unpatched software, insecure configurations and other vulnerabilities on your campus network:

› Network Vulnerability Testing
› Continuous Vulnerability Monitoring

The integrated internal vulnerability scanning keeps you abreast of vulnerabilities on your university network, so you can prioritize patch deployment and remediation. Continuous correlation of your dynamic asset inventory with our vulnerability database provides you with up-to-date information on the vulnerabilities in your network, in between your periodic scans.

USM Feature 3 - Intrusion Detection: Coordinates incident response and threat management across your university network with built-in security monitoring technologies, emerging threat intelligence from AlienVault Labs, and seamless closed-loop workflow for rapid remediation:

› Network-based IDS (NIDS)
› Host-based IDS (HIDS)
› File Integrity Monitoring (FIM)

Built-in file integrity monitoring in host-based agents installed on in-scope servers alerts you to unauthorized modification of system files, configuration files or content. Monitoring of network access across both wired and wireless campus networks using host- and network-based detection systems identifies who tried to access those systems, files, and content.

USM Feature 4 - Behavioral Monitoring: Identifies anomalies and other patterns that signal new, unknown threats in your campus network, as well as suspicious behavior and policy violations by authorized users and devices:

› Service and Infrastructure Monitoring
› Netflow Analysis
› Network Protocol Analysis / Packet Capture

Integrated behavioral monitoring gathers data to help you understand “normal” system and network activity, which simplifies incident response when investigating a suspicious operational issue or potential security incident. Full packet capture enables complete protocol analysis of university network traffic, providing a comprehensive replay of the event that occurred during a potential breach.

USM Feature 5 - SIEM: Identify, contain, and remediate threats in your campus network by prioritizing your risk and response:

› Log Collection
› Event and Intelligence Correlation
› Incident Response

You can automatically correlate log data with actionable security intelligence to identify policy violations and receive contextually relevant workflow-driven response procedures. You can also conduct forensic analysis of events using digitally signed raw logs for evidence preservation.

Accelerate Compliance with USM

Higher education institutions also need to meet a number of regulatory compliance guidelines, including FERPA, HIPAA, PCI, GLBA and SOX. FERPA compliance is one of the most critical, as it pertains to the privacy of student records. There are a number of elements to FERPA compliance, but a frequently misunderstood area concerns the log requirements. FERPA requires institutions maintain logs of who has authorized access to student records, and mandates requirements around user access to those records. Therefore, as a higher education institution, you need to ensure you have the technologies and procedures in place to provide this log maintenance and access control.

AlienVault USM delivers key capabilities to help you achieve FERPA compliance. USM features a logger as one of its main architectural components which stores log files and other data for extended periods of time. The USM platform also has the ability to digitally sign the logs at the line level, ensuring that the logs you have stored have not been modified since their creation. In addition, USM allows for data integration from legacy security tools to ensure you can meet additional compliance requirements.

USM also offers hundreds of built-in compliance reports for managing your HIPAA, PCI, GLBA, or SOX programs. These reports are automatically updated as asset and vulnerability assessment data changes, and you can quickly customize them based on your own compliance priorities.

Leverage AlienVault's Threat Intelligence

Threat intelligence is an essential component to any effective security program. And very often, it is too resource intensive and too costly for organizations, particularly higher education institutions, to invest in effective threat intelligence. That's where the Threat Intelligence delivered by AlienVault steps in. AlienVault collects millions of threat indicators daily, including data from the Open Threat Exchange (OTX), the world's first truly open threat intelligence community.

The AlienVault Labs team curates the data and combines it with additional information about attackers' tools, infrastructure, and methods to detect malicious behaviors -- true threat intelligence. This enables the AlienVault Labs team to continuously tune the USM platform to detect emerging threats. The Labs team incorporates their research into the library of over 2,700 customizable correlation rules that are included with the USM platform, eliminating the need for you to conduct the research on your own.

Harness the Power of the Open Threat Exchange (OTX)

OTX is the world's first truly open threat intelligence community that enables collaborative defense with open access, collaborative research, and integration with AlienVault USM and OSSIM. OTX's open access enables collaborative research by allowing everyone in the OTX community to actively share the latest threat data, trends, and techniques. It also accelerates the distribution of the latest threat data and automates the process of updating your security infrastructure.

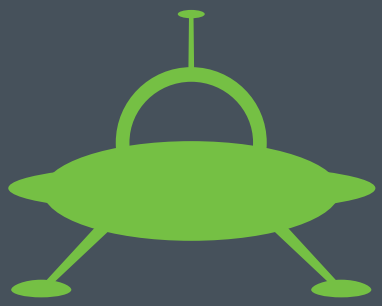
OTX enables everyone in the OTX community to actively collaborate, which strengthens your defenses while helping others do the same. And the USM platform integrates OTX 'pulses', which are community-generated groups of indicators of compromise (IOCs) that provide users with a summary of the threat, a view into the software targeted, and the related IOCs that can be used to detect threats.

AlienVault OTX benefits include:

- Shifts the advantage from the attacker to the defender
- Open for anyone to participate, not just AlienVault customers
- Each member benefits from the incidents affecting all of the other members
- Automated sharing of threat data accelerates the distribution to all members
- Data collected from over 140 countries ensures broad visibility of threat trends

Conclusion

Higher education institutions have unique security challenges to overcome in order to protect their infrastructure and data, and to maintain compliance. Often these institutions are resource constrained. AlienVault USM delivers the five critical security capabilities that your institution needs to detect threats, remediate responses, and maintain compliance. With USM, you can detect the latest threats without having to buy, deploy and manage multiple products or recruit, hire and retain a staff of security analysts. This gives you dollars back in your budget and hours back in your day.



About AlienVault

AlienVault has simplifed the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unifed Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowdsourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).