THE Simple SOLUTION

DATA SHEET

Simplify Reporting with AlienVault® USM Anywhere™

The reporting features in AlienVault® USM Anywhere™ make it fast and simple to get the visibility you need to maintain a strong security posture and to satisfy the reporting requirements of your compliance auditors, your executives, and your board of directors.

USM Anywhere delivers a comprehensive library of predefined reports for PCI DSS, HIPAA, and NIST CSF, so you can accelerate your compliance process and be audit-ready faster. It also includes 50+ predefined event reports by data source and data source type, helping to make your daily monitoring and reporting activities more efficient.

In addition to predefined reports, USM Anywhere gives you powerful security investigation capabilities at your finger tips. Its intuitive and flexible interface allows you to quickly search and analyze your security data, plus you can create and save custom views and export them as executive-ready reports. Because USM Anywhere gives you centralized visibility of all your cloud and on-premises assets, vulnerabilities, threats, and log data from your firewalls and other security tools, you have the most complete and contextual data set at your disposal.

This data sheet describes the predefined reports available in USM Anywhere out of the box. It also describes search and analytics capabilities in USM Anywhere that empower you to quickly produce your own custom reports.

Predefined Compliance Reports

To meet regulatory compliance requirements like PCI DSS and HIPAA and to ensure that you continuously meet those requirements, you must demonstrate that you regularly monitor your environments. This demands rigorous reporting to gain insight into your assets, vulnerabilities, and potential threats, which can be extremely time-consuming if executed manually.

AlienVault USM Anywhere delivers the following set of predefined compliance reports that map directly to common regulatory compliance requirements and frameworks, so you can quickly and easily provide evidence of compliance during your next audit.

In addition, you can easily customize any of the predefined compliance reports in USM Anywhere, adding dynamic graphs and charts to create a professional, executive-ready report.

PCI DSS

In USM Anywhere, once you define the PCI Asset Group—the servers, applications, and storage entities across your environment that are considered in-scope of a PCI DSS card-holder data environment (CDE)—then, you can readily view, export, and customize the following predefined reports.

ALIENVAULT USM ANYWHERE REPORT	PCI DSS REQUIREMENT
Summary of USM Anywhere hot and cold storage. Audit trail history for 12 months; three months for immediate analysis	10.7.a
Last 90 days of events available for analysis	10.7.c
File Integrity Monitoring (FIM) events on Windows systems	11.5.a
File Integrity Monitoring (FIM) events on Linux systems	11.5.a
Login failure events on Windows systems	10.2.4
Login failure events on Linux systems	10.2.4
Privilege escalations on Windows systems	10.2.5.b
Privilege escalations on Linux systems	10.2.5.b
Changes, additions, or deletions to any account by an administrator on Windows systems	10.2.5.c
Changes, additions, or deletions to any account by a root user on Linux systems	10.2.5.c
Account lockouts on Windows systems	8.1.6.a
Instances of plain text passwords on the network	8.2.1.c
Vulnerabilities identified across all environments	5.1.2
Vulnerabilities with risk rankings	6.1
Vulnerability scan history against all assets	Supplemental

HIPAA

In USM Anywhere, once you define your HIPAA Asset Group—the part of your environment that touches protected health information (PHI) data—then you can readily view, export, and customize the following predefined reports.

ALIENVAULT USM ANYWHERE REPORT	HIPAA CONTROL
Demonstrate that ePHI has not been altered, modified or destroyed in an unauthorized manner - Windows	§164.312(c)(1)
Demonstrate that ePHI has not been altered, modified or destroyed in an unauthorized manner - Linux	§164.312(c)(1)
Does your practice have policies and procedures establishing retention requirements for audit purposes?	§164.312(b)
Does your practice analyze the activities performed by all of its workforce and service providers to identify the extent to which each needs access to ePHI?	§164.312 (a)(1)
Does your practice categorize its information systems based on the potential impact to your practice should they become unavailable?	§164.308(a)(1)(ii)(A)

NIST Cybersecurity Framework (CSF)

USM Anywhere allows you to quickly and easily report out the status of controls across the NIST CSF functions of Identify, Protect, Detect, and Respond. The following predefined NIST CSF are available out of the box in USM Anywhere.

ALIENVAULT USM ANYWHERE REPORT	NIST CSF CONTROL
Asset Management	
Physical devices and systems within the organization are inventoried	ID.AM-1
Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	ID.AM-5
Risk Assessment	
Asset vulnerabilities are identified and documented	ID.RA-1
Threat and vulnerability information is received from information sharing forums and sources	ID.RA-2

ALIENVAULT USM ANYWHERE REPORT	NIST CSF CONTROL
Access Control	
Identities and credentials are managed for authorized devices and users	PR.AC-1
Information Protection Processes & Procedures	
A vulnerability management plan is developed and implemented	PR.IP-12
Protective Technology	
Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	PR.PT-1
Anomalies and Events	
Detected events are analyzed to understand attack targets and method	DE.AE-2
Event data are aggregated and correlated from multiple sources	DE.AE-3
Incident alert thresholds are established	DE.AE-5
Security Continuous Monitoring	
Personnel activity is monitored to detect potential cybersecurity events	DE.CM-3
Malicious code is detected	DE.CM-4
Monitoring for unauthorized personnel, connections, devices, & software	DE.CM-7
Vulnerability scans are performed	DE.CM-8
Detection Processes	
Event detection information is communicated to appropriate parties	DE.DP-4
Analysis	
Forensics are performed	RS.AN-3

Predefined Event Reports

To give you insights into key events by different data source types or by specific solutions, AlienVault USM Anywhere delivers the following predefined event reports out of the box.

EVENT REPORT BY TYPE OF DATA SOURCE

- Anomaly Detection Events
- Anti-virus Events
- Application Events
- Application Firewall Events
- Authentication Events
- Authentication and DHCP Events
- Cloud Application Events
- Cloud Infrastructure Events
- DNS Server Events
- Data Protection Events
- Database Events
- Endpoint Protection Events,
- Endpoint Security Events
- Firewall Events
- IDS Events
- Infrastructure Monitoring Events
- Intrusion Detection Events
- Intrusion Prevention Events
- Load Balancer Events
- Mail Security Events
- Mail Server Events
- Management Platform Events
- Network Access Control Events,
- Operating System Events
- Other Devices Events
- Proxy Events
- Router Events
- Router/Switch Events
- Server Events
- Switch Events
- Unified Threat Management Events
- VPN Events
- Web Server Events
- Wireless Security / Management Events

EVENTS REPORTS BY DATA SOURCE

- AlienVault NIDS
- AWS
- Amazon DynamoDB
- Amazon S3
- AWS VPC Flow Logs
- AWS Load Balancers
- Azure
- Cisco Umbrella
- Cylance
- FireEye
- Fortigate
- G Suite
- McAfee ePO
- Office 365
- Okta
- Palo Alto Networks
- SonicWall
- Sophos UTM
- Watchguard
- VMware
- Windows

Custom Reports

With USM Anywhere, you can easily create custom reports as you need. Here's how.

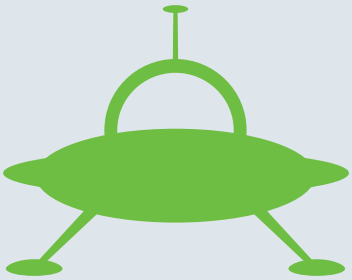
USM Anywhere's powerful log management capabilities give you a highly efficient way to search, filter, and analyze your security-related data. From either the Events or Alarms Views, you can filter the view by any data field or time frame or by entering your own search phrase. Because USM Anywhere stores your recent log and event data within its Elasticsearch hot storage, you can be assured that your search results generate extraordinarily fast.

In your filtered (or "custom") data view, you can drill down to view the details of any event or alarm to investigate it. You can select the data fields you want to display, and adjust the order in which they appear in the custom list view. And, you can sort the list based on key data fields, such as time created.

When you finish building the custom view that best suits your needs, you can click to save the custom data view for quick and continued access. For example, you may wish to save a custom data view that shows all login activities of a flagged suspicious user, so that you can review it daily.

You also have the option to export any predefined or custom data view in an HTML or CSV format, with options to define the report name and description, date range, number of records, and more. You can select from several rich predefined graphs to add visual elements to your data, perfect for analyzing trends or presenting an executive-level summary.

Explore USM Anywhere to Discover How Simple Reporting Can Be!



About AlienVault

AlienVault has simplified 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 Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowd-sourced 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.