SOLUTION BRIEF

Accelerate GDPR Compliance with AlienVault® Unified Security Management® (USM)

Privacy of personal information has always been seen as a fundamental right by the citizens of the European Union (EU). However, this right is one that is constantly challenged by ongoing technological developments and international business practices, particularly with more personal information being stored and transmitted electronically. In response, the EU passed the General Data Protection Regulation (GDPR), which was adopted on April 27, 2016, and will become enforceable on May 25, 2018.

AlienVault® Unified Security Management® (USM) helps you to quickly implement and demonstrate the appropriate technical measures required to protect personal data before, during, and after processing in accordance with the GDPR. AlienVault USM combines multiple essential security capabilities into a single platform, giving you an affordable and easy-to-use solution for security and compliance management. In addition, AlienVault USM provides highly customizable reports out of the box, as well as the ability to create your own custom reports and dashboards, making it fast and simple to get the visibility you need to maintain your organization's security posture and to demonstrate continuous compliance.

The General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), also known as EU Regulation 2016/679, is designed to strengthen and unify data protection for the personal information of all individuals ('data subjects') within the European Union (EU). Organizations with over 250 employees (or all organizations wherein processing of personal data is not occasional or includes particular types of sensitive personal data) and that store personal data of those individuals within EU states, must comply with the GDPR, even if the organization is located or operates outside the EU. When it becomes enforceable on May 25, 2018, it will replace the current Data Protection Directive (Directive 95/46/EC) of 1995.

GDPR provides the context, guiding principles, and governance framework for collecting and processing personal data of data subjects within the EU. A key focus of the regulation is on the data controllers and processors who manage and execute the processing of personal data. The GDPR highlights expectations of the data controllers and processors to implement appropriate technical and organizational measures to maintain the confidentiality, integrity, and availability of personal data.

Unfortunately, with 11 chapters, 99 articles, and 173 recitals, the GDPR is a very dense and difficult to comprehend regulation. That, along with its lack of prescriptive guidance on which controls to implement and how, has left many organizations ill-prepared to satisfy the requirements of the GDPR. This is particularly prevalent in organizations with smaller IT security teams, and those with few resources to acquire, configure, and manage multiple security technologies.

Unified Security and Compliance with AlienVault USM

To manage cybersecurity risk, an alternative to deploying and managing multiple point security solutions is to use a unified solution that combines several technologies into a single platform with a single management console. AlienVault® Unified Security Management® (USM) does just that. It provides multiple essential security capabilities, continuous threat intelligence, and a comprehensive set of dashboards and reports, all in a single, unified platform. Whether you manage AlienVault USM yourself or work with any of the AlienVault partners who can deliver managed security services for GDPR compliance on your behalf, AlienVault USM can help any organization accelerate their GDPR compliance program across their on-premises and cloud environments and cloud applications.

Multiple Essential Security Capabilities in a Single Platform

AlienVault USM Anywhere™ provides multiple essential security capabilities in a single solution, enabling you to rapidly deploy technical measures to meet many of the desired outcomes listed within the GDPR.

- **Asset Discovery**: Know who and what is connected to your cloud, on-premises, and hybrid environments at all times.
- **Vulnerability Assessment**: Know where vulnerabilities exist to avoid exploitation and compromise.
- **Intrusion Detection**: Continuously monitor your networks, hosts, and cloud environments to detect anomalies and attacks like malware, ransomware, and brute force authentication.
- **Behavioral Monitoring**: Identify suspicious user and administrator behaviors that could indicator an insider threat or account compromise.
- **Orchestrated Incident Response**: Enable discovered threats to be quickly contained and mitigated.
- **SIEM Log Management & Reporting**: Aggregate, retain, and enable analysis of security event data from across your network.
- **Integrated Threat Intelligence**: Receive continuous updated threat intelligence from the AlienVault Labs and the AlienVault® Open Threat Exchange® (OTX™), including correlation directives, vulnerability signatures, indicators of compromise, guided threat responses, and more.

Supporting GDPR Compliance with AlienVault USM

Articles 24 (Responsibility of the controller), 25 (Data protection by design and by default), 28 (Processor)

The primary outcomes of these articles are that the controller and processor must implement appropriate technical controls, in addition to organizational processes and procedures, to address cybersecurity risks.

CAPABILITY	EXAMPLES OF HOW ALIENVAULT USM HELPS
Continuous Monitoring	• Monitor for indicators of malware-based compromise, such as communication to a known Command & Control (C&C) Server. • Monitors successful and failed logon attempts to external applications through Azure Active Directory and Okta, and to Office 365 and G Suite. • Monitors user and administrator activities, including access and modification of files and content, in cloud applications such as Office 365 and G Suite. • Identify which assets have remote access services running. • File Integrity Monitoring (FIM) detects access and modification to files and directories on Windows and Linux systems. • Runs regularly scheduled scans to identify new and updated assets and to identify any vulnerabilities on each asset. • Continuously updated threat intelligence ensures that the AlienVault USM platform is operating with the latest correlation directives, vulnerability signatures, reports, guided responses, and more. • Identifies recommended patches for discovered vulnerabilities.
Personal Data Security	• Monitors for communications with known malicious IP addresses, which could identify exfiltration of data. • Monitors for changes to Office 365 policies including Data Leakage Protection (DLP), information management, and more. • File Integrity Monitoring (FIM) detects and reports on access and changes to system binaries, content locations, and more.
Incident Detection	• Aggregates events from across your on-premises and cloud environments and cloud applications, including Office 365 and G Suite. • Uses machine learning and state-based correlation capabilities to detect threats. • Classifies threats across a kill-chain taxonomy to inform the threat risk level. • Monitors public and dark web sources for the trade of stolen credentials. • Built-in notification capabilities enable analysts to be alerted to alarms through email, SMS, Datadog, PagerDuty, and Slack. • Customizable and searchable alarm and event views enable fast and simple review of events and detected incidents. • Continuously updated threat intelligence from the AlienVault Labs Security Research Team and the Open Threat Exchange® (OTX™) delivers the latest correlation rules and Indicators of Compromise (IoCs) to the AlienVault USM platform.
Incident Response	• With the AlienApp™ for Forensics and Response, enables automatic forensics tasks to be executed in response to a detected threat. • Enable forensics investigation with rich filter, search, and reporting capabilities event and log data. • With AlienApps, enables orchestration of manual and automated actions to be executed to contain threats, such as isolating systems from the network or blocking communications with known malicious IP addresses.

Articles 33 and 34 (Notification of a personal data breach)

Controllers are expected to notify supervisory authorities within 72 hours of the detection of a breach, where the breach is known to be able to do real harm to the affected data subject. Should the breach need reporting to the supervisory authorities, it also requires communication to the affected data subject(s). AlienVault® Unified Security Management® (USM) can support forensic investigation to determine the nature and extent of any breach, helping organizations determine what notification actions may be required.

CAPABILITY	EXAMPLES OF HOW ALIENVAULT USM HELPS
Continuous Monitoring	• Monitor for indicators of malware-based compromise, such as communication to a known Command & Control (C&C) Server. • Monitors successful and failed logon attempts to external applications through Azure Active Directory and Okta, and to Office 365 and G Suite. • Monitors user and administrator activities, including access and modification of files and content, in cloud applications such as Office 365 and G Suite. • Identify which assets have remote access services running. • File Integrity Monitoring (FIM) detects access and modification to files and directories on Windows and Linux systems. • Runs regularly scheduled scans to identify new and updated assets and to identify any vulnerabilities on each asset. • Continuously updated threat intelligence ensures that the AlienVault USM platform is operating with the latest correlation directives, vulnerability signatures, reports, guided responses, and more. • Identifies recommended patches for discovered vulnerabilities.

Article 35 (Data protection impact assessment)

Determining the level of risk of processing personal data includes assessing the processing environment for cybersecurity risks. Particularly with new processing environments and with applications created to process data, it is critical to understand the state of that processing environment and to regularly test for vulnerabilities. Doing so will help you to assure the confidentiality and integrity of personal data in that environment as well as the availability of the processing environment. AlienVault USM can support this effort through automated asset discovery, so you always know what is deployed across your on-premises, cloud, and hybrid environments, and can assess those assets for vulnerabilities.

CAPABILITY	EXAMPLES OF HOW ALIENVAULT USM HELPS
Asset Discovery	• Built-in asset discovery discovers physical and virtual assets running in on-premises and cloud environments (including AWS, Azure, VMware, Hyper-V). • Asset Groups deliver dynamic or analyst-defined grouping of assets, such as business-critical assets, HIPAA assets, PCI CDE assets, Windows assets, and more.
Vulnerability Assessment	• Identifies systems susceptible to known vulnerabilities or that may not have antivirus installed and/or operational. • Continuously updated threat intelligence from the Open Threat Exchange® (OTX™) and AlienVault Labs Security Research Team ensures that the AlienVault USM platform has the latest vulnerability signatures.

Reporting GDPR Compliance with AlienVault USM

Many of the requirements across GDPR are governance and/or process activities. Where technical security controls are in place, you must be able to quickly and easily report out on their status, whether for daily reporting or to meet an auditor's or executive's request.

Out-of-the-Box Reports

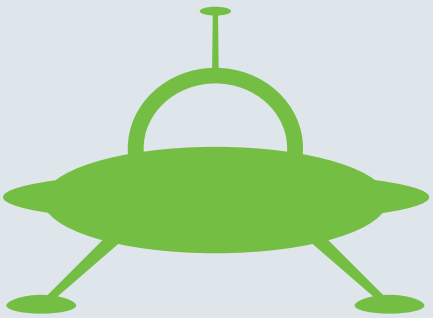
AlienVault® Unified Security Management® (USM) allows you to quickly and easily report out the status of technical controls across your cloud, on-premises, and hybrid environments with reports showing events by the type of data source, as well as by individual data sources.

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

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

Custom Views and Reports

With AlienVault® Unified Security Management® (USM), you can easily create custom reports and data views as you need. Its powerful log management capabilities give you a highly efficient way to search, filter, and analyze your security-related data. You can also customize the Alarms and Events views to best suit your needs and either save that view or export for future use. You can also export that view into a report and select from several rich predefined graphs to add visual elements to your data, perfect for analyzing trends or presenting an executive-level summary.



softwerx

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.