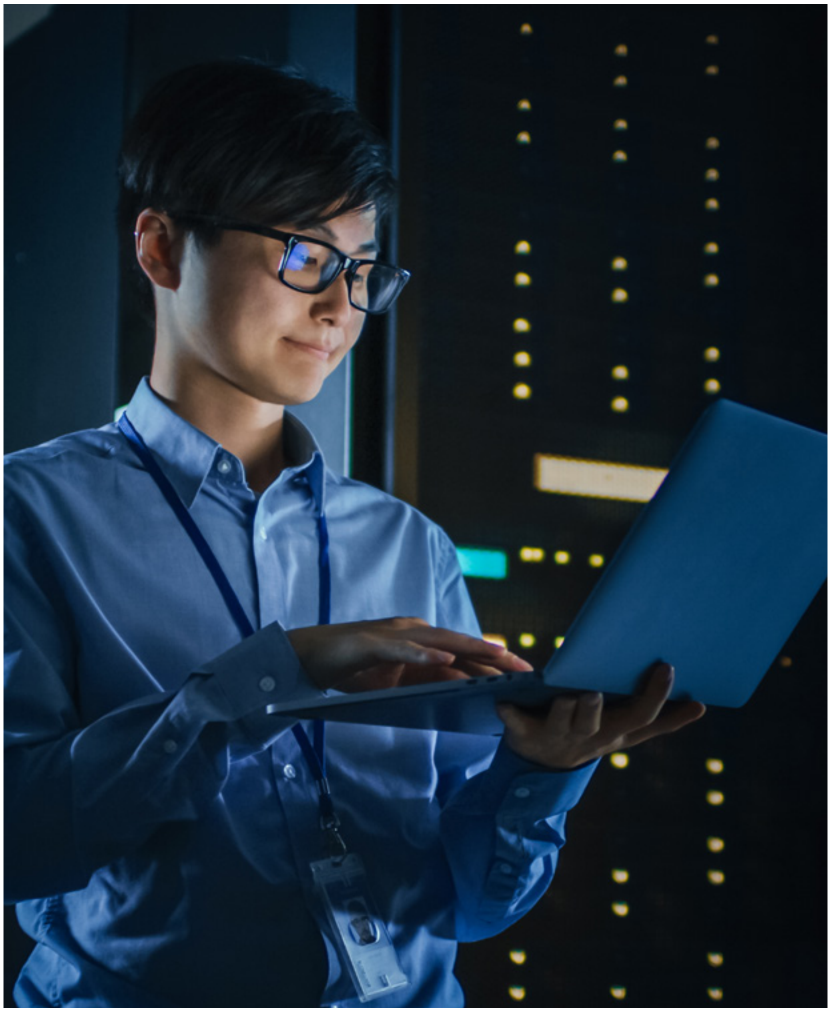
AT&T Cybersecurity

AT&T Business

Comparing USM Anywhere to AlienVault OSSIM

How to choose between open source and commercial products



AT&T Cybersecurity believes in an open, collaborative, and integrated approach to security—not a patchwork built of proprietary point solutions.

Most IT security teams struggle to build an effective IT security monitoring solution that can scale and adapt as their infrastructure changes. They are often resource-constrained, with limited time, tools, and security expertise. As a result, many teams cobble together solutions from a combination of open source and commercial products and do their best to monitor what they can. They find, of course, the best IT security monitoring solutions are those with integrated capabilities—which is why AT&T Cybersecurity has built a unified platform designed with the resource-constrained IT professional in mind.

IT professionals can choose between an open-source platform, AlienVault Open Source Security Information and Event Management (AlienVault OSSIM™), and the commercially-supported platform, USM Anywhere™ from AT&T Cybersecurity.

AlienVault OSSIM

AlienVault OSSIM provides a feature-rich, open-source SIEM (security information and event management) complete with event collection, normalization, and correlation. It distinguishes itself from other SIEMs in the marketplace with its integrated security management toolset, which reflects a subset of the capabilities offered by our commercial platform. Because of the time investment required to get the most out of an open-source solution, this product is best suited for IT professionals at smaller organizations with very few resources, security researchers, and members of the academic community.

USM Anywhere

The USM Anywhere platform delivers a comprehensive approach to security monitoring, providing resource-constrained organizations with virtually everything they need for effective threat detection, incident response, and compliance—all in a single pane of glass. The Unified Security Management® (USM) platform is best-suited for organizations that want to achieve greater operating efficiency, demonstrate regulatory compliance, and stay up to date with the latest threat intelligence, even without having dedicated security researchers in house.

Take a look at the table below to explore which solution best suits your needs. Next, we'll take a closer look at each item in the table to help you understand your options.

Find the right solution for you

	AlienVault OSSIM	USM Anywhere
Product availability	Open-Source software download	In the cloud
Pricing	Open source	View pricing options
Security monitoring	On-premises physical and virtual environments	AWS® & Azure® cloud environments Endpoints (cloud, on-premises, and remote) Cloud apps On-premises phsyical and virtual environments
Deployment architecture	Single server only	SaaS delivery with sensors deployed in each monitored environment Federation-ready
Security capabilities		
Asset discovery and inventory	✓	✓
Vulnerability assessment	✓	✓
Intrusion detection	✓	✓
Behavioral monitoring	✓	✓
SIEM event correlation	✓	✓
Endpoint detection and response	✗	✓
Log management	✗	✓
AWS & Azure cloud monitoring	✗	✓
Cloud apps security monitoring	✗	✓
Security Oorchestration and automation	✗	✓
Integration with third-party ticketing software (Jira®, ServiceNow®)	✗	✓
Threat Intelligence		
Powered by the AT&T Alien Labs™ Open Threat Exchange® (OTX™)	✓	✓
Continuous threat intelligence subscription	✗	✓

Support and documentation		
Community support through product forums	✓	✓
Full documentation and knowledge base	✗	✓
Dedicated phone and email support	✗	✓
Reporting		
Rich analytics dashboards and data visualization	✗	✓

USM Anywhere vs AlienVault OSSIM: a detailed product comparison

As you compare these two platforms, it may be helpful to picture a bicycle and a car. Both are effective means of transportation, but one of them relies entirely on your strength and effort. The other has more automated components and requires much less manual effort to use. Knowing how each vehicle works makes it clear why both are reasonable options for a short commute, whereas a car is a much better choice for transporting a family of four cross-country in the middle of winter.

Similarly, the platforms have different structures and capabilities that are important to understand to make an informed decision. This paper will delve a little deeper into each of the categories laid out in the summary table above to help you understand your options.

Product availability

USM Anywhere and AlienVault OSSIM are available in different form factors. AlienVault OSSIM is available as a software download and requires that you find a server and deploy the product to that server. AlienVault OSSIM can be installed to a server of your choice and will perform based on the hardware resources made available to it. Alternatively, source code is available and can be downloaded and modified to support your specific needs.

USM Anywhere, in contrast, is a cloud-hosted, SaaS-delivered solution that centralizes security monitoring across your cloud, on-premises, and hybrid environments. The platform's cloud sensors natively monitor Amazon Web Services and Microsoft Azure® Cloud. On-premises, virtual sensors run on VMware® and Microsoft Hyper-V® to monitor your physical and virtual IT infrastructure. Data is sent from the sensors through an encrypted connection to our secure cloud, where your data is stored in an isolated, single-tenant data store with unique SSH credentials.

Pricing

AlienVault OSSIM is an open-source product, available to you for free. You can download it directly from the AlienVault OSSIM web page on the AT&T Cybersecurity web site. USM Anywhere is an affordable commercial solution sold as a monthly subscription, with pricing options to fit a wide range of budgets. See more detailed pricing information on our web site.

Security monitoring

It's important to understand what your requirements are, what you need to monitor, and why, before deciding whether USM Anywhere or AlienVault OSSIM is the right solution for you. AlienVault OSSIM is designed to help you monitor a small on-premises environment. It includes some of the built-in security capabilities that USM Anywhere provides but does not include log management nor native cloud monitoring. You should consider your threat detection, incident response, and compliance requirements as you determine which product to use.

USM Anywhere provides a variety of options based on the scope of your organization's needs, allowing you to monitor all your environments from a single pane of glass and scale your security capabilities as your business grows. The USM platform offers on-premises, private cloud, and public cloud monitoring capabilities for organizations at a wide range of sizes, enabling you to centralize your security and compliance monitoring in one comprehensive platform instead of piecing together different solutions.

Deployment architecture

Consider the scope of your deployment to determine what you need today and how much flexibility your environment will require as you grow and change.

AlienVault OSSIM allows you to quickly and easily deploy with an AlienVault OSSIM sensor and server installed on the same machine. It's a great way to get started. To extend your monitoring to other parts of your infrastructure (like a different location or network), you can deploy one or more sensors to collect data from those other environments and centralize it within the server. The product, however, does not include a log management tier, so the data is used primarily to pass through the built-in SIEM correlation engine, where the correlation directives (i.e., rules) evaluate the data to look for and identify threats. Keep in mind that because AlienVault OSSIM only deploys to a single server, it is most appropriate for low-volume deployments that do not require federation.

USM Anywhere is a cloud-based, SaaS-delivered version product designed to eliminate the costs and complexity of having to manage a full deployment yourself. The USM platform uses lightweight cloud sensors to monitor Amazon Web Services and Microsoft Azure cloud natively. On-premises, virtual sensors run on VMware and Microsoft Hyper-V to monitor your physical and virtual IT infrastructure. You can also deploy USM Anywhere agents on your Windows and Linux® endpoints. Data collection, security analysis, and threat detection are centralized in our highly secure cloud and provide you with a single view into both your cloud and on-premises infrastructure. Deployment is fast and easy, and the solution scales easily as your business needs change.

USM Anywhere also supports multi-tier deployments with its federated architecture, ideal for large, distributed environments and managed security service providers (MSSPs). A federated deployment allows users with multiple locations or USM platform instances to centrally monitor all alarms, vulnerabilities, and events in USM Central™.

Security essentials

Both USM Anywhere and AlienVault OSSIM are equipped with essential security capabilities to help you safeguard your business: Asset Discovery and Inventory, Vulnerability Assessment, Intrusion Detection, Behavioral Monitoring, and SIEM Event Correlation. However, like the bicycle and car mentioned earlier, it takes different amounts of time and effort to get anywhere with the two products. As you examine your options, consider the resources available to you— including time—relative to the security needs of your organization.

Asset discovery and inventory

Asset discovery is a critical and necessary step in understanding who and what is connected to your infrastructure. AlienVault OSSIM and USM Anywhere both provide built-in asset discovery. On a physical network, both products provide the ability to scan the network to identify assets on the network, determine basic information about those assets such as operating system, IP address, and MAC address, and what ports are active and listening. USM Anywhere, however, also enables asset discovery within Amazon Web Services and Microsoft Azure, allowing a comprehensive asset discovery capability across your public cloud, private cloud, and on-premises infrastructures.

Vulnerability assessment

Although USM Anywhere and AlienVault OSSIM both allow you to schedule vulnerability scans of your assets, a key consideration to keep in mind is the intelligence that powers the scans. In both platforms, vulnerability scans depend on a database of vulnerability signatures. For the USM platform, that database is both robust and dynamic, with new signatures added continuously in threat intelligence updates from the AT&T Alien Labs™ security research team. In AlienVault OSSIM, the default database is small and static—unless you regularly contribute your data to power the scans.

Intrusion detection

Intrusion detection is another area where data changes the playing field. Both USM Anywhere and AlienVault OSSIM offer intrusion detection capabilities. However, the correlation rules and vulnerability signatures that power each solution's intrusion detection capabilities are wildly different. AlienVault OSSIM offers a small number of static correlation rules that mostly serve as examples for users who want to write their own rules. While that makes it possible for you to customize rules based on your research, you should be aware of the significant time cost associated with tackling threat intelligence research on your own.

In contrast, the Alien Labs security research team continuously delivers threat intelligence updates to the USM platform automatically, so its collection of correlation rules and vulnerability signatures is current with the ever-changing threat landscape. In case an intrusion is detected, the threat intelligence updates include incident response guidance within the platform itself to help you respond quickly and effectively.

Having the Alien Labs security research team's research delivered to your platform is comparable to hiring your own in-house research team, but saving you that expense. See the Threat Intelligence section to learn more.

Behavioral monitoring

Yet again, data makes a difference. As with intrusion detection, behavioral monitoring and threat intelligence research in USM Anywhere is driven by the Alien Labs security research team. In AlienVault OSSIM, the capabilities are there—but not the correlation rules to drive them. You are responsible for creating those rules and keeping them up-to-date based on your threat intelligence research.

SIEM event correlation

AlienVault OSSIM provides SIEM event capabilities that allow you to correlate and analyze security event data from across your critical infrastructure and respond quickly to incidents.

USM Anywhere offers faster, more dynamic SIEM functionality using a unique graph-based analytics engine that allows it to correlate SIEM events more quickly. As a result, you're also able to run ad-hoc queries on the large data sets generated by centralizing security monitoring of all your cloud and on-premises IT environments, providing you with an efficient way to view and parse that data in with a high degree of granularity.

Endpoint detection and response (EDR)

Another delta between AlienVault OSSIM and USM Anywhere is EDR. In USM Anywhere, you can deploy agents to your hosts for continuous endpoint monitoring, as well as proactive querying during incident investigations. The agent is a lightweight, adaptable endpoint agent based on Osquery that is easy to deploy and manage directly from USM Anywhere.

Log management and log retention

To decide between USM Anywhere and AlienVault OSSIM, you need to consider your log retention requirements—especially if you are in a regulated industry or have stringent log retention requirements as a best practice. Even if you don't need it for compliance purposes, log retention is important to forensic and threat investigations. AlienVault OSSIM only retains SIEM events, which means you'll have a limited backlog of data to investigate in case of an intrusion, making it difficult to determine how long ago the intrusion began or how pervasive the effects have been.

The more data you need to store in your database, the fewer days' worth of data you'll have on hand, which can hinder your remediation efforts.

For organizations that require log retention, USM Anywhere provides robust log management, log search, and highly secure long-term log retention, making it a complete solution for your logging and SIEM needs.

USM Anywhere supports long-term log retention, known as "cold storage." By default, USM Anywhere stores all data associated with a customer's subdomain in cold storage for the life of the active USM Anywhere subscription. In addition, USM supports a "write once, read many" (WORM) approach to prevent log data from being modified. Logs can be readily requested for a specific date range from within the platform as needed.

AWS and Azure Cloud Monitoring

While both USM Anywhere and AlienVault OSSIM enable you to monitor on-premises infrastructure, only USM Anywhere provides security and compliance monitoring across on-premises, cloud, and hybrid environments from a single console.

Traditional network security and compliance monitoring capabilities can't provide visibility into the public cloud. Yet, security and compliance requirements apply regardless of where your data resides. Organizations that use or plan to implement AWS or Azure cloud environments need security tools built to overcome the security and compliance challenges posed by the public cloud.

USM Anywhere uses purpose-built cloud sensors to monitor your AWS and Microsoft Azure Cloud environments, helping you to eliminate your security blind spots and regain control over Shadow IT. Through the USM platform, for example, you can immediately discover new AWS or Azure instances or misconfigurations, detect and alert on abnormal behavior such as instances being spun up or down at odd times, and run continual

Cloud apps security monitoring

For many organizations, cloud applications mark an entry point into public cloud computing. As your users migrate business-critical data and operations to cloud apps, security concerns can include data loss or leakage, data privacy, unauthorized access, and more.

USM Anywhere provides insight into the activities of your admins and users in cloud applications such as Microsoft Office 365 and Google G Suite™. With the USM platform, you can put the proper controls in place to help keep your data and your organization highly secure and support compliance.

Security orchestration and automation

Security practitioners often need to juggle multiple solutions to meet their security needs. The security capabilities provided by AlienVault OSSIM can help somewhat to consolidate that toolset.

For organizations without the time to manage a proliferation of different security and compliance management tools, USM Anywhere comes with out-of-the-box security orchestration features to help you to reduce the time between detection and response. For example, if USM Anywhere detects evidence of ransomware on one of your assets, you can automate a response action to isolate or disable networking on that asset immediately.

By integrating security automation across both internal and external IT security and management technologies, USM Anywhere simplifies end-to-end security management across your entire critical infrastructure.

Integration with third-party ticketing software

In small IT departments where ticketing software is not an essential workflow tool, teams can manually create tickets based on AlienVault OSSIM alarms. Larger IT teams should consider USM Anywhere.

When threats and vulnerabilities are detected in the USM platform, you can open an incident ticket in third-party ticketing software, automatically or manually. By connecting with tools like ServiceNow® and Jira®, USM Anywhere helps security teams respond efficiently to threats and vulnerabilities without requiring any additional integration or installation. This enables teams to work more efficiently to remediate vulnerabilities and security threats.

Threat intelligence

Without threat intelligence, a SIEM is an empty shell. The threat landscape is continuously changing with the almost-daily discovery of new vulnerabilities, new attack techniques, and new strains of malware. You don't have the time or the resources to research these emerging threats on your own, let alone determine if your environment is at risk or already compromised.

AT&T Cybersecurity lightens the burden for security researchers at organizations of all sizes, making it possible for you to do more with less time. For both USM Anywhere and AlienVault OSSIM users, AT&T Alien Labs® Open Threat Exchange® (OTX™) provides threat data contributed daily from a global community of security researchers and practitioners. USM Anywhere takes that threat data to the next level with continuous threat intelligence updates from the Alien Labs security research team, making it easier for IT professionals to keep up with the latest threats.

Community-powered threat data from the OTX

The OTX™ is the world's largest open threat intelligence community. It enables collaborative defense with actionable, community-powered threat data, and global insight into attack trends and bad actors. OTX pulses provide users with a summary of the threat, a view into the software targeted, and the related indicators of compromise (IOC) that can be used to detect the threats. IOCs include:

> IP addresses
> Domains
> Hostnames (subdomains)
> Email
> URL
> URI
> File hases: MD5, SHA1, SHA256, PEHASH, IMPHASH
> CIDR rules
> File paths
> MUTEX name
> CVE number

Both USM Anywhere and AlienVault OSSIM users have access to community-powered data from the OTX. A major difference is the delivery.

As an AlienVault OSSIM user, you can connect your instance to OTX to receive updates from researchers you trust and view OTX pulse data for context on threats. When an indicator of compromise identified by the OTX community appears in your environment, the platform will notify you through an alarm. However, it's important to keep in mind that these alarms lack context. They provide a clue about a possible intrusion for you to investigate further, not a complete picture of what happened.

In USM Anywhere, the most recent OTX threat data is baked into your security plan. In addition to their research, the Alien Labs security research team analyzes and validates OTX threat data, which informs the threat intelligence updates this team provides to the USM platform. As a result, your security plan is constantly updated with lessons learned from in-the-wild attacks and thousands of contributors spread all over the world.

Continuous threat intelligence from Alien Labs security research team

Whereas AlienVault OSSIM provides the tools for you to put your threat intelligence research to work, the USM platform's integrated threat intelligence subscription from the Alien Labs security research team eliminates the need for IT teams to spend their limited time conducting their own research. Instead, this team spends countless hours mapping out the different types of attacks and the latest threats, suspicious behavior, vulnerabilities, and exploits they uncover across the entire threat landscape. After collecting and interpreting all this data, using machine and human intelligence, the team turns it into actionable threat intelligence that it delivers to the USM platform as a coordinated set of advanced correlation rules and product updates multiple times per week.

Because AT&T Cybersecurity owns both the data sources and the management platform, the Alien Labs security research team has an understanding of the interactions between the different data types being correlated and analyzed as well as the latest attack techniques. This expertise gets embedded in the USM platform's built-in security controls and integrated threat intelligence, providing you with guidance on emerging threats, regardless of your environment. Because these updates also include context-specific remediation guidance on how to mitigate the threats quickly and effectively, they help to accelerate and simplify threat detection and remediation rather than forcing IT teams to research every alarm to understand how to respond.

Support and documentation

Even the best products require a little assistance from time to time. If security is a business-critical function at your organization, ongoing support is a serious consideration.

AT&T Cybersecurity hosts and moderates community forums for AlienVault OSSIM users and is a resource for anyone looking to have a quick question answered. It's also an excellent place to collaborate with peers on security topics. We also offer user training sessions in the product forum.

AT&T Cybersecurity offers a range of paid support options for USM Anywhere customers in addition to the no-cost collaborative community forums. We provide dedicated phone and email support, as well as free monthly product training webinars. USM Anywhere also includes comprehensive deployment guides, user guides, and knowledgebase articles to help you get the most out of your AT&T Cybersecurity products.

Reports and dashboards

Without an easy way to visualize and interpret your data, it's easy to get lost. Whereas AlienVault OSSIM offers some basic dashboards, USM Anywhere provides a wide range of data visualization capabilities to interpret and communicate the dynamic nature of the threat landscape and the value of the security systems that you have put in place.

For example, the USM platform's intuitive dashboard and analytics interface allow you to view an at-a-glance analysis of top assets and networks affected by discovered vulnerabilities. You can view threats by severity, allowing you to prioritize your efforts better, and quickly drill down to get more information about any particular threat.

Learn more about AlienVault OSSIM:
Download here

Learn more about USM Anywhere:
Download a free trial | Watch the 2-minute overview | Explore our online demo environment

About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer your business to innovate.

AlienVault, AlienApp, AlienApps, USM Appliance, USM Anywhere, USM Central, Open Threat Exchange, OTX, OTX Endpoint Security, AlienVault OSSIM, Unified Security Management, and USM are trademarks of AlienVault and/or its affiliates. Other names may be trademarks of their respective owners.