FEDERATION

A Modern Approach to Managing Multiple Customers with AlienVault USM

In the world of Managed Security Services, Multi-Tenancy is often the default approach to managing the security of multiple subscribers. However, like most things in IT, the default approach is rarely the right choice. Multi-Tenancy has a number of technology challenges, such as maintaining true separation of customers and their data, and creates an unpredictable business model for most MSSPs.

A better approach is Federation, which delivers the same functionality of Multi-Tenancy without the technical and business limitations. AlienVault® Federation treats each of your end customers' deployments as its own autonomous monitoring instance that communicates AlienVault USM Central™—a federation console that centralizes multiple USM Anywhere™ and USM Appliance™ deployments. To understand the technical and business benefits of AlienVault Federation over Multi-Tenancy, we will discuss several facets, including:

- **Cost**
- **Quality of Service**
- **Reliability**
- **Data Management**
- **Privacy / Compliance**

Cost

Cost is always a major consideration in delivering any managed service, with the need to minimize both your up-front and ongoing costs as your subscriber base grows. Traditional approaches to multi-tenancy are on-premises, which requires you to incur significant up-front equipment costs. Regardless of the number of subscribers, you need to invest in a long list of equipment and services: server hardware, network hardware, cabling, license cost, HVAC, and so forth. This model repeats itself as you grow and you approach the capacity limits of your software licenses and / or hardware, requiring you to invest in another round of infrastructure spending.

A significant challenge with Multi-Tenancy is that if you build out your infrastructure too far in advance of your subscriber base, you've invested in unnecessary capacity. At the same time, if you don't build out sufficient capacity to meet demand as you grow, you are limiting sales and potentially degrading user experience by being unable to scale quickly. In other words, Multi-Tenancy requires very accurate forecasting of infrastructure requirements to avoid unnecessary CapEx and OpEx. Even with years of experience, your forecast will be a guess at best because your potential subscribers' needs and environments differ greatly.

With AlienVault Federation, you gain cost **predictability** with a lower up-front fixed cost because of USM Central's capacity to support multiple subscribers. This cost model allows you to maximize ARPU (Average Revenue Per User) by scaling quickly to support a growing subscriber base while minimizing costs. The Federated approach also relieves the pressure to accurately forecast your subscriber profile. It allows you to add subscribers of any size or architecture, meaning you can size and scope each project without having to accurately predict every new subscriber's requirements.

"Whether you have 1 subscriber or 50, the cost of federation with AlienVault remains the same"

Quality of Service

In a Multi-Tenant environment, subscribers share computing resources, which can be both a benefit and a disadvantage to you as the service provider. The benefit is that shared computing resources lower your costs. The disadvantage is that, if one subscriber decides to add new logging sources or experiences a DoS attack, all of the other subscribers in this shared environment will suffer.

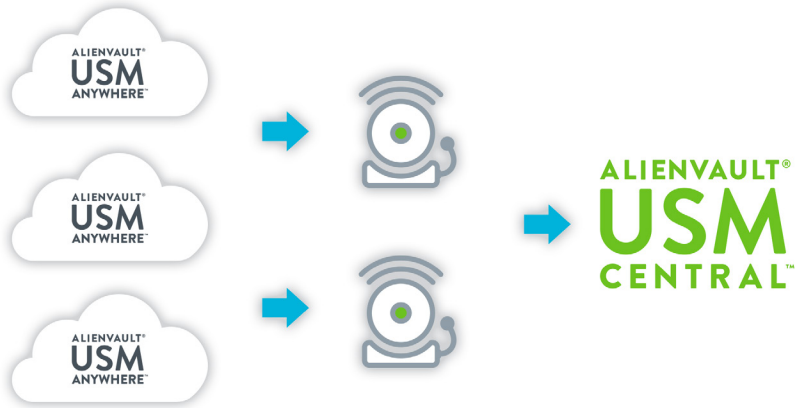
Multi-Tenancy makes your environment a potential single point of failure. Because your Multi-Tenant infrastructure is responsible for threat detection and analysis of all your customers, if you experience a service interruption so will all your customers. Event processing stops, risk assessment stops and any type of alerting you may have stops. The ability to deliver accurate threat information is the core of any MSSP service, and using Multi-Tenancy adds significant risk to the delivery and awareness of that critical threat information.

With Federation, problems experienced by one subscriber remain isolated with that subscriber and allows you to maintain a high QoS (Quality of Service) with your other subscribers. Because the Federated architecture involves individual deployments of USM Anyhwere and USM Appliance that communicate with USM Central, each deployment serves as its own autonomous monitoring instance. Even if the link between you and your subscriber goes down, your subscriber's individual AlienVault USM deployment is still monitoring the network and producing events/alarms. Importantly, you as the MSSP have the ability to log into each AlienVault USM deployment and manage the subscriber's security controls remotely.

Deployment Simplicity

The infrastructure you need to deploy your managed services is an important consideration. Multi-tenant models are typically limited in that they are complicated with high-availability and redundancy requirements that can be difficult to implement.

USM Central provides a SaaS-delivered federation model that is provisioned quickly for you, and only requires that you configure AlienVault USM deployments to communicate with USM Central. This simple approach accelerates your time to monitor your customers, and removes the headache of managing traditional multi-tenancy approaches.



Reliability

MSSPs are highly sensitive to downtime, as any lack of availability or downtime has specific, measurable costs. With Multi-Tenancy, several services must operate with a high degree of uptime for you to achieve your SLAs (Service Level Agreements). Unfortunately, you may not have control over some services, such as data links between sites.

In contrast, an AlienVault Federation deployment reduces your chance of downtime. USM Central is a modern, scalable cloud service that is hosted, maintained, and secured by AlienVault. This eliminates your burden of having to deploy, maintain, update, and secure on-premises federated monitoring software, saving you time, money, and resources.

Data Management

Managing the security of a single environment is always a challenge as you are constantly inundated with events, alarms, false positives, and more. Tracking and prioritizing multiple environments' security events and alarms is a frustrating exercise, especially when the monitoring solution is not designed to work in this type of architecture.

Unfortunately, Multi-Tenancy can add to that frustration at the management level and make your job even more difficult. Keeping track of what alarms belong to which subscriber and which subscriber has access to what assets can distract you from focusing on the task at hand: securing your subscribers' environments.

Also, with a Multi-Tenant approach, you have to worry about subscriber cross-contamination or leakage of data. This can be due to misconfiguration of the software, data tagged incorrectly, or even product malfunctions at the UI level.

In the AlienVault Federated model, because each subscriber has their own dedicated AlienVault USM deployment and data storage, the chance of any accidental data leakage is virtually non-existent. Federation eliminates the need to manage different subscribers' data, and allows you to deliver the managed security your customers expect.

Data Privacy / Compliance

Maintaining continuous compliance with standards like PCI DSS and HIPAA is a challenge for your subscribers. With the centralization of all security event data in your SOC, you must maintain compliance of that environment.

USM Central has been attested as compliant to PCI DSS, SOC 2, and HIPAA, giving assurance in our ability to secure the confidentiality, integrity, and availability of your subscribers' data within USM Central.

Co-Managed Services

Some subscribers request co-managed services as a way to have some continued oversight into their deployment and security posture, and to be able to run reports on demand. To offer this service with a Multi-Tenant architecture, you would be required to grant access to your environment and write custom "portals" for your subscribers to use, putting your environment at higher risk of compromise.

With AlienVault Federation, you can grant a subscriber limited access to their individual AlienVault USM deployment to achieve the same functionality. No complicated permissions lists, no custom code, and no risk to your environment.

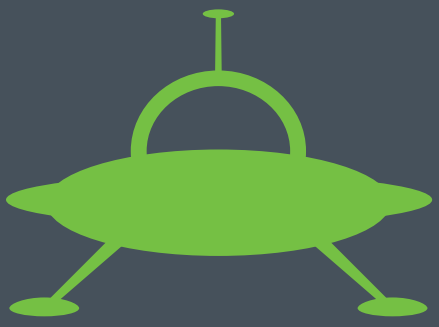
AlienVault Federation: The Better Approach

AlienVault Federation architecture offers a number of advantages over a Multi-Tenant approach, including lower costs, greater scalability, and easier management. Your predictable initial and incremental costs are more manageable, your subscribers are not competing for resources as business grows, and you don't have to predict the future with your equipment purchases.

The advantage of the AlienVault USM Federated architecture include:

- **Cost** - The low startup cost model of the AlienVault USM Federated architecture enables you to minimize your costs while growing your subscriber base
- **Quality of Service** - AlienVault 's Federated architecture is designed to isolate and prevent any issues affecting one of your subscribers to affect the QoS delivered to the rest of your subscribers.
- **Reliability** – The AlienVault USM platform is designed to support a Federated architecture and deliver advanced threat detectionwithout the concern of having to manage the reliability or uptime of USM Central, a cloud service.
- **Data Management** - With each subscriber having their own dedicated AlienVault USM deployment and data storage the chance of any accidental data leakage under the AlienVault Federation model is virtually non-existent.
- **Data Privacy / Compliance** - AlienVault's Federated architecture helps you to maintain continuous compliance with PCI DSS, HIPAA, and more.

With AlienVault USM deployed in a Federated architecture, you can provide an exceptional managed security solution at a competitive cost. AlienVault USM accelerates and simplifies the complicated task of monitoring the security of your subscriber's environment.



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.

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