Xsuite for Amazon Web Services Management APIs

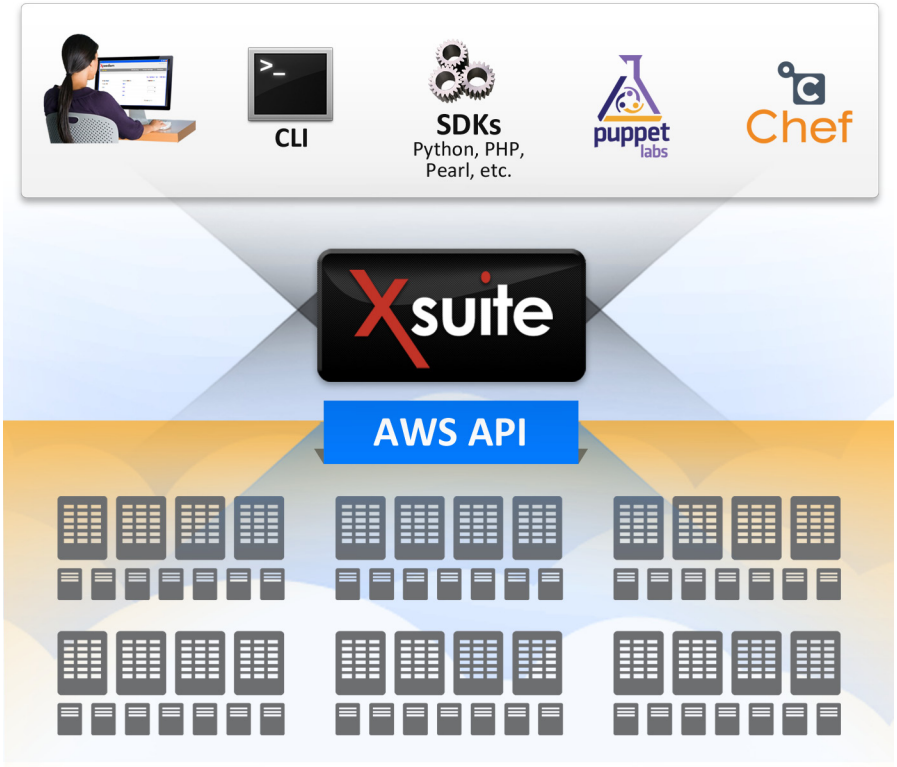
Privileged Identity Management for the Hybrid Cloud

Xsuite for Amazon Web Services Management APIs

Xceedium Xsuite® is the first and only privileged identity management solution designed specifically to support the Amazon Web Services environment. Xsuite for Amazon Web Services Management APIs extends that protection to the powerful application programing interfaces used to automate administration and operation of the AWS environment. Xsuite provides a full audit trail and session recordings of privileged access to AWS Management APIs, enforces separation of duties, provides full password and credential management, and enables a single point of privileged identity management for all of AWS and the rest of the hybrid cloud.

In many organizations, cloud automation requirements prompt administrators to bypass the manual management console to interact directly with the comprehensive set of management APIs provided by Amazon Web Services. Management APIs offer direct access to AWS administrative and operational functions through the command line, via programs developed using the library of software development kits supported by Amazon, and through automated configuration management systems like Puppet and Chef. By providing full access to AWS management capabilities, these APIs represent a sensitive asset that must be carefully managed with respect to privileged access.

Secure Automated Operations and Administration



Xsuite for AWS Management APIs protects infrastructure, enabling secure automated operations and management from the command line, configuration management tools like Chef and Puppet, and via a wide range of SDKs.

Xsuite AWS Management API Proxy Protections

Role-based privileged access control & single sign-on for both programmatic and manual AWS API Access. Xsuite enables full, federated credential provisioning for access to the AWS public, government, and VPC clouds. As is the case with manual access to management consoles, it's all too common for organizations to share a single set of credentials for all administrative access to cloud management APIs. With Xsuite's AWS API Proxy, users are issued individual credentials that only work with the proxy. Organizations know who issued manual or programmatic API calls without having to add each user to the AWS IAM system. And because Xsuite maintains control over direct interactions with AWS, users can't bypass access controls and audit.

Xsuite for Amazon Web Services Management APIs

Full Bi-directional Audit Trail and Session Recording across all API Access

Providing a level of real-time visibility into API-based access and operations unavailable to AWS API users. This audit trail proves invaluable in understanding what's happening, from a privileged access standpoint, within the cloud, as well as providing the forensic details needed to investigate security incidents or questionable activity. Xsuite logs both calls and requests made to AWS, as well as responses for subsequent review. Logs can easily be reviewed using built-in integration with Splunk.

Separation of duties for the AWS API Console Interface

Xsuite implements a centralized API Policy Manager that enforces role-based access controls for all API access via a proxy. Xsuite ensures individuals–and the scripts, programs, and tools operating on their behalf–can only execute the tasks expressly authorized in policies and roles.

Password and Access Key Management

Password and access key management, including vaulting and lifecycle management of all privileged user credentials for AWS REST-based console access. As is the case with virtually all application-to-application privileged credential use, it's difficult, if not impossible, to effectively manage privileged user credentials. Key pairs are hard-coded and shared among multiple individuals. Changing those credentials becomes a configuration management task of Herculean proportions.

It's just too much work–so organizations live with the risk of widely exposed, infrequently changed, and often shared credentials. Xsuite's lifecycle credential management capabilities protect credentials within a vault and enable rotation. Actual interactions with AWS are performed using ephemeral keys, created by Xsuite following validation of the key pair presented by or on behalf of a user.

Single Point of Privileged Access Control, Monitoring, and Audit For AWS

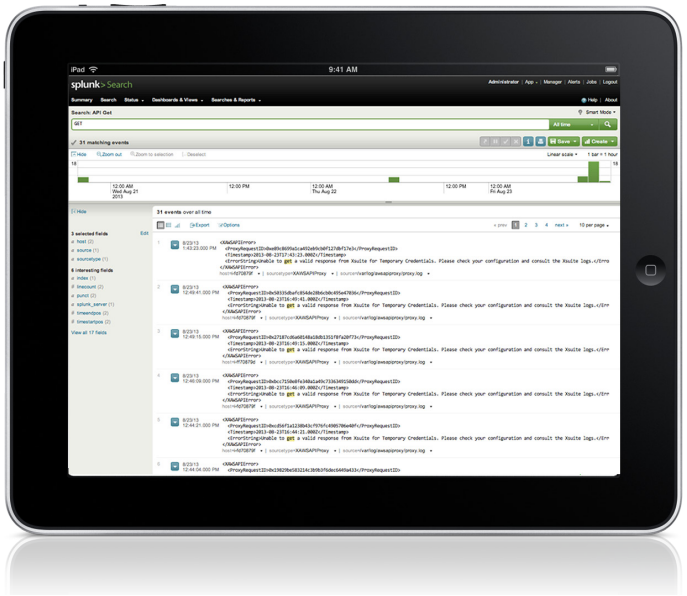
Xsuite provides a single policy store for privileged users across the hybrid cloud. So administrators and auditors gain access to a single point of control for privileged users, across all of Amazon Web Services, as well as virtualized infrastructure, online services, and the physical data center.

Xceedium provides privileged identity management and controls administrator access across the entire hybrid cloud. Xceedium's Xsuite reduces the risks privileged users and unprotected credentials pose to systems and data. Xsuite ensures consistent policies, management, monitoring, and control of privileged users across traditional data centers, virtualized infrastructure, and public/ private clouds.

amazon web services | Partner Network

ADVANCED TECHNOLOGY PARTNER

Xsuite's AWS Management API protection generates comprehensive records of all API activity, making troubleshooting and incident investigation easier. Log records can be viewed in management tools like Splunk.



Xceedium

www.xceedium.com

 | 2214 Rock Hill Road, Suite 100 , Herndon, VA 20170 | +1 (877) 636-5803