Privileged Account Security Service Overview

Trusted partner for your **Digital Journey**

Atos

Service Overview

Atos Privileged Account Security (PAS) provides the strongest protection of privileged accounts, including their abuse by malware and human error. This service is unique in its ability to analyze user and account behavior to detect, alert and respond to critical credential thefts.

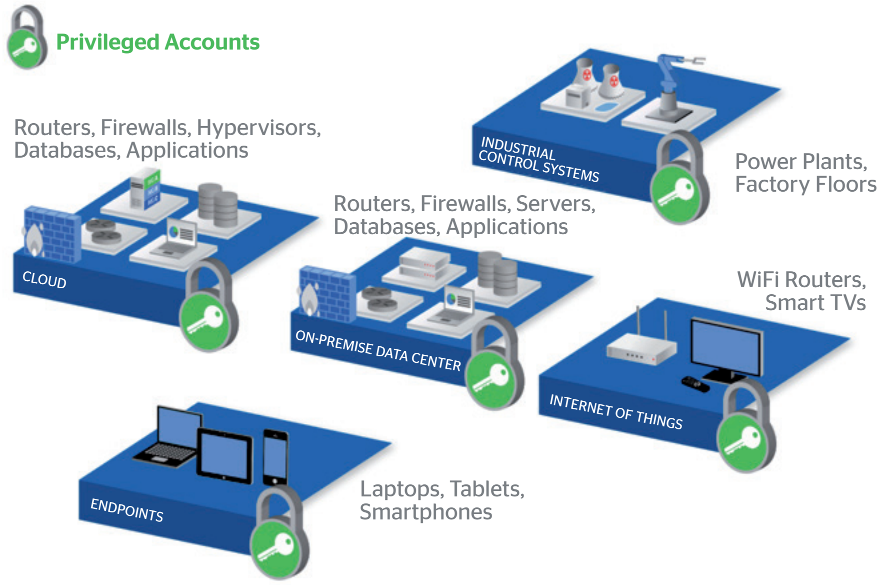
Stolen credentials are implicated in an extremely large number of breaches. Indeed, acquiring credentials is the purpose of many intrusions and phishing scams with the stolen credentials being used to access additional systems. While any user credentials are useful to hackers, the 'keys to the kingdom' are privileged user credentials. These credentials are used to access everything from credit card data to human resources information to infrastructure hardware and more. PAS is a particularly relevant service today given the prevalence of contractors, vendors, and contingent workers all of whom may need to be given occasional access to important company assets.

A privileged account is a special account that provides elevated, non-restrictive access to a system that non-privileged user accounts do not have access to.

These accounts are designed to be used by system administrators to deploy and manage IT technology, like operating systems, network devices and applications. They provide access to just about everything important.

Since privileged accounts can be virtually found on every system – see diagram above – they are a main target for attackers when trying to get access to information within a company.

In addition to granting or denying privileged access to systems, PAS also monitors and audits access. This can be crucial in demonstrating compliance, forensic investigations, post hoc analysis of attacks and data loss.


Privileged Accounts
Routers, Firewalls, Hypervisors, Databases, Applications
CLOUD
INDUSTRIAL CONTROL SYSTEMS
Power Plants, Factory Floors
Routers, Firewalls, Servers, Databases, Applications
ON-PREMISE DATA CENTER
WiFi Routers, Smart TVs
INTERNET OF THINGS
ENDPOINTS
Laptops, Tablets, Smartphones

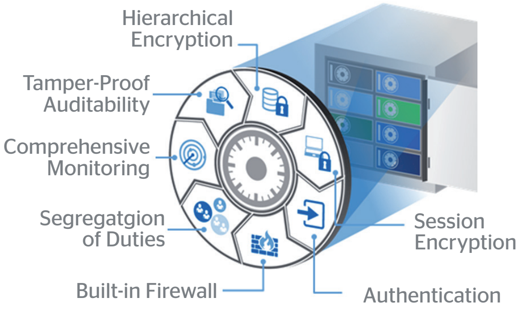
Features

Atos' solution has a variety of features that make it the ideal access management service for your company, including full-time employees, contractors and vendors who may need occasional access to important assets. Notable features include:

1. It is the most complete solution for end-to-end protection of all privileged accounts, backed by the market leader in PAS software
2. Aids in protection against 1,000,000+ malware variants, alerting on suspicious activity and the misuse of privileged access
3. Enable authorized users to elevate privileges when needed for business purposes, allowing organizations to strengthen security while keeping IT users productive

The service consists of a number of modules that an organization can select depending upon their requirements.

- **Privileged Session Manager:** Isolate, monitor and control privileged sessions on critical systems including Unix and Windows-based systems, databases and virtual machines. It provides real-time monitoring, enabling security teams to track user activity and detect suspicious events in real-time. This feature also provides remote session termination to immediately terminate suspicious privileged sessions.
- **The Enterprise Password Vault:** enables discovery, security, rotation and control of privileged account passwords used to access systems throughout the enterprise IT environment. (see graphic below)
- **Privileged Session Manager With Recording** provides text and DVR-like recording and playback of individual sessions. It offers searchable detailed session audit logs and video recordings, enabling security teams to pinpoint the moment an incident started, understand how the incident began, and quickly assess any damage.
- **On-Demand Privileges Manager:** Control and monitor the Unix commands super-users can run. This reduces the usage of privileged rights within an enterprise and enforces least privilege policies for super-user rights.
- **Privileged Threat Analytics:** Profiles and analyzes individual privileged user behavior and creates prioritized alerts when abnormal activity is detected. When integrated with Enterprise Password Vault (EPV) it can initiate password rotation when there is suspected credential theft, and can be integrated with the Privileged Session Manager to automatically terminate sessions when there is abnormal activity.



Privileged Credentials Stored in a Secured Vault

This Atos service offering is truly unique not only in its wide PAS capabilities but the integration of this service into Atos SIEM. SIEM solutions are widely used to collect, analyze and alert on network activity. Atos SIEM, however, is more robust because it is integrated not only into network activity but also into endpoints, gateways, threat feeds, and remediation tools. The Atos SIEM uses OpenDXL which means that any product that supports OpenDXL can be added to the security infrastructure, creating a scalable and robust risk management ecosystem.

Atos is also able to enhance the information provided by SIEM solutions through a two-way integration with optional privileged user threat analytics. Privileged account activity on systems can be collected by the SIEM and fed into threat analytics. This data is processed by a set of complex algorithms and correlated with privileged user information. The analytics engine then detects anomalous activity and generates targeted, actionable alerts for high-risk incidents. Completing the integration, the alerts can then be sent to the SIEM solution, enabling an organization to efficiently prioritize and respond to the most serious threats.

Benefits

Today's threats require a flexible yet secure way to manage superuser and privileged user credentials. As mentioned, privileged user credentials are one of the most targeted assets for hackers. One of the main benefits of Atos Privileged Account Security service is the reduction of risks organizations face from hackers. The risks organizations face makes a PAS service a necessity. As shown in the diagram above, privileged user credentials are stored in a highly secure vault.

Additional benefits of the Atos PAS service include:

- Improving security with dynamic credentials without increasing the burden on IT administrators, who may be overloaded with a variety of security requirements and demands. This frees up scarce resources to work on other risk related matters.
- Automation of password changes for privileged accounts, reducing help desk calls and minimizing loss productivity due to forgotten passwords.
- Monitoring of privileged user activity to create a full audit trail to identify individual actions. This can vastly improve an organization's ability to successfully conduct forensics and meet compliance requirements.
- A full audit trail, making it easy to report on activity and reduce the cost of both compliance and audits.contractors, vendors, and contingent workers all of whom may need to be given occasional access to important company assets.

Technical Overview

Delivery Scope and Implementation

The Privileged Account Security service is modular and offers various capabilities depending upon customer need. As a group, the modules provide the comprehensive protection, monitoring, detection, and reporting that enable organizations to thwart the malicious insider and advanced attacker.

The Atos PAS service supports a very wide variety of technologies and vendors, including:

- **Security appliances** such as CheckPoint, Cisco, IBM, RSA Authentication Manager, Juniper, and more
- **Public Cloud Environments:** Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform
- **Network devices:** Cisco, Juniper, 3com, F5 and more
- **Applications:** SAP, WebSphere, WebLogic, JBOSS, Tomcat, and more

Due to the potential complexity of PAS deployments, the service setup is performed in a phased approach with a clear split between the setup of the service itself and the onboarding of the privileged users and the target systems / environments. Project templates and best practices will be made available to optimize the overall project throughput time.

Why Atos for PAS?

The Atos PAS solution is unique in the marketplace due to both its wide capabilities and also its integration into the Atos SIEM. Both of these capabilities are of paramount importance in combatting today's ransomware and insider threats. Atos PAS service is built upon the best IAM solutions available in the market. Atos combines this with market-leading SIEM and endpoint tools.

Atos is a €13B company, recognized globally by market analysts and customers as a Leader in Identity & Access Management. Atos is one of the market leaders in Managed Security Services worldwide.

Atos has more than 20 years of experience in Identity & Access Management with a wide range of implementations in multiple environments and industries:

- More than 1000 IAM customer implementations worldwide
- A significant number of very large customers for which Atos manages more than 12 million Identities.
- More than 500 IAM specialists worldwide with in-depth knowledge and experience in IAM products, processes and services.

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of € 13 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together