Staying on top of privileged account security and compliance

WM Gruppe fortifies server admin accounts while saving hours of work using Safeguard

ONE IDENTITY by Quest

WM GRUPPE

Country: **Germany**

Employees: **450**

Industry: **Financial Service Media**

Website: **www.wmgruppe.de**

Cybersecurity is of particular concern for the financial services industry because, well, as everyone knows, "that's where the money is." In Germany, the Bank Regulatory Requirements for IT [Bankaufsichtliche Anforderungen an die IT] (BAIT), is helping tackle internet crime by setting down guidelines on IT governance among banks.

While WM Gruppe isn't a bank, it provides banks and other financial services companies with data on financial markets and instruments. And with its systems hooking up to those of customers via application programming interfaces (API), it must ensure its cybersecurity is as robust as that of its clients.

Time for privileged accounts control to step up

As such, WM Gruppe wanted to improve its position around privileged account management (PAM). Privileged accounts are known to be vulnerable to attack, resulting in catastrophic consequences when hacked. PAM processes in WM Gruppe were home-grown, meaning they'd evolved over time as the company expanded.

Unfortunately, PAM processes at WM Gruppe were manual and time-consuming to operate, posing security risk across its 800 applications

Challenges

With regulatory requirements increasing, WM Gruppe wanted to reinforce privileged account management (PAM) to counter cybercriminals while improving operational efficiency.

Solutions

The company implemented One Identity Safeguard for Privileged Passwords, closing any potential holes in PAM processes while saving hours of work through automation and improving auditing capabilities.

Benefits

- Improves PAM processes by 100%, making governance easier
- Saves time with PAM automating around 80% of tasks
- Gains transparency and control over access like never before

and multiple privileged accounts. It was easy for procedures like password changes to be delayed if a member of the IT infrastructure team responsible for making the changes was out-of-office or otherwise engaged. Plus, reporting on who had access to what servers and applications, and when, was a constant concern due to data inaccessibility.

A solution that fills all the PAM gaps

WM Gruppe looked for a PAM solution as part of a wider cybersecurity review across the entire organization. It chose One Identity Safeguard for Privileged Passwords for a couple of key reasons. It fully automated PAM processes, removing password management, and it made PAM fully auditable. Comments Frank, "With One Identity Safeguard could simply strengthen privileged account controls and place ourselves on a better footing."

The company worked closely with One Identity Partner Patecco, which supported WM Gruppe with the initial deployment of Safeguard. Frank comments, "The implementation was very smooth, and although we had a lot of IT projects at that time running in parallel, Patecco did a great job of supporting us. The communication was excellent, and I had a lot of good feedback across my team."

Saves hours of work and increases protection

With Safeguard in place, WM Gruppe has resolved any challenges around PAM, strengthening a key part of its cybersecurity armor. Highlights for Frank are the PAM automation which saves many hours of work and recording privileged sessions of administrators, which makes governance easier . Also, using the workflow engine in Safeguard, Frank has set an overnight password expiration policy, which drastically reduces the window of opportunity if a password gets hacked.

Delivers a 100% improvement

The switch to Safeguard has imposed a "greater level of discipline" among IT teams, according to Frank. They must plan for scheduled maintenance; aware the workflow engine enforces processes, such as approvals, that need to be adhered to for work to proceed. "Everything is more transparent and controlled with Safeguard," he says.

Frank concludes, "We've seen a 100 percent improvement in PAM using Safeguard. We have raised PAM to a new level without increasing our workloads whatsoever."

> **"With One Identity Safeguard could simply strengthen privileged account controls, and place ourselves on a better footing."**
>
> *Felix Frank,*
> *Team Leader for IT Administration,*
> *WM Gruppe*

About One Identity

One Identity, a Quest Software business, helps organizations achieve an identity-centric security strategy with a uniquely broad and integrated portfolio of identity management offerings developed with a cloud-first strategy including AD account lifecycle management, identity governance and administration and privileged access management. One Identity empowers organizations to reach their full potential, unimpeded by security, yet safeguarded against threats without compromise regardless of how they choose to consume the services. One Identity and its approach is trusted by customers globally, where more than 5,000 organizations worldwide depend on One Identity solutions to manage more than 250 million identities, enhancing their agility and efficiency while securing access to their systems and data – on-prem, cloud or hybrid. For more information, visit www.oneidentity.com.

ONE IDENTITY by Quest