Osirium Case Study

thinkmoney

Company: UK Retail Bank
Location: Manchester, UK
Industry: Finance
Osirium solution: Osirium PAM

Challenge

- Significantly improve management control and governance
- Protect against insider threat and sophisticated cyber attacks
- Address security challenges across a wide range of databases, servers, network and security devices

Solution

- Minimise access to privileged services using privileged access management and automation with Osirium PAM

The Challenge

thinkmoney are a new generation UK retail bank founded in 2001. It wanted to transform its IT platform to support its key products: Current Account, Personal Loan and Travel Card. It was also looking to significantly improve management control and governance of privileged access to critical IT systems.

Two specific risk areas were considered:

- Insider threats: Where a malicious insider obtains super-user or administrative passwords - through social-engineering, key-logging, or the malpractice of password sharing, to mitigate internal attacks, compromising confidential data or sabotaging systems.
- Sophisticated cyber-attacks: Where an external attacker gains covert access to the network and captures super-user or administrative passwords with which to carry out an attack.

The regulator suggests that it is good practice to implement 'powerful administrator passwords to additional controls'; entrusting those passwords to the minimum number of people, ensuring that use and access is always logged and regularly reviewed, and following up any exceptions or anomalies. This therefore became a firm project goal.

A relatively small but highly secure subsystem was required. It needed to encompass 50 multi-platform servers, backend databases, firewalls and other network and security devices.

> *"within an hour we were proving our use cases"*

The Approach Taken

thinkmoney's team arranged a proof of concept programme with Osirium and other comparable products. After thoroughly researching the market for privileged account management (PAM) they found that Osirium was the best fit, not only for privilege access management but also for task automation. thinkmoney found that Osirium deployment was simple and fast; "within an hour we were proving our use cases," said thinkmoney.

Aware that thinkmoney needed the best security, the team also knew that ensuring the best security aids workflow efficiency. Task automation is used to map business workflow tasks to users with non-privileged accounts. This means that tasks are secure, repeatable and properly audited. "We realised that the beauty of task automation was twofold," they said. "First, privileges need not be granted in the first place, and second, the tasks are consistent and audited."

The Approach Taken - Continued

Osirium PAM is used to provide RDP single sign-on (SSO) to all the servers, Web SSO to management consoles, SSO to the database servers, and SSH SSO to the firewalls.
In SSO terms, not only can Osirium PAM cover the simple RDP and SSH requirements, but also the more complex HTTP/HTTPS requirements. thinkmoney then took it a step further by also providing SSO and credential isolation for the critical database servers.

The team then began to engage Osirium on the tightly integrated cases where devices use authentication services, such as Active Directory. The Osirium 'Device Group Separation' function was utilised to ensure that team members could not have concurrent connections mixed between live and development environments.

Benefits and Next Steps

"Osirium PAM makes it obvious who can access what, where and when. Their interface is simple and intuitive to use, delivering quick results, but it also has great depth and quality," said thinkmoney. "Our team love the look of the analytics and management pages and in day to day use they've proven really useful – they definitely show us when and how work gets done. I like the way I can see exactly what Osirium costs and can chose exactly where to deploy it for the greatest business benefit".

In addition to the core protection of credentials, thinkmoney can now delegate tasks to the most business appropriate users without having to worry about skill, training, or privilege escalation issues.

> *"Osirium PAM makes it obvious who can access what, where and when."*

Speaking of Osirium's session recording, they commented, "it's a great deterrent against the insider threat, and replaying a session from a support incident helped us solve an issue that would previously have been near on impossible to resolve, so that was a great benefit".

Summing up their experience with Osirium PAM, thinkmoney said, "these days Osirium is part of our workflow landscape. Initially, we had a small estate on the Osirium platform, but now we consider all devices and applications as 'Osirium-able'. We feel that they are an extended part of our team. We can point Osirium at new devices and applications, and they can customise tasks to meet our business procedures."