CASE STUDY

Keeping IT Secure with Osirium PAM

How a leading university adopted Osirium PAM

OSIRIUM

OSIRIUM **PAM**

Keeping University IT Secure with Osirium PAM

The Challenge

The Higher Education community is a prime target for cyber-attack. According to the Sonic Wall Cyber Threat 2021 report, an above average 22.5% of education establishments were attacked each month.

Universities can be more challenging to secure than other organizations because they try to balance security and business functionality with the openness of a university where everyone is there to share information. Back-office systems are much like any sizeable business except that many of the systems have evolved over decades. For example, email was deployed across universities before being generally available, over 40 years ago.

This university, a member of the Russell Group with a history dating back to first half of the 19th century, found they had significant risks due to their Active Directory (AD) infrastructure. They had too many users with Domain Admin role (effectively, users with “god-like” power – the ideal target for attackers) and poor controls over admin credentials.

When the current cybersecurity manager joined the university in 2014, he made privileged access management (PAM) a priority. In parallel to implementing PAM, he knew they also had to clean up the AD infrastructure. “There was reluctance in the AD team because of the scale of the task, and it was not a priority for IT in the University. But that all changed when we suffered a cyber-attack” said the Cybersecurity Manager.

Company:	Leading UK University
Location:	UK
Industry:	Higher Education
Solution:	Osirium PAM

Challenge

- Managing administrator accounts on IT systems
- Enforcing account credential management
- Implement security without impacting staff productivity

Solution

- Ensure all admin access is via Osirium PAM

> **Looking back, we should have just enforced PAM in the first place**
>
> Cybersecurity Manager

The Approach Taken

The university had been looking for a PAM solution for some time and already had a test installation of Osirium PAM. As is usual in the public sector, they started a tender process to choose a PAM partner.

Osirium PAM scored highly, showing not just good functionality, but good value for money. Crucial in the public sector.

Key to that good value is that the Osirium pricing is based on the number of devices being managed, not users, unlike many competitors. At the time of writing, there are approximately 150 users, possibly growing to 200, with access to over 500 devices.

“Looking back, regardless of the price, it was still the right decision” they say. Expanding further, “the Osirium team have been great. Very knowledgeable and very helpful.”

> **Regardless of the price, it was the right decision**
> Cybersecurity Manager

The Approach Taken Continued

The plans took a major change following the cyber-attack.

An initial deployment of Osirium PAM was scheduled, but before the project could start, the attack struck. “In a way, it was a godsend. It woke everyone up, we got their attention” says the Cybersecurity Manager.

External consultants, brought in as part of the incident response plan, highlighted the problems with the AD infrastructure. Admin credentials weren’t being actively managed. With some accounts being many years old, there was no visibility or control.

Following the attack, the university completely restructured their AD infrastructure and accelerated their PAM plans to protect all devices, not just those in the original plan.

They have implemented a hybrid model, where most admins access devices via Osirium PAM, but a very few senior administrators have access to Privileged Access Workstations (PAWS), following the Microsoft model, when they need “god-like” accounts.

Previously getting attention was difficult. Traditionally PAM can be seen as an inhibitor to admin productivity. “Looking back, we should have just enforced PAM in the first place once we were sure it worked. We had to be quite tough with people. Now we have very good synergy between the AD and PAM teams, and it feels like every day, there’s someone else who wants to use PAM.”

> **The Osirium team have been great. Very knowledgeable and very helpful**
> Cybersecurity Manager

Looking Forward

A big issue in academia is Cyber Essentials (CE). Many organisations are adopting PAM to control and audit privileged access as required by CE. One of the recently updated requirements in CE is Multi-Factor Authentication (MFA) which is a standard feature in Osirium PAM, but it also integrates with existing infrastructure, which was the route taken by this university. Another team is considering adopting Osirium’s Automation solution, Privileged Process Automation (PPA), to securely automate common IT processes.

About Osirium

Osirium is the UK's innovator in Privileged Access Management. Founded in 2008 and with its HQ in the UK, near Reading, Osirium's management team has been helping thousands of organisations over the past 25 years protect and transform their IT security services.

The Osirium team have intelligently combined the latest generation of Cyber-Security and Automation technology to create the world's first, built-for-purpose, Privileged Protection and Task Automation solution.

Tried and tested by some of the world's biggest brands and public-sector bodies, Osirium helps organisations drive down Business Risks, Operational Costs and meet IT Compliance.

OSIRIUM

Theale Court, 11-13 High Street, Theale, Reading, Berkshire, RG7 5AH
+44 (0) 118 324 2444, info@osirium.com, **osirium.com**