CASE STUDY

University of Reading and Osirium PAM

Managing vendor access to protect IT systems

OSIRIUM

University of Reading

University of Reading and Osirium PAM case study

The Challenge

The University of Reading is one of the leading universities in the UK (ranked in the top 30 UK universities in world rankings). With over 18,000 students and 4,500 staff spread over three campus locations, a relatively small team of about 20 is responsible for keeping all student and infrastructure systems running and secure. They manage on-premises data centres, networks, cloud services in Azure, telephony, Microsoft 365 and more.

Many business systems are supported externally by vendors/partners. The University used to grant access to these suppliers via Virtual Private Network (VPN) connections, but that didn't provide visibility and control over who could access which systems and what they did while connected.

When Kevin Mortimer, Head of Operations, Digital Technology Services Department, joined the University in 2017, he prioritised getting control over vendor access.

Company: University of Reading
Location: Reading, UK
Industry: Higher Education
Solution: Osirium PAM

CHALLENGE

- **Managing supplier and third-party access to IT systems**
- **Protect critical systems with a limited team**
- **Provide audits of who had access, where and when**

SOLUTION

- **Ensure all vendor access is via Osirium PAM and record all sessions**

The Approach Taken

Mortimer had the experience of privileged access management (PAM) at a previous employer. He set out to find a PAM solution that would be easy to adopt and manage for the University's complex infrastructure.

After reviewing several vendors offerings, he quickly focused on Osirium PAM. "As we were introducing PAM for the first time, we wanted to ensure it would be straightforward to implement and use as possible. There are bigger brands in the market, but they are considerably more complex and expensive. From a capability and cost point of view, Osirium came top of the contenders." says Mortimer.

Implementation started with a small set of vendors onboarded with PAM and then expanded usage. That's a typical deployment pattern with Osirium PAM and an excellent way to show early benefits without large, all-encompassing projects. Now, almost all vendors can only access systems via PAM.

Administrator accounts on the target systems and devices are protected because the vendor never has direct access and can never discover the administrator credentials. Access can also be granted for specific periods, for example, only during working or non-working hours. Occasionally, access may be set up for a vendor for a short period around a specific project, for instance, during a recent upgrade to the campus CCTV system.

Since adopting Osirium PAM, whenever any issues were found, the University worked closely with the Osirium support team have been able to do everything they wanted to do, and now PAM "just ticks over and we have one less treat actor to focus on."

> *"As we were introducing PAM for the first time, we wanted to ensure it would be straightforward to implement and use as possible. There are bigger brands in the market, but they are considerably more complex and expensive. From a capability and cost point of view, Osirium came top of the contenders."*

Benefits and Next Steps

Almost all suppliers now use Osirium PAM, and the University has complete visibility into who from the vendor accesses their systems. Using the Osirium PAM MAP server, they can also control which applications are used. As sessions are recorded, the University has a complete record of exactly what the vendor did while connected, if they ever need to investigate an incident. "PAM is like an insurance policy you hope to never need to use in that regard," says Mortimer.

For vendors, there's nothing to install locally, and, if appropriate, they can let multiple staff members share access to the account on the university system.

Looking forward, endpoint management is becoming a priority. Many professional and academic staff want local admin rights to install and run their applications, but that opens a potential entry point for attackers. The University is interested in Osirium Privileged Endpoint Management (PEM), which allows approved applications to run with elevated privileges without local admin rights.

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**