

CASE STUDY

TalkTalk and Osirium PAM, PPA and PEM

How a leading UK telecommunications company
adopted Osirium PAM, PPA and PEM



TalkTalk

TalkTalk and Osirium PAM, PEM and PPA

The Challenge

The Telecommunications (Security) Act 2021 (TSA) aims to improve the resilience and security of telecoms infrastructure to ensure it maintains availability during emergencies such as natural disasters and cyber security events. The TSA includes the ability of the UK Government, in liaison with the National Cyber Security Centre (NCSC), to make regulations and recommendations that improve cybersecurity and resilience within telecommunications providers.




The recommendations are currently in final draft format and the telecoms industry has worked with the National Cyber Security Centre (NCSC) to identify best practices and the implications on their security strategies to fulfil the requirements of the TSA. Many of the recommendations being considered for TSA compliance include management of privileged access to services and devices that are components of critical national infrastructure. TalkTalk started the process of finding a suitable provider of privileged access management (PAM) solutions to improve security in this area.

“

The Osirium architecture was a lot simpler. Clearly, this was a single solution from the vendor, not a set of tools acquired over time that haven't been fully integrated

Once they started managing access to IT systems, they saw that user account management would be a critical capability. They had to ensure that the right people were members of the right groups, that access permissions were correctly linked to these groups for new starters and also updated when staff moved between teams or left the company. As a manual task, access management is time-consuming and open to potential errors.

TalkTalk

Company	Leading UK telecommunications and broadband provider.
Industry	Telecoms
Location	United Kingdom
Challenge	<ul style="list-style-type: none">• Address cyber-resilience for critical national infrastructure requirements• Reduce workload, and improve the accuracy of the joiners, movers, leavers process• Reduce potential attack surface without impacting developers and engineers
Solution	 OSIRIUM PAM  OSIRIUM PPA  OSIRIUM PEM

User workstations are the largest potential entry point for attackers as there are so many laptops and desktop systems to manage. TalkTalk undertook a desktop modernisation programme part of which was to confirm that users didn't have local admin rights. Some teams, especially software developers, have legitimate reasons for temporarily elevated rights, so TalkTalk needed a solution that didn't interfere with their work but still provided control over how these powerful rights were used.

The Solution

Securing Critical Systems with PAM

Nomios are a longstanding TalkTalk Security Partner and worked with the TalkTalk Security Architecture team to evaluate the PAM market space. An RFI was issued to 10 potential PAM suppliers, whittled down to three for an RFP and eventually a lab test of two preferred vendors. Osirium PAM performed well in comparison to the competition, however, the inclusion of Task Automation was a clear differentiator as no other vendor offers it.

Brent Alldred, Principal Security Architect at TalkTalk, explained, *“The Osirium architecture was a lot simpler. Clearly, this was a single solution from the vendor, not a set of tools acquired over time that haven’t been fully integrated.”*

He continued, *“Of course, it was also helpful that the price point was right! Osirium were flexible in working with us to define the right solution.”* While the TSA regulations and scope are not finalised, Osirium PAM offers a package that allows for flexibility and predictability of costs.

Nomios Professional Services Consultants worked with TalkTalk’s Principal Security Architect to finalise and document the deployment of PAM (and later PPA) in their lab environment.

Automating User Account Management

Osirium PAM was quickly integrated with the user identity platforms. It became clear that user management would need to be a priority as ongoing staff changes significantly impact the Access Control team. Osirium Privileged Process Automation (PPA) looked like the ideal solution.

Although PPA can be standalone, TalkTalk has used its integration capabilities to connect PPA with its HR system, which is the “source of truth” for employees. When the HR team adds a new starter, the necessary user accounts, and appropriate groups are created by PPA.

Similarly, the identity store is automatically updated when someone moves between teams or leaves the organisation. This reduces the load on the Access Control team and improves security. *“Manually creating users and updating groups is time-consuming, and errors can occur. The last thing you want is someone to have too much access by being in the wrong group or not having enough access to do their work,”* said Brent.



Removing Local Admin Rights

Another strand of cybersecurity improvement included updating user workstations – laptops and desktops. It also meant removing Local Admin rights from some teams that historically had these enabled. *“The fewer people that have privileged access, the better,”* said Brent.

Some user groups, such as software developers, still need privileged access to do their work, for example, developers that require administrative level changes to connect to various development environments.

With their experience working with Osirium PAM and Automation, Privileged Endpoint Management (PEM) came onto TalkTalk’s radar. Other options were considered, but they could be expensive (e.g., duplicating hardware to have secure “jump boxes”). No solution was as focused on solving this particular challenge. PEM was a clear choice because of the experience with Osirium, the low maintenance overhead, and its realistic pricing.

By running PEM in “Learning mode,” TalkTalk can roll out PEM team-by-team and create policies for each team before turning on enforcement mode to reduce any impact on the user’s work.

Looking Forward

Brent said, *“Working with Osirium has been very good. Osirium has always been very quick to respond to questions. Osirium Professional Services have always been quick to help when we’ve asked for it.”* It also helped that Osirium are UK based and smaller. TalkTalk found more prominent, US-based vendors to be much more bureaucratic and hence less agile.

The work never stops improving cyber security and resilience in critical national infrastructure. The future evolution of TSA may include a requirement for programmatic updates to network infrastructure by 2025, which could be a good fit for Osirium Automation.

“Working with the TalkTalk team over several years has shown how important privileged access security is for securing critical infrastructure. But it has also shown the business benefits of looking beyond the traditional view of security systems as blocking access. Using modern, secure automation can transform how a business operates, as seen in their use of Automation for access management,” said Catherine Jamieson, Strategic Accounts Manager at Osirium.

“

Osirium Professional Services have always been quick to help when we’ve asked for it

“As a longstanding TalkTalk Security Partner, it has been fulfilling to work further within the TalkTalk Security Architecture team, to evaluate the PAM market space and develop and build a partnership with Osirium. We see real value in their work in the PAM space, and the automation elements of their tooling set them apart. We look forward to continuing the project as it evolves, bringing security and value to TalkTalk’s Security and Networking teams,” said James Mully, Sales Manager, Nomios UK&I.



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