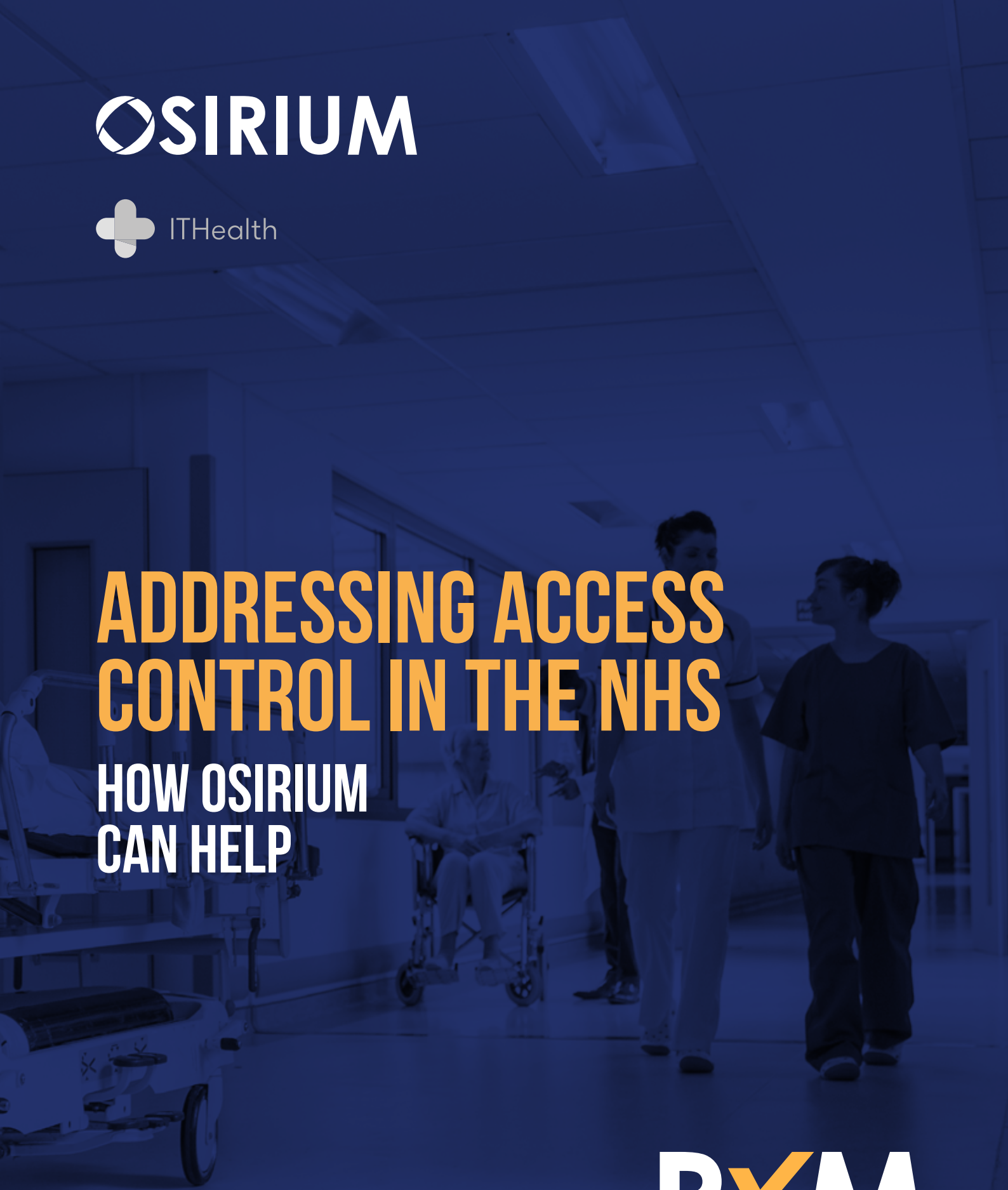
OSIRIUM

ITHealth



ADDRESSING ACCESS CONTROL IN THE NHS

HOW OSIRIUM CAN HELP

osirium.com

PXM PLATFORM

OSIRIUM & ITHEALTH

ADDRESSING ACCESS CONTROL IN THE NHS

OSIRIUM ITHealth

INTRODUCTION

Controlling access represents a significant challenge to the NHS.

NHS organisations need to provide access to data, servers and sensitive applications for a wide range of users with legitimate reasons, and prevent access from people without legitimate reasons.

They must also consider the risks associated with unauthorised access from malicious software, and cyber-attacks such as malware and phishing.

The nature of the target servers and devices users wish to interact with must be considered, along with the sensitivity of the content on those devices, and the user's reasons for requiring access.

Legitimate users could include medical staff, operational staff, third party service providers, help desk staff, Dev Ops or auditors.

Target servers and devices could include operational resources such as Windows servers that are used to run the day-to-day organisation, networking infrastructure devices, and database systems that hold sensitive patient information.

With so much complexity and so much potential value in a data breach, NHS organisations require a robust access control policy.

At the heart of the Access Control challenge is identity. Manage identity effectively and the risk of breach and data theft is mitigated.

NHS DIGITAL GUIDELINES

NHS Digital outlines very clear guidelines to help organisations manage access control.

These guideline state that access should be granted using the principle of ***least privilege***. This means that every user of a system should operate using the least set of privileges necessary to complete the job.

To enforce greater accountability users must be identifiable with a unique identity when connecting in to servers.

The following summarises the key guidance points issued by NHS Digital.

Role-Based Access Control

- All staff and contractors shall be given access in accordance with the requirements for access defined by their roles.
- All staff and contractors shall only have access to sensitive systems if there is a business need to do so and they have successfully completed any additional necessary vetting processes.
- Segregation of networks shall be implemented, and administrators shall group together users and systems to achieve the required segregation on networks.

Password Management

- Password change policy must be enforced to ensure passwords are changed at frequent intervals.
- Only authorised people shall have access to system utilities and access should be revoked when there is no longer a business reason for access.
- Where there is a requirement for the use of identifiers that are not associated with an individual, such as service accounts, these shall be created only after consultation with the security team.
- Passwords are core to access control and so they must be kept confidential, changed regularly, and not shared.

Process

- User access rights shall be reviewed regularly and users shall have unique identities so they can be held accountable.
- Privilege Access Management shall be controlled through a formal process and only the minimum privileges shall be granted to carry out the role or task.
- All staff and contractors shall only be granted access to those application functions required to carry out their roles.

Auditing

- Records of privileged user access may be used to provide evidence in the event of a security incident investigation.
- For audit purposes, systems shall be configured to capture the unique user identity being used.
- A formal record of all privileges allocated shall be maintained
- Unused accounts shall be monitored, and appropriate action taken in line with NHS procedures for disabling and deleting accounts.

Summary

Prescriptive guidelines are an excellent starting point, outlining clear steps to help organisations meet acceptable levels of security. However, in complex and diverse environments with large numbers of systems and users, prescriptive guidelines can be difficult to apply.

This issue is exacerbated by the move to **hybrid cloud operating models** and the proliferation of **outsourced IT partnerships**.

Historically, organisations have had to address access and segregation with a combination of process, multiple platforms and multiple technologies. The problem with processes are that they are often prone to manual error and don't always **scale** easily. Unless process can be enforced with a technology platform, it cannot be relied upon.

IT departments depend on **efficiency** to maintain an organisation's availability and uptime of services. Security technologies have typically added a level of protection at the expense of efficiency. Shared accounts are there to make life easier; because if the whole team knows the password then any one of them can run that command or carry out that task to keep the organisation running.

Complex passwords and those that require regular change are not easy to remember, so users write them down or tokenise the password to make it easier to remember.

As cloud computing has evolved, the battle for the traditional network perimeter has already been lost. Identity is the real key to an organisation's resource, regardless of where it sits. Control the identity and you have a better chance of protecting the resource.

The problem is that hackers, state funded activists and disgruntled insiders all realise that to inflict the most damage or extract the most value from a breach they need to elevate their privilege.

Without elevating privilege levels, attacks are limited to end points where there is less data of value and therefore less risk of serious data loss.

Insiders with malicious intentions are capable of abusing their level of privilege to access an organisation's infrastructure and wreak untold havoc.

Hackers who issue malicious malware know that their code needs to identify repetitive key strokes as potential privileged credentials, which can then be used by the hacker to access the network, seemingly legitimately.

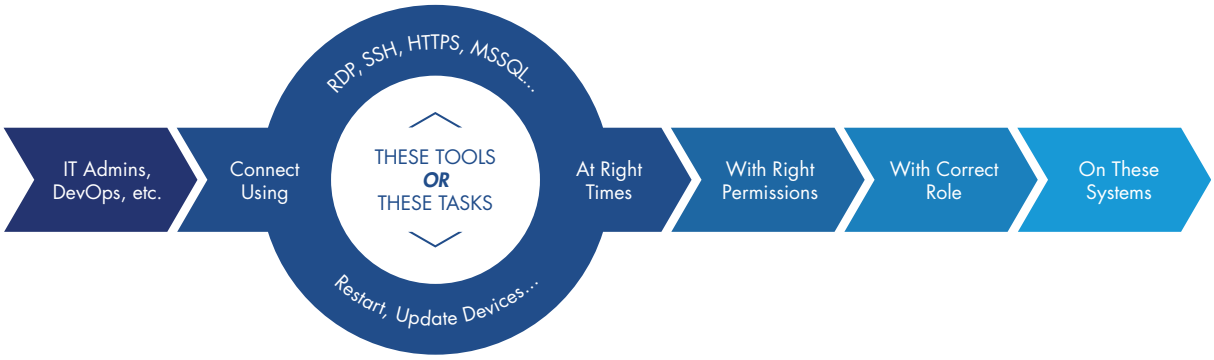
But it's not just those with malicious intentions who pose a threat. 25% of breaches occurring in the UK occur due to mistakes made by over-privileged team members who have made genuine errors.

Osirium

Osirium has a track record in helping NHS organisations enhance their IT security posture through the control and management of privileged user credentials.

With Osirium's Privileged Access Management solution, the PxM Platform, already embedded within a number of Trusts, we have identified a number of ways in which we can help.

We believe there is significant opportunity for other NHS Trusts to recognise the same or greater levels of security and cost saving within their own IT function by leveraging Osirium's PxM Platform.



HOW OSIRIUM WORKS

Osirium's PxM Platform sits between privileged users and the servers and devices they need to interact with. As such, it acts as a powerful enforcement point, allowing organisations to control who has access to what, when, and why.

Addressing the Password Challenge

Osirium's PxM Platform separates privileged users from their passwords. The solution encrypts passwords at rest and in transit, as well as randomising and changing them regularly.

As users do not know the privileged passwords they cannot be shared or written down. As passwords are injected into the target servers they never traverse the endpoint device and so the privileged credentials are no longer at risk from malware, phishing and social engineering attacks.

Addressing the Complexity Challenge

Instead of administrators having to remember or write down dozens of passwords to access target servers, Osirium's PxM Platform provides a Single Sign On (SSO) experience. Now, a privileged user simply has to access the PxM Platform and it will log them into the server they require. Its faster, easier, and does not expose the password.

Addressing the Accountability Challenge

Osirium's PxM Platform enables organisations to enforce a role-based approach to privileged users. In this case, organisations are able to map local user identities to roles when a user accesses a server. For instance local user dave.smith can access the Domain Controller with the role of Administrator and all the privileges that come with it. But from an accountability perspective the PxM Platform maps the local user name to the role so the organisation knows that individual user dave.smith carried out that piece of work even though he used a shared account.

Addressing the Audit Challenge

Osirium's PxM Platform can be used to record connections. This enables organisations to record activities carried out by privileged users, store them, and refer to them in the event that an issue occurs that needs to be investigated.

The PxM Platform takes this functionality further and uses the intelligence within the platform to provide real time analytics of privileged user behaviour. This enables organisations to identify anomalous behaviour in real time and address it accordingly.

EXAMPLE USE CASES

Visually Record and Log All 3rd Party Access For PSN Compliance

Osirium's PxM Platform provides the ability to visually log and capture the key strokes of any administrator session against systems within the network. A full audit trail of all 3rd party or contractor access is available from the platform if desired. As a pre-requisite for PNN and PSN compliance, the PxM Platform's Privileged Session Management and recording function is well placed to service this requirement.

Launch and Inject Privileged Credentials to System Vendor Applications

Osirium's PxM Platform offers the ability to access vendor applications and thick client tools using its MAP Server feature. Hosting thick client applications in a central location rather than on local desktops allows the sharing of these tools via the PxM Platform's Desktop Client, injecting the credentials needed without them ever reaching the users workstation. This also helps enforce least privilege at the desktop and promotes the use of standard build devices across the organisation.

An example of this would be the Check Point Smart Dashboard tool. The PxM Platform can launch this tool with full admin access or read only negating the need for users to know the credentials. By using time windows on the profile, we can decide when users have access to the tool. By employing session recording we can visually capture the work being done and by enabling Change Tickets we can force users to provide a valid and approved ticket before being able to access the tool.

Delegate Network Switch Tasks to Non-network Admins

Common network infrastructure tasks such as opening and closing ports, changes to VLAN, adding a device name or finding a port by MAC address can all be run as automated tasks. This allows any member of staff to execute these privileged tasks, without having direct access to the device and therefore without the risks associated with making these changes to critical infrastructure.

This reduces reliance on specific team members and removes the need for lengthy and expensive training courses for staff. Passwords are never revealed and CMD Line access is never granted under an automated task but can still be made available for network administrators who need full access.

Tighten Firewall Rules by Routing All Sessions Through the PxM Platform

As all device connections now originate from the PxM Platform's IP address, organisations can lock down all access to critical systems and networks to this appliance. This removes the need for designated user IP addresses or having to set static IP's on specific machines. Instead you can simply use a single rule for the PxM Platform which covers everything.

Support a Dual User Account Model Out of the Box

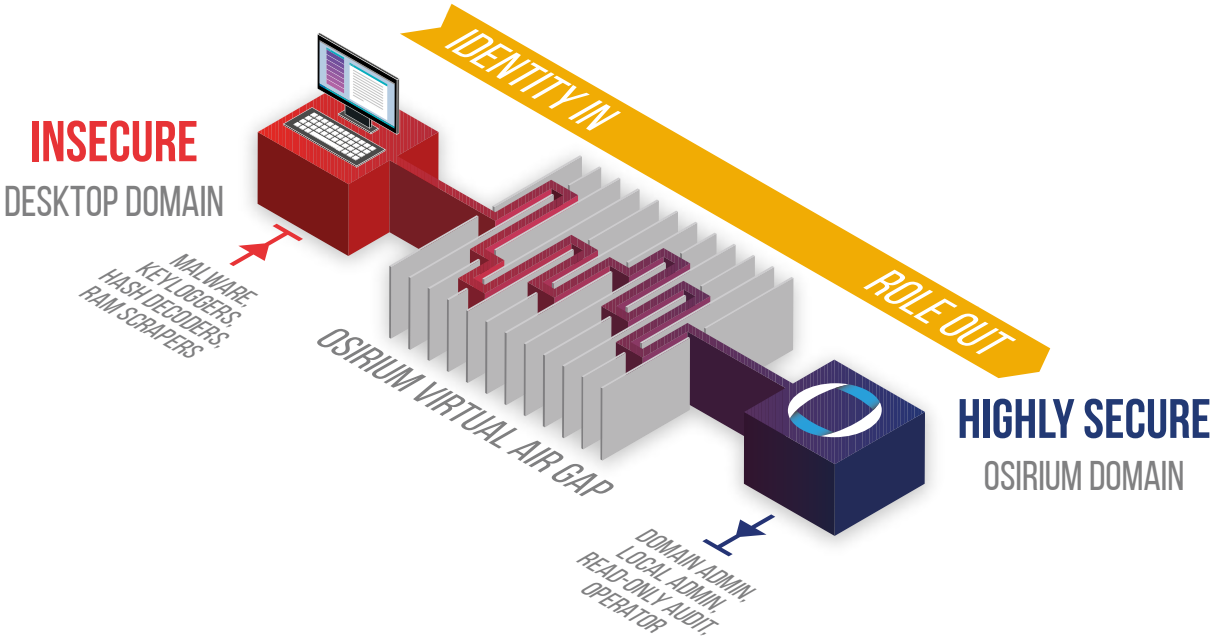
For organisations that have adopted secondary accounts with elevated privileges, the PxM Platform can accommodate this out of the box. The PxM Platform is able to map a user's non-privileged account to their privileged account, taking over the ownership and managing the password in the background.

The PxM Platform can refresh the passwords at a frequency of your choosing and never expose the credential to an end user's desktop. Having the PxM Platform manage the password removes the risk of it being lost, shared or written down. It doesn't obstruct those needing an elevated account but provides a level of protection and improved digital hygiene across the organisation. The PxM Platform allows you to truly remove the need for logging onto a desktop with a privileged account.

Secure and Audit Contractor and 3rd Party Access

To avoid the risk of exposing credentials directly to your contractors, you can instead grant them access via the PxM Platform. Access can be granted based around specific dates and times, automating account access on the appropriate systems as required. Time windows, session recording and change tickets can be applied by policy to enforce adherence to standards and compliance regulations.

The PxM Platform removes the need for specific user accounts to be created for third parties and contractors. The PxM Platform has the potential to significantly reduce the overheads required when provisioning 3rd party access to your systems. Common tasks that a third party might be conducting on a regular basis can be automated, removing the need for full management access over RDP/SSH.



Manage DMZ Systems / Segregated Services e.g. BWV

If you are hosting services outside of the main network, the PxM Platform can automate a number of tasks relating to these systems. For example file transfers, retrieving logs, service tasks or triggering and reporting vulnerability scanners such as Tenable Nessus.

Simplify Tasks and Delegate Them Back to 1st or 2nd Line Helpdesk Staff

The PxM Platform can convert common tasks that were previously being actioned by 2nd or 3rd line staff members and simplify/automate them to the point where any staff member can carry them out without needing in-depth training or specific system knowledge. Handy in event of regionalisation and collaboration supporting multiple environments with multiple systems.

Users are given a number of variable fields to populate depending on the nature of the task, all they have to do is click a single button for execution in the background. This could be a simple password reset or a multi-step task needing to be actioned against multiple devices, for example setting up a new mobile device, registering it and adding it to specific user/security groups.

About Osirium

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password life cycle management, and then hand the pre-prepared session back to the incoming request ready for system management. The session can be recorded, subject to time windows and device group separation. Osirium has delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.

OSIRIUM

11-13 High Street, Theale
Reading RG7 5AH

0118 324 2444
osirium.com