PXM PLATFORM

A multi-faceted cyber-security solution
for all IT dependent businesses

osirium.com

OSIRIUM

SECURE • SCALE • SIMPLIFY

X = Account, Access, Analytics, User, Task & Session manaagement

A multi-faceted cyber-security solution for all IT dependent businesses

Written by **Andy Harris**
Osirium Engineering Director

What is the PXM Platform?

Osirium's PxM Platform is comprised of four core modules designed to make the execution of privileged tasks and DevOps faster and more secure than ever before – offering complete end-to-end accountability and audit trail of precisely who did what, where and when.

For a Cyber Attacker there are hundreds of ways into an organisation, but once in, they will always need use of a privileged account to access and exfiltrate any interesting data. In 2014, 86% of passwords were simply stolen from user's workstations, 10% were phished and 4% were brute forced. The first half of 2015 saw this trend continue, but with less brute force and more phishing.

Mirum est notare quam littera gothica:

- Quam nunc putamus parum claram
- Anteposuerit litterarum formas humanitatis per seacula quarta
- Decima et quinta decima
- Eodem modo typi, qui nunc nobis videntur parum clari, fiant sollemnes in futurum
- Lorem ipsum dolor sit amet, consectetuer

Adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

PxM

PxM is all about managing privilege by bringing together what you've already got and what you already know. It's about making Privileged Tasks and DevOps faster and more secure. As a simple example, why allow admin access to systems without an incident ticket?; now the attacker needs both

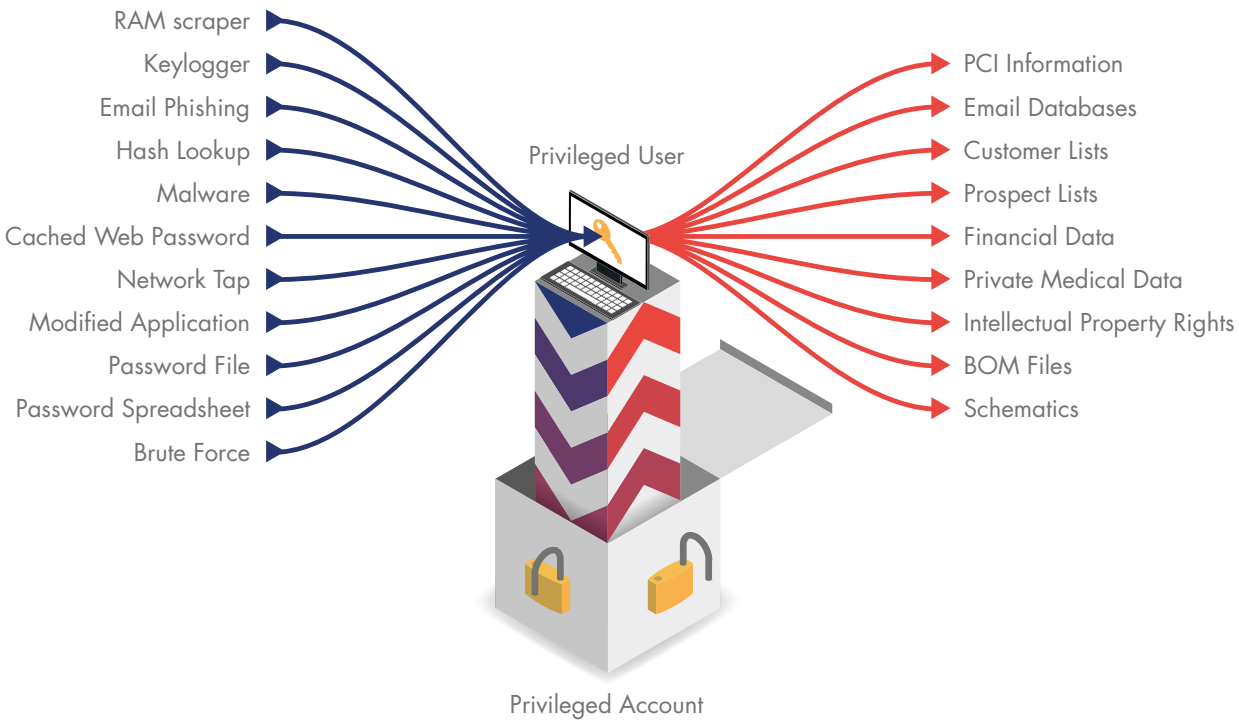
the admin account credentials and a valid incident ticket. This is the essence of JIP or Just In Time Privilege. The Privileged Account is only available at the time it's needed and only available to the authorised person's identity, whilst they are in possession of the change/incident ticket.

Identity In - Role Out is JEP: Just Enough Privilege. Osirium can easily handle multiple roles so it's simple to use profiles to map identities to different roles for different tasks. This avoids SysAdmins and DevOps automatically reaching for the highest privilege no matter what the task in hand.

In the current world of outsourcing and outsourcers' outsourcing, it can be hard to see who has access to what on your systems. These days, the lowest paid people have the highest privileges - and they don't work for your organisation. PM readdresses this balance for end-user organisations and uniquely allows MSSPs to manage tens of thousands of account credentials, outsource safely and keep their clients happy on the compliance front.

Separating people from passwords

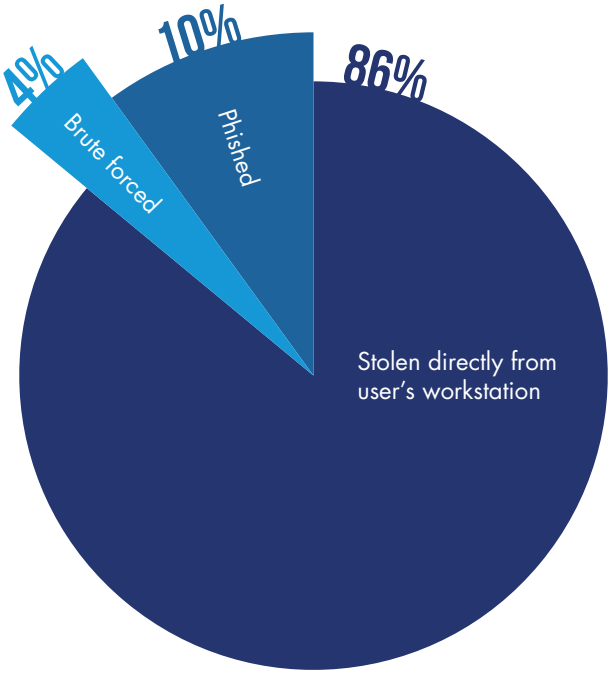
Osirium prevents attacks on Privileged Accounts by separating people from passwords. In our world you arrive as an identity and leave as a role, privileged passwords never enter the workstation domain. Passwords for privileged accounts undergo Enterprise Class Password Life Cycle Management. Osirium removes the need for direct system access using Privileged Task Automation and Session Recording allows you to see who did what, where and when.



How do passwords get stolen?

As we've got better with our password policies, external brute forcing of accounts is no longer viable. Therefore attackers move to the next weakest link in the chain. Right now, this is the users workstation.

Complex passwords are harder to remember, so users are recording them more. Savvy users are even using password vaults, but these are fundamentally weak if the password has to go to the user's work station. Seen right is a rundown of currently popular attack vectors.



Text files, spreadsheets and emails

Yes, really! More and more users are simply putting all their complex passwords into text files and spreadsheets right on the desktop. Malware writers know this, they also know it's the fastest route to Privileged Accounts. Encrypted spreadsheets are no more than a minor irritation to attackers. They are easily brute forced offline where there is no warning to the organisation.

A surprising number of users email passwords to themselves.
This is of real concern when they have access to corporate email from their home systems. It is estimated that 65% of all corporate workstations have a malware incident each year, it's assumed that home systems are almost certainly insecure. 32% of all computers worldwide are assumed to have a current infection. (Symantec).

"Osirium is a UK software development team that has pioneered the concept of a 'Virtual Air Gap' for Privileged Account access"

Key logging

This is the practice of logging all keystrokes looking for password sequences. It's quite easy to find password sequences since they often happen after time lapses and tend to have high keystroke rates. Key logging is a common type of malware that is often targeted at specific organisations or even individuals. This huge variation makes it hard for anti-malware products to spot these one-off attacks.

RAM scraping

This phrase is applied to two types of attack. Firstly, for searching for passwords and hashes in RAM and secondly to extract credit card and other personal data from known memory locations.vThe most obvious target will be the 'Paste' buffer. This is often likely to contain passwords throughout the working day and a neat way to get around password vaults.

Hash reversing

On many windows systems, when the user has a remote session they are authenticated against their password. The session details along with the password are then hashed and it is this hash that is used by the remote system to keep track of the users session.

The web holds tables of 131 billion hash to password lookups. So given that a hash can be extracted from a workstation session there is a reasonable chance that an attacker can make the reverse lookup to recover the original password. Most of the time the accounts will be non-privileged. This is why these kinds of attacks are often in play for a year before the attacker has sufficient high quality account details to extract data.

Phishing

There are two approaches to phishing, but both have the same outcome. The most common approach is to construct a feasible looking email that fools the recipients into entering their login details to an external website. You would have seen the near daily attempts telling you your PayPal account has been terminated, etc. A more directed approach uses DNS masquerading or software layering to fool a user into logging into an internal system. The best attacks simply pass on the connection and the user is none the wiser.

Are passwords really that bad?

In many ways passwords are still a really effective way of securing systems. In tests against brute force tools, Osirium generated passwords of 14 characters remained secure after a week of run time. It's the combination of people and passwords that cause the problems. There is always a need for passwords during the initial deployment of systems, devices and applications.

Securing all the end points - boiling the ocean?

The initial conclusion is that most of the endpoints are insecure.
This is a reasonable assumption. It is possible, at significant expense to secure all the endpoints using a variety of technologies, the most popular method being virtualised sandboxes for each application running on a work station. This means that the sandboxes need to be capable of running all the applications on all the platforms used by an organisation. That's a lot of testing, and the exceptions are allowed to run "as-is". We're still not past the keyloggers and phishing. We also need to take into account all those users that have access to the systems who are not directly controlled by the organisation: Contractors, Third Parties and outsourced IT. Securing the endpoint is not securing the people, they are still vulnerable to phishing.

"We separate the people from the passwords, then we ensure that the passwords never enter the user's workstation"

What does Osirium's PxM Platform do about all this?

In many ways passwords are still a really effective way of securing systems. In tests against brute force tools, Osirium generated passwords of 14 characters remained secure after a week of run time. It's the combination of people and passwords that cause the problems. There is always a need for passwords during the initial deployment of systems, devices and applications.

The operational model is: 'Identity in, role out'. By this we mean that we use profiles to map the identity of a user to the role that they should have on a system, device or application. Osirium users prove their identity first, then they request a connection to a device, system or application using their regular tools. Osirium then performs the single sign-on and then connects the resulting session to the user.

What is a role?

The PxM Platform deals with roles from simple to complex. A role could be as simple as mapping to a specific account, like 'root', 'administrator' or 'maint'. At the top end of functionality, Osirium creates accounts on the target system/device/application based on templates used in profiles. For example, the inbound identity of 'alice' could be mapped onto an account 'alice_auditor' that is specifically provisioned with a precise range of privileges and only ever used in a one-to-one mapping to 'alice'.

Osirium's PxM Platform accounts into either:

UNAPPROVED

An unknown account.
(should this be deleted?)

APPROVED

An approved account.
but not available for SSO or Tasks

KNOWN

An account with known credentials,
available for both SSO and Tasks.

MANAGED

An account that the PxM Platform
manages the password for,
SSO and Task valid.

OSIRIUM MANAGED

An Account that the PxM Platform can
create, destroy, enable and disable
by policy, SSO and Task valid.

These categories can be presented as reports, with a granularity that goes from the whole IT estate down to an individual device. The reports can be graphical or tabular and in the case of the table reports the columns are actionable. For example, filtering by a set of devices, and then by the unapproved accounts on those devices allows you to delete or disable those accounts as a single action.

Where Osirium is making the regular audits, any new accounts created out of band will show up as Unapproved. This is the first stage of ongoing automated account management.

'Osirium Managed' accounts are particularly useful in compliance since they only arise as a direct result of policy - if the policy changes, Osirium will delete and create accounts to meet that change. At this level of operation, accounts are fully automated, with instant changes to reflect policy. As any Compliance Officer knows, it's not just passing the audit that counts - it's the ongoing controls that really enforce security.

At the Compliance level the ultimate step is to remove direct access to the device, this can be replaced by task level access. Therefore the user gets the intended effect of the privilege; tasks are consistent and error-free, and of course there is no opportunity for unauthorised wandering across the IT estate.

Analytics allow the Compliance Officer to take multiple views across the data that Osirium accrues. Each of the data points are linked through to tables. For example you could see what actions are taking place outside of working hours and tabulate these by IP address, user identity, system, category, etc. If one of these seems unusual you can click through to the Session Recording and even search through the keystroke history.

Third party access?

It is highly likely that one or more of the blocked users would have been from vendors or outsourcing, who 'inherited' the password as part of installation or support work. With the PxM Platform you can switch on their access at will, and they still don't need to know the actual device-account password. You simply move the vendor user in and out of the Profile to grant access.

Built for scale

A single instance of Osirium's PxM Platform can handle hundreds of users and thousands of devices, all mapped through multiple profiles per customer. All the accounts that the PxM Platform manages can be set for Password Lifecycle Management. With the PxM Platform, the MSP can do all this without direct access to a customer's Active Directory. The PxM Platform can even handle different policies for different customers as well as coping with the scenario where the MSP further outsources specific operations to a specialist MSP.

Built for cooperation

There are often situations where companies are customers of each other or cooperate on a shared infrastructure. In these cases Osirium instances can mesh together. You get both a cooperative environment and a clear definition of who can do what, where and when.

Built for ease of use

SysAdmins in organisations have spent a lot of time getting their digital tool chain together. With the PxM Platform we keep that tool chain fully intact. SysAdmins use the same tools to the same systems, but the PxM Platform makes the connections and performs the logins, thus representing a time saving in and of itself.

We take this one level higher with our searchable interface, it can be searched by system name, connection type, role or any metadata such as location, team or function.

Password Lifecycle Management

When directed, the PxM Platform can manage passwords of the accounts used on devices, systems and applications. The PxM Platform knows the longest password any particular account can have, and then generates properly random passwords. Passwords can be updated either by a PxM Platform task or on a scheduled basis.

There's always the possibility of a device needing to be restored from a backup, the PxM Platform keeps track of all the passwords and the periods used for every account it manages. When a device is restored, the admin simply directs the PxM Platform to roll back to the date of the backup, once the platform has restored access the password is refreshed to match the current date.

Solving the shared account problem

Because the PxM Platform makes the mapping between the identity and the role, there is no need for the user to know the passwords of the 'device-accounts'. So if you've inherited a situation where many people in a team use the same 'domain-admin' account you can quickly fix this with the PxM Platform.

Simply put all the authorised users in a profile. Then add the systems that use this account to that Profile. Now use the PxM Platform to change the password of the 'domain-admin' account. At this point all the authorised users still have the access they need, all the users who may have been given access in the past are blocked.

Delegating the task, not the privilege

With Privileged Task Management, Osirium combines the benefits of:

SECURITY

No need for users to have access to privileged accounts.

EFFICIENCY & TIME SAVING

Tasks are pre-packaged and parameterised, making them much faster to select and execute.

ACCURACY

Eliminate the possibility of errors caused by user input.

Security

Every time a user is given access to a Privileged Account a risk is created.
We've already seen how the credentials for these accounts can be stolen but we've not yet considered the possibilities for insider wrongdoing or simple mistakes.

If a user has full access to a system or application, they may be tempted
to go everywhere or peruse all the data. This could be as simple as a waste of effective working time, or at worst an insider driven data breach à la Snowden.
A classic example would be giving the help desk domain admin rights so that they
can change passwords.

Privileged Task Management (PTM) is the cleanest and safest way of granting the ability to perform a series of known, auditable tasks without granting excessive privileges to the user. The actual tasks can all run under the same Privileged Account and Osirium will keep track of who issued the commands and the parameters used.

Efficiency - time and cost saving

We tend to visit our larger customers and active POC's every two weeks. It's of great interest to note that 'security' is a 'solved issue':- it rarely comes up in these meetings – it's all about tasks, tasks and more tasks.

This is where our customers are reaping the benefits of Osirium. If we take a simple example of a command line task that needs to be run across several machines before PTM, we find that the user has to find the credentials for each system, login, issue the commands, logout and then move on to the next system. With Osirium, they select the task, check the systems required and submit the job. Typically a 20 minute task can be reduced to an error and risk-free 8 seconds.

That 19 minutes and 52 seconds gained can be used by staff for more interesting and productive work. Taken further it allows organisations to amplify the power of their DevOps teams. DevOps can design the Osirium tasks into the workflow of the help desk, transferring responsibility to the help desk teams. The benefits of this are twofold: the Privileged Tasks have been delegated to cheaper resources, and to the people best placed to deliver a first call fix. Now that 19 minutes and 52 seconds is not just saved in DevOps but has made the whole organisation more efficient.

Accuracy

One of our customers outsources their network changes and moves to BT through a ticketing system. Each change is defined in a ticket and BT staff close off the ticket as the change is completed.

Before Osirium, the BT staff needed full admin access to the network infrastructure. They suffered from a few simple issues such as assuming that an empty port was unallocated and occasionally using ports 1 and 2 which were reserved for up-links. There are some confidential VLANs that our customer would configure directly and then inform BT via the ticket that a change was ready.

With Osirium, this process is much simplified and considerably faster. Field staff now use Osirium Tasks: they can run a

task against a switch to find the properly unallocated ports - no more guessing. When they configure ports, 1, 2 and 47, 48 are not available in the task – no more accidentally overriding an uplink. Since the field staff have no direct access to the infrastructure the tasks can configure the confidential VLANs safely – shorter workflow. As part of the 'port configure' task there is a field for the ticket number – the workflow loop is automatically closed.

As icing on the cake, Osirium takes backups at each stage of the change so it's easy to roll back any mistakes in the field.

Record the sessions, shadow the sessions

Oftentimes it is vital to know exactly what has been done to a system. For example it may be useful to see how a vendor has solved an issue. If a mistake has been made a Session Recording shows the series of events that lead up to the problem. If you know what has been done, you know what to undo. With Osirium, you can get a overview of a session through thumbnails and then zoom into the details through video and keystroke analysis.

In the case of security-sensitive third party access, Osirium has the facility to shadow the session, you can see in realtime what the remote admin has done whilst the session is simultaneously recorded.

Osirium makes it very clear what is being recorded: there's a red box around the recorded session. This acts as a constant reminder to the good to get in the right. To malicious insiders it's a real deterent, even if they are using a generic account such as 'root' or 'administrator'. Osirium ties the recording to both the identity and the account used.

The 10,000m view

Osirium provides great analytics, with the data visualised through many slices and filters. It’s an excellent way of seeing the outliers and unusual activity. It is easy to tie these back to the identity and location of those using the sessions, and with click-through you can get straight to Session Recordings or see the profile structure that authorised their access.

Breakglass mechanisms

For day-to-day breakglass you can use the 'Reveal Password' task for individual devices. In this case, Osirium effectively acts as a password vault - revealing the password at the SysAdmin's workstation. This raises a security event as we at Osirium believe that a password is compromised once it enters any workstation.

For bulk breakglass we have our password protected PDF mechanism. As expected this generated a password protected PDF of all the passwords that Osirium manages. This function can only be run by a 'Super-admin'.

Console break glass: this is for that dire situation when the hypervisior that Osirium itself runs on has been orphaned from the network. It works on a standalone codebase and addresses the database directly. The SysAdmin will need the 'Master Encryption Key' to access the passwords, in itself serving to allay the fear that 'everything can be stolen'.

There are secondary issues, mostly cultural or arising from the fear of altering well-honed workflows. We understand this - we understand that SysAdmins are getting more scrutiny than they've ever had... So from the outset we've designed Osirium with the view that: "If we have to have a Guard, Osirium would be friendliest Guard you've ever met - so long as you're a legitimate user".

Osirium will help you find the systems and devices you need to access by using all available data - start typing a fragment of name, location, protocol, tool or metadata and Osirium will narrow the list until you see what you want; and it's realtime, as you type.

Don't change your workflow! Osirium allows you to use your current toolset and lets you change tools whenever better ones become available.

Osirium will let you collaborate with your consultants, suppliers and third party outsourcers - you can safely grant access for defined periods and shadow what they do on your systems. You can record and playback sessions at will to see how problems were solved.

A compliance officer's dream

Because Osirium maps Identities to Roles, it already goes a long way in delivering 'Active Compliance'. This means that we can automatically close the loop between Audit and Action. Within the Osirium UI it's easy to visualise:

The accounts that already exist on systems, not just Windows and Linux but a wide range of systems, applications and devices - for example Cisco Switches, Storage Area Networks and Mobiles.

The identities (i.e the users) that can be mapped into roles.

The relationships between the users, the roles and systems that they can use along with the time windows and the status of session recordings.

When Osirium is managing a device it runs a regular 'Device Audit'. This Audit discovers all accounts on the device, whether they are user, service or daemon based.

Managed Service and Security Server Providers - Meeting Customer Expectations With Greater Security and Better Efficiency.

Osirium is the ideal tool for MSPs and MSSPs:

- On-boarding is supremely simple and effective
- Task automation enables huge time and cost savings
- Securely outsourcing to other specialists couldn't be easier
- Reporting is built-in and be filtered by customer, location, system type, etc.
- Password life-cycle management is automatic; set for customer requirements and you're done

Onboarding

Osirium can accept CSV lists of devices and their credentials - it takes just minutes to ingest hundreds of devices. However it doesn't stop there: with our bulk profile upload tool MS/SPs can sort all devices into appropriate profiles and match these profiles to their team structures. Devices, Systems and Applications can have rich metadata definitions, for example customer, location, production/development/user acceptance test (UAT), etc.

Task automation

Tasks are covered fully on pages 7 & 8, but suffice it to say that these are an MS/SPs best friend. In general we've noticed that before an installation of Osirium takes place the discussion revolves around security, just weeks after, the entire focus is on tasks and more tasks. Security based tasks, for example bulk updating blocked IP lists across an estate of dissimilar firewalls, can be reduced to a few clicks - faster, safer, cheaper.

Outsourcing for the outsourcer

The very reason that MS/SP's are successful is that they focus on what they are good at - delivering and replicating this over their customer base. It stands to reason that there is a market for specialist and niche Outsourcers that sell to the prime Outsourcers. These functions are often fulfilled by niche contractors or small specialist companies, for example those that deal in Malware prevention. The nature of Identity in - Role Out allows for trust relationships to be formed between organisations which are defined in profiles. These profiles are quick to build
and easy to visualise and report on.

Osirium just makes it easier for organisations to work together.

Management reports

The built-in reports can be filtered against all available device data, including all metadata available during on-boarding. These reports show all the password lifecycle coverage and the percentages of accounts in the states 'Unapproved, Approved, Known, Managed and Osirium Managed' For example, it would be trivial to find out how many UAT systems and accounts you support for a particular customer at a particular location.

Password policies.

Password lifecycle management is a cornerstone of ISO 27001 information security (Section 9.2.all). MS/SP's will have their own policies. Once a contract is underway, your customers expect their MS/SP to conform with their password policies. If you have many customers with many policies, then automation is a must. Your staff will present their Identities to Osirium and Osirium will automatically manage all Device/System/Application credentials.

No more password Sundays…

Part of an ecosystem

Of course Osirium doesn't exist in a vacuum... there are other tools in the cyber-security chain, products like SIEMs and Sailpoint. Osirium plays well with SIEMs, creating CEF syslog messages for all the significant account and user-based events that it handles. For SIEMs this is a vital link in tying together things that happen on systems and which account was logged in at the time. With Osirum the account is tied back to the Identity of the user, so now you know which user used which account on which system.

Sailpoint is the user account audit tool of choice among the audit teams of the big four. It can walk through Active directory and deduce which accounts have access to which applications - and which rights they will have on the server estate. Sailpoint can go even further in that it can request changes to those accounts and even request the provision of new accounts.

In the world of Privileged Accounts, there are many systems with set accounts and roles, along with built in root and administrator accounts. This means that those accounts need shared access, and shared access means a loss of accountability. If we add Osirium to Sailpoint two good things happen:

- Accounts can be shared with accountability to user identity.
- Accounts on devices that Sailpoint can't access are surfaced to the Sailpoint UI.

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 Ltd.
Theale Court, 11-13 High Street, Theale, Reading, Berkshire, RG7 5AH

0118 324 2444 | **info@osirium.com** | **osirium.com**