EDISON

Osirium Technologies

H119 results

Product innovation supports order growth

Software & comp services

Osirium won a number of new customers and saw a 100% renewal rate in H119. It has signed up its first customer for the recently launched privileged process automation solution and is due to launch its first endpoint privilege management solution in Q4. With a broader product range, it has the opportunity to win new customers in the wider privileged access security market and cross-sell to its existing customer base.

Year end	Revenue (£m)	EBITDA* (£m)	EPS* (p)	DPS (p)	P/E (x)	EV/sales (x)
12/17	0.65	(1.61)	(18.1)	0.0	N/A	4.7
12/18	0.96	(1.77)	(18.1)	0.0	N/A	3.2
12/19e	1.25	(2.17)	(19.6)	0.0	N/A	2.4
12/20e	1.82	(1.88)	(19.7)	0.0	N/A	1.7

Note: *EBITDA and EPS are normalised, excluding amortisation of acquired intangibles, exceptional items and share-based payments.

Strong multi-year order intake in H1

Osirium saw strong bookings momentum in H1 (+69% y-o-y) from a combination of contract renewals and new customers. Due to a number of multi-year deals, revenue grew only 11% y-o-y. The company reported an EBITDA loss of £1.2m during the period versus £1.0m a year ago. Net cash at the end of H119 was £0.89m, and post period end Osirium received an R&D tax credit of £0.47m. While our bookings forecasts are maintained, we have revised our forecasts to reflect the operating costs and capex incurred in H119, resulting in a wider EBITDA loss in FY19–20. The company noted that it planned to raise funds in H2. Since the end of H1, a customer has extended an initial one-year contract for 250 devices to cover 2,600 devices over three years, providing support to our H2 bookings forecast.

Broadening the product range

Building on the success of PxM's privileged task management (PTM) module, in May Osirium launched a secure privileged process automation (PPA) solution known as Opus, and last month confirmed its first customer for the product. The company is also entering the endpoint privilege management market and expects to launch its first product in Q4. This broader suite of privileged access security solutions provides a larger addressable market for Osirium, as well as the opportunity to cross-sell the new products to its existing customer base.

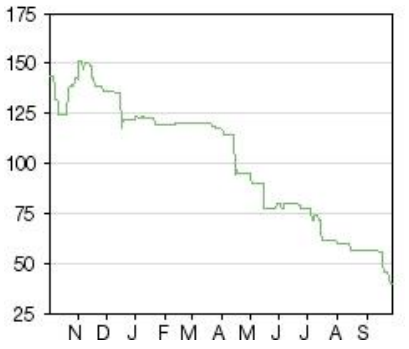
Valuation: Bookings growth the key driver

After a decline in the share price over the last year, Osirium is trading at a discount to peers on an EV/sales basis. As it is an early-stage company several years from profitability, we have performed a reverse DCF to analyse the assumptions factored into the current share price, using a WACC of 11% and a terminal growth rate of 3%. We estimate that the share price is discounting average bookings growth of 23% for FY21–28, break-even EBITDA in FY24, average EBITDA margins of 1.9% for FY21–28 and a terminal EBITDA margin of 35%. In our view, bookings growth and confirmation of funding are the key drivers of share price performance.

30 September 2019

Price	**40.0p**
Market cap	**£5m**
Net cash (£m) at end H119	0.9
Shares in issue	13.6m
Free float	91%
Code	OSI
Primary exchange	AIM
Secondary exchange	N/A

Share price performance



%	1m	3m	12m
Abs	(29.2)	(48.4)	(72.4)
Rel (local)	(32.2)	(48.8)	(71.9)
52-week high/low		151p	40p

Business description

UK-based Osirium Technologies designs and supplies subscription-based cybersecurity software. Its PxM platform includes privileged access, task, session and behaviour management. It recently launched a secure process automation solution and is soon to launch a privileged endpoint management (PEM) solution.

Next events

FY19 trading update	January 2020

Analyst

Katherine Thompson +44 (0)20 3077 5730

tech@edisongroup.com

Edison profile page

Osirium Technologies is a research client of Edison Investment Research Limited

Investment summary

Innovative privileged access security software vendor

Osirium's privileged access security software helps protect critical IT infrastructure from unauthorised use of privileged IT accounts, whether from hacking or internal threats. Osirium's PxM software platform introduces innovative concepts such as the virtual air gap (to prevent passwords being shared and from making it onto users' workstations) and task automation (to delegate tasks rather than privilege). The recent development of secure privileged process automation and endpoint privilege management solutions has expanded the company's addressable market. Osirium is following a land and expand strategy – selling licences to enterprise customers to help resolve pain points, then expanding licences to cover a larger number of end devices or users, additional modules and additional functionality. Management is also targeting the mid-market, where the ease of deployment and maintenance of Osirium's software makes it an ideal solution to sell through channel partners. The complexity of established solutions means fewer mid-market businesses use privileged access management (PAM) software than enterprises, so this is a market ripe for development. The company has distributors and resellers covering the UK, the Middle East and North Africa. To support partners, Osirium recently hired a channel director, and to support customers provides 24/7 global technical support.

Financials: Bookings growth outpacing revenue growth

Osirium saw strong bookings momentum in H1 (£1.03m, +69% y-o-y) from a combination of contract renewals and new customers. Due to a number of multi-year deals, revenue grew only 11% y-o-y while deferred income was 70% higher y-o-y. The company reported an EBITDA loss of £1.2m during the period versus £1.0m a year ago. Net cash at the end of H119 was £0.89m and post period end the company received an R&D tax credit of £0.47m. While our bookings forecasts are maintained, we have revised our forecasts to reflect the operating costs and capex incurred in H119, resulting in a wider EBITDA loss in FY19–20. We forecast a shift to a net debt position of £0.5m by the end of FY19 – the company noted that it planned to raise funds in H2.

Valuation: Bookings progress the key driver

After a decline in the share price over the last year, Osirium is trading at a discount to peers on an EV/sales basis. As it is an early-stage company several years from profitability, we have performed a reverse DCF to analyse the assumptions factored into the current share price, using a WACC of 11% and a terminal growth rate of 3%. We estimate the share price is discounting average bookings growth of 23% for FY21–28, break-even EBITDA in FY24, average EBITDA margins of 1.9% for FY21–28 and a terminal EBITDA margin of 35%. In our view, bookings growth and confirmation of funding are the key drivers of share price performance.

Sensitivities: Pace of adoption, renewals, channel success

Osirium's financial and share price performance will primarily be sensitive to the rate at which its software is adopted. This includes the rate at which enterprises and managed security service providers (MSSPs) sign up to use the software, the amount of upsell to existing customers, and the rate at which channel partners sign up new customers. Achieving high renewal rates will also be crucial to maintaining a high level of recurring revenues. The mix between direct and channel sales will influence the rate of revenue growth. There is already an active market for PAM software and several well-established and well-funded competitors.

Company description: Privileged access software

Osirium is a UK-based provider of privileged access security software. Although small from a revenue perspective, the company has signed up a number of blue-chip enterprises and MSSPs, providing validation for its innovative, subscription-based software. Over the last year, the company has expanded its product range from privileged access management (PAM) to include secure privileged process automation (PPA) and privileged endpoint management (PEM). The company is focused on building its customer base and expanding into the mid-market.

Background

Osirium was founded in 2008 by David Guyatt (CEO) and Kevin Pearce (technical services director). Working together to develop solutions to customers' cybersecurity issues, they identified that PAM was an area ripe for innovation. They developed a solution that was adopted by several blue-chip customers and, from there, decided to standardise the technology into modular solutions: the PAM module and the PTM[1] module. Between 2011 and 2015 the company raised funds of £4m to support development and rollout, and in February 2016 the Osirium PxM 2.0 platform was launched. In April 2016, the company listed on AIM to access growth capital, raising net proceeds of £5.1m from the issue of 5.66m shares at 156p per share. In March 2018, Osirium raised a further £4.0m from the issue of 3.14m shares at 134p per share. The company is based in Theale, UK, with a staff of 50.

Strategy: Expand into the mid-market

Osirium's technology was originally developed to meet the exacting demands of enterprise customers. More recently the company started moving into the mid-market, where the risks relating to misuse of privileged access are as relevant, although companies may not have the same level of IT resource to manage this risk. Consequently, a large proportion of the potential market is a greenfield opportunity, as mid-market awareness of the need for PAM is growing. Osirium's technology has been designed to be easy to implement and simple to use and maintain, reducing the amount of external and internal IT resource required to get the technology up and running and to use on an ongoing basis.

In the longer term, the company wants to have a thriving channel-driven mid-market customer base complemented by direct relationships with enterprise and MSSP customers. It uses a direct sales approach for enterprise customers and has developed a channel strategy to access the mid-market (companies with 200–2,000 employees).

Experienced management team

Osirium is headed up by CEO David Guyatt. David has an extensive background in the cybersecurity software market and has worked for many years with other members of the management team. In the 1990s he worked with the COO, Catherine Jamieson, CTO, Andrew Harris, and technical services director, Kevin Pearce at cybersecurity integrator Integralis. While there, they developed several products, including MIMEsweeper (email security and content filtering software), which was spun off into Content Technologies in 1998. In 2000, Baltimore Technologies bought Content Technologies for $1bn, and then sold it to Clearswift Systems in 2002. David joined Clearswift as a non-executive director in 2002 and was CEO from 2003–05. In 2008, he was approached by Kevin Pearce with an idea for a PAM solution, which led to the founding of Osirium. Catherine Jamieson joined Osirium in 2009, with Andrew Harris joining in 2011. CFO Rupert Hutton joined Osirium in 2015; he served as CFO of AIM-listed Atlantic Global for 12 years.

[1] Privileged task management

PAM market

Privileged access – what it is and who has it

The majority of IT users within a business have standard access to the software and devices that they need to use; this enables them to use the applications and devices but does not give them any rights to change any elements of the underlying software or device. System administrators (sysadmins) and developers need to have enhanced access to IT infrastructure and applications to maintain services on a day-to-day basis, resolve problems encountered by other users and to test new services and devices within a corporate network. This enhanced access is described as privileged and typically each device and application requires a separate user name and password for this (privileged account). As privileged accounts can make substantial changes to systems such as creating or deleting users, accessing customer data or configuring the company's internet access, they are extremely powerful. Incorrect or malicious use of a privileged account could shut down a business's internet presence preventing online sales, could leak personal or commercially sensitive data or in extreme circumstances, impact on implanted medical devices.

In some cases, only one privileged user will have access to the password but in other cases, passwords are shared by a group of privileged users. The increasing prevalence of outsourcing increases the number of privileged users. For example, if a company outsources its IT support to a third party, users within the third-party company will need remote privileged access to the company's IT to resolve problems. In some cases, outsourced IT providers in turn outsource some of their services to another third party, extending the number of privileged account holders. With this increasing complexity, shortcuts are taken including uncontrolled sharing of passwords, giving poor visibility into who has what access and where.

Privileged accounts a focus for internal and external threats

Historically, cybersecurity has focused on protecting businesses from external security threats, putting in place solutions to protect the perimeter, such as firewalls, and to protect endpoint devices from malware, such as anti-virus software. This is still a crucial element of IT security, but businesses also need to consider the threat from internal users as well as the need to secure assets against hackers if they do manage to breach the network. To complicate matters, with the increasing use of cloud-based software, the perimeter is no longer clearly defined. Any connected system is at risk, so as use of internet of things (IoT) increases, it provides a larger attack surface (ie number of points within a network that could be attacked to breach the network). Companies should aim to minimise the attack surface by ensuring users only have the level of privileged access they require for each device/application to do their jobs effectively (known as 'least privilege').

External attackers seek out privileged accounts

Hackers particularly target privileged accounts, as they can be used to access more users or data within a business. Once a hacker has breached the network, it can be very difficult to detect it – some breaches are not detected for months and a few continue for years. Once in, a hacker may place malware on the system that is not used until an attack several months later, or the hacker may quietly siphon off data over a long period of time.

Internal users can also represent a threat

The most obvious internal threat is a 'bad actor', an authorised privileged user who decides to leak data or access to outsiders for a variety of reasons including money, revenge, blackmail, or terrorism. A prime example of this was Edward Snowden and his leaks of NSA information. Another internal risk comes from elevating the rights of existing users – this means that if a hacker does

manage to penetrate the system, he could obtain access to a large number of devices. A report by Verizon[2] in 2019 estimated that 34% of attacks were perpetrated by insiders.

Regulation drives need for PAM solutions

For certain industry-specific regulations, demonstrating control over privileged access is a requirement. Examples include PCI DSS regulations for debit and credit card payments, and HIPPA regulations for US patient healthcare data. In the EU, the directive on security of network and information systems (the NIS Directive) requires operators of essential services (OES) in critical national infrastructure and digital service providers (DSPs) to:

- take appropriate technical and organisational measures to secure their network and information systems;
- take into account the latest developments and consider the potential risks facing the systems;
- take appropriate measures to prevent and minimise the impact of security incidents to ensure service continuity; and
- notify the relevant supervisory authority of any security incident having a significant impact on service continuity without undue delay.

The solution: PAM software

While a company must be responsible for user identity policy and process and for deciding what levels of privilege to grant to users, PAM software can assist in implementing these policies. It can also reduce a company's dependence on spreadsheets containing passwords and the use of shared passwords, and should improve operational efficiency for sysadmins. Such software should enable a company to manage the ownership of all privileged accounts, whether individual or shared, and should prevent the elevation of privilege above the necessary level. The software should have reporting capabilities and threat analytics and should integrate with other applications and overall security architecture. Early this year, market research firm Gartner released a report on best practice in PAM, with the four pillars being:

- track and secure every privileged account;
- govern and control access;
- record and audit privileged activity; and
- operationalise privileged tasks.

Market forecasts are for strong growth

Gartner estimates the PAM market generated revenues of $690m in 2015, rising to $900m in 2016 (+30%). It is forecasting the market to grow to $2.274bn by 2020 (CAGR 27% 2015–20), with demand driven by regulation, the shift to the cloud and adoption spreading to smaller organisations. In June, Gartner produced a top 10 list for CISOs,[3] listing priorities for new security projects once basic security measures had been put in place – PAM was named as one of the ten priority projects.

Competition

There is a well-established market for PAM software, with a number of competitors focused on PAM software as well as a number of broader software vendors with PAM offerings alongside other cybersecurity offerings. CyberArk is the market leader, established in 1999, and is Osirium's biggest competitor in the enterprise market. In the mid-market space, Osirium traditionally competed more

[2] Verizon Data Breach Investigations Report, 2019

[3] Chief Information Security Officers

with smaller players Thycotic, Bomgar, BeyondTrust and Wallix. Consolidation accelerated in 2018 with Bomgar buying several PAM vendors (see page 14) – it is now of a similar size to CyberArk and brands all solutions as BeyondTrust. Since being acquired by Thoma Bravo, Centrify has spun out its identity and access management business into a separate company, Idaptive, with the remaining business focused on PAM. Customer numbers per Exhibit 1 reflect the differing size of customers by vendor, eg Thycotic offers a freemium product in the SME market based on its cloud-based password vault.

Exhibit 1: Competitive environment

Company	Ownership	Annual revenues	No. employees	HQ	Products	No. customers
PAM focused vendors						
CyberArk	Nasdaq: market cap $3.8bn	FY18 $343m, FY19e $423m	1,146	US	Core Privileged Access Security, Application Access Manager, Endpoint Privilege Manager, CyberArk Privilege Cloud, CyberArk Alero	>4,800
Beyond Trust*	Francisco Partners	c $300m		US	Password Safe, Privileged Remote Access, Remote Support, EPM, Vulnerability Management, Auditor	>20,000
Centrify	Thoma Bravo (majority stake)	FY18 $115m	c 500	US	Privileged Access Security	>5,000
Thycotic	Private; includes Insight Venture Partners	$46.7m		US	Secret Server, Privilege Manager, DevOps Secret Manager, Privileged Behaviour Analytics.	>10,000
Wallix	Euronext: market cap €63m	FY18 €12.6m, FY19e €19.1m	145	France	Wallix Bastion, Wallix Discovery, Wallix DataPeps	1,000
Broad-based vendors						
CA Technologies	Broadcom	FY18 $4.2bn	11,300	US	Privileged Access Manager	
Micro Focus	LSE: market cap £3.8bn	FY18 $3.7bn of which $762m from Security products.	14,000	UK	Privileged Account Manager	
ManageEngine	Zoho Corporation (private)	N/A	4,000	US	Password Manager Pro	

Source: Edison Investment Research. Note: *Incorporates products from Avecto, Bomgar, BeyondTrust and Lieberman Software.

Gaining increasing recognition from industry experts

As Osirium has grown over the last three years, it has been recognised by market research analysts Gartner and KuppingerCole. Gartner featured Osirium as a Cool Vendor in Identity and Fraud Management in 2017 and recognised it as a niche player in its inaugural Magic Quadrant for PAM software published in December 2018. Gartner analysts highlighted that Osirium's task-management capabilities were best in class.

KuppingerCole analysts recognise that Osirium's innovative features (virtual air gap, automated tasks) take a different approach to its competitors and therefore make it hard to assess on a like-for-like basis, but also highlight that these features may be exactly what is required by some customers. KuppingerCole reviewed the recently launched PPA solution, highlighting that it could be used more broadly across a business, for example in HR or finance. It also noted that PPA was able to address a challenge that is not dealt with well by existing ITSM[4] offerings or PAM tools.

Osirium's product portfolio

Over the last year, the company has invested in expanding its product offering, adding privileged process automation and EPM to existing PAM capabilities.

PxM platform – managing privileged access

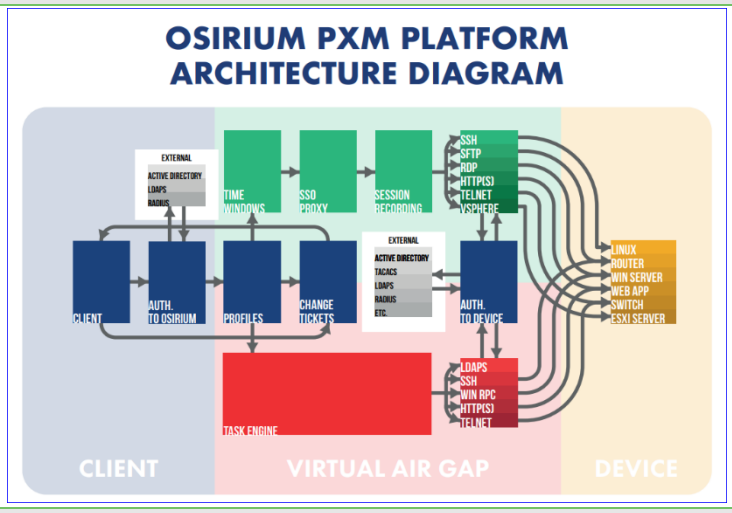
Osirium's PxM platform offers four modules: PAM, PTM, privileged session management (PSM) and privileged behaviour management (PBM). Exhibit 2 shows the platform architecture. The solution consists of software loaded on to a server (Osirium server) and an application that is

[4] IT service management

loaded on to the desktop of privileged users. The Osirium server is installed as a virtual appliance and acts as a proxy server between the privileged user and the end device. End devices managed by Osirium software include servers, routers, switches, databases and load balancers. Also available via the desktop client is the web management interface. This is the interface that allows the customer (ie the superadmin) to manage and implement role-based access controls.

Although many customers deploy Osirium's software on-premise, the software is also available on AWS and Azure for cloud deployment.

Exhibit 2: Osirium platform architecture

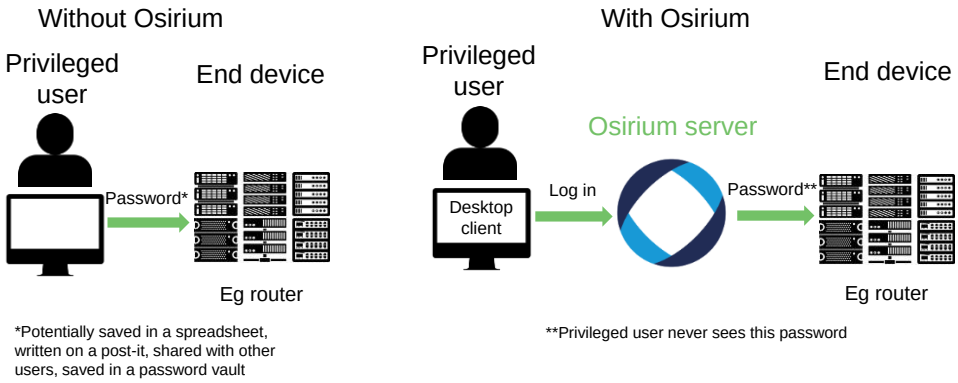


Source: Osirium

PAM

Once the superadmin has defined which devices the Osirium software will manage, the Osirium server connects to each of these devices using its library of device knowledge. The software identifies all the privileged accounts associated with each device. This means the superadmin can remove obsolete accounts (eg those belonging to leavers or used for test purposes) and assess whether privileges have been correctly assigned. Via the web management interface, the superadmin can grant privileged access to users.

Exhibit 3: Accessing an end device with or without Osirium software



Source: Edison Investment Research

All passwords for privileged accounts are saved on the Osirium server in the Osirium Keystore. When a privileged user wants to access a device, they must authenticate themselves on the Osirium server using the customer's preferred method, eg user password or two-factor authentication. The user is presented with a list of all devices for which they have privileged access and under each device they can see which tools and tasks they can access (as Osirium describes

it, 'Identity in, role out'). They then select the device they want to access and the Osirium server provides the correct password to the device. This is the Osirium virtual 'air gap' – the user never actually sees the passwords for the privileged accounts. Instead, as long as the user's identity is verified by the Osirium server, they can access all their privileged accounts with the passwords never making their way on to the user's workstation. Analysis by Verizon in 2014 calculated that 86% of passwords are obtained from user workstations, with only 10% via phishing and 4% from brute force (ie repeatedly guessing the password until the correct one is found). If the password is not available on a workstation, this significantly reduces the ability of a hacker to obtain it. Other features of the PAM module include:

- **Password management.** Passwords can be managed by the Osirium server in several ways. Initially, customers often set up the server to use existing passwords and manage the life-cycling of passwords themselves. Once comfortable with using the software, customers often switch to password-management mode, which means the Osirium software takes care of the password life-cycling – this is more secure as no users would know the passwords to any devices.
- **Integration with ticket management software**. To provide an additional level of security, the Osirium Change Management tool requests a change/incident ticket reference and comment before a task or tool is opened by a user. Once the ticket has been opened, all subsequent connections and tasks are tracked under this ticket reference. Multiple tools and tasks can be used under each ticket, and multiple users can work under the same ticket. Admin reports show all connections made under each ticket reference. Osirium can be integrated with ServiceNow to validate ticket references entered into the Osirium Change Management tool.
- **'Plays well with' automatic device enrolment.** Each time Osirium engineers encounter a new device they have not seen before, they go through a process to register it so it is compatible with Osirium's software. It is then automatically added to the 'Plays well with' list that contains all devices that can managed by the Osirium server.
- **Providing security for legacy applications and operating systems.** Osirium's MAP server is an innovative way to enable customers to continue to use devices that rely on legacy applications and operating systems. Companies often have key business processes or devices that rely on software that is no longer supported by the original software vendor. This legacy software could contain vulnerabilities and could therefore be a key target for hackers. Sysadmins often end up installing a variety of different legacy applications and different versions of operating systems either on their own machines or on dedicated (often shared) desktops, all of which increase the risk of a security breach. The user loads the legacy software management application on to the MAP server. When the user wants to access a device that uses legacy software, the Osirium server will determine which management tool is required and will project its window onto the user's workstation. This means the user is isolated from the legacy software. Instead only the Osirium server is allowed to communicate with the MAP server, effectively isolating it and creating a 'security cell' for the legacy software.

PTM – automating simple tasks

The PTM software enables a business to automate frequently performed tasks that require privileged access such as user password resets or switching/closing off firewall ports. This enables companies to delegate the task rather than the privilege, ie the user will be able to perform specific tasks on a device but will not have more general privileged access to the device. We view this is a form of robotic process automation, with the focus on security.

Analysis of the use of task automation by several customers has shown that time savings of up to 98% per task are possible, which has the benefit of freeing up staff to undertake more complex work. By predefining tasks and reducing the amount of user input required, accuracy is greatly increased, which improves both efficiency and security. This is particularly helpful for companies

that outsource a high volume of support activity, as it means third parties do not need to be granted as much privileged access. An MSSP can delegate the top 20 or 30 tasks to first-line support, sure in the knowledge the tasks will be performed securely and accurately. As long as the user is authenticated by the Osirium server, the user will then have access to all their individual delegated tasks.

We understand that the level of task automation enabled by Osirium's software is well ahead of that offered by other PAM vendors and was the key reason for Gartner's inclusion of the company in its Cool Vendor list. This also ties in well with the fourth pillar of PAM best practice we refer to in the recent Gartner report (see page 5).

PSM – recording user activity

PSM software is designed to record sessions undertaken by a privileged user. The customer defines which user activities are recorded. This means that as well as knowing who accessed data, when and where, the business can track exactly what was done during each active session. The software records only the active window and only records when there is activity. It does this by taking one screenshot every second. So a privileged user could be logged into an account for an hour, but only actively interact with the account for five minutes – in this case the recording would show how long the user was logged in for, but would only record the live five minutes. This reduces storage requirements, but more importantly makes it easier for sessions to be reviewed in the event of an issue. Recorded sessions can be searched by keyword. The recording is usually set to show a red box around the window that is being recorded – this in itself can act as a deterrent to unauthorised behaviour. The red box can also be switched off so the user does not know they are being recorded. All keystrokes by the user are also logged. The company estimates that more than half of customers take this module, usually for audit or compliance reasons.

PBM – monitoring user behaviour

This module monitors a privileged user's behaviour to create a base line for 'normal' behaviour. For example, if someone accesses a device at an unusual time, this is flagged up. The software presents the results in terms of active threat (unusual activity) and latent risk (connections between people and high privileged device accounts that are never or rarely used).

Privileged process automation (PPA)

Over the last 18 months, Osirium has invested in developing its task automation technology to provide wider process automation functionality and in May launched its privileged process automation (PPA) solution. This was previously known by the project name, Opus. Based on several years' experience in providing privileged task automation technology and customer feedback, PPA provides a significantly more powerful approach to securing privileged process automation. New features and functionality include:

- Automation of wider processes by linking together a series of automated tasks.
- Co-ordination across different systems so that the user does not need to log in to each system separately, eg ServiceNow, Active Directory, Infoblox. It also enables the output from one system to be the input into another system, without human intervention.
- Human-guided processes. The system can ask the human operator for input where different options are available, or to deal with exceptions as they arise.
- Ability to access credentials from suppliers other than Osirium. As well as the ability to pull credentials from the PxM platform, PPA can also access credentials held in HashiCorp[5] vaults. Osirium can add access to other vault providers as required.

[5] HashiCorp is an open-source vault focused on DevOps infrastructure.

- Ability to be used with customers' existing tools ('bring your own code') and for tasks to be written in different programming languages. This allows a customer to re-use existing tasks and scripts, but also ensures no credentials are exposed within the tools.
- Provides a full audit trail of all operations, tracking who runs which processes, where and when.
- Use of containerisation to create different layers of security isolation. PPA allows for any API or library to be added to a container (previously only APIs or libraries created by Osirium were available in the PTM module). Older systems may need libraries with known issues and vulnerabilities that would not be allowed on the PxM Platform. With PPA, these can be neatly secured, isolated and controlled for use with only the relevant legacy systems.
- Improved integration with ServiceNow (IT service management software). A process can run without a ServiceNow ticket until the point at which a notable event or exception occurs, at which point a ticket can be raised as part of the task.
- Each task is given a unique URL identifier that can be included in the ITSM ticket.
- Permissions from the PxM platform can be mapped onto PPA.
- Long-running tasks do not have to be completed by the same operator – a task can be started during one operator's shift and continue into and be completed by an operator on the next shift.

Early adopters of PPA have found tasks that were complex enough to need second or third level administrators to deal with them can now be delegated to first-line support engineers.

Multiple use cases

The company highlighted a variety of use cases for PPA (see Exhibit 4). While we would expect PPA initially to be of interest to IT operations teams, it is possible that some privileged automated processes could ultimately be delegated to other business departments. For example, HR teams typically request that new joiners are provided with email addresses and added to particular email groups. PPA would allow the IT department to create an automated process to do this, which could be delegated to authorised HR staff and bypass the IT department entirely. PPA is also likely to be of interest to DevOps and NetOps teams.

Exhibit 4: Examples of automated processes enabled by PPA

New starter – developer	Network operations	Reset password
Create account in Active Directory	Update ports	Verify requesting user ID
Create virtual machines for development and test	Create DNS records	Set temporary password in Active Directory
Create development databases Create accounts in CI/CD tools	Configure routings, across different hardware vendor platforms	Set 'reset next log-in' flag Update ServiceNow ticket
Update HR records		

Source: Osirium

Widens addressable market

As PPA can operate using credential vaults other than Osirium's PxM platform, it can be used by customers using PAM software from a different vendor. Osirium has found that within some companies, different PAM software is used for different processes. This gives Osirium the potential to sell into all processes using PAM software rather than just those processes that depend on its PxM platform. The company is selling PPA as a separate module with per-user licensing. It can be licensed on its own or alongside the PxM platform. Osirium signed up its first customer for PPA in August – this is an existing PxM customer.

PEM – protecting the endpoint

Osirium has developed a privileged endpoint management (PEM) solution that it expects to launch in Q4. An endpoint is a remote computing device that communicates with the network to which it is connected. Examples include desktops, laptops, smartphones, tablets, workstations and servers.

Endpoints often represent a vulnerable entry point for hackers, giving them the ability to take control of the device (for example to launch a botnet), to use the device as an entry point into an organisation, to access data on the device, or to hold the device owner to ransom. Anti-virus software is commonly used to protect endpoints, but this may not be sufficient to fully secure the device. Endpoints need administrator rights (ie privileged access) to perform certain functions, eg downloading new applications or updating existing applications. A business must weigh up the risk of giving the user these admin rights with the cost of reduced productivity if the user has to request permission to access commonly used applications or resources. PEM software is designed to enforce least privilege ie all local admin rights are removed from the user and only whitelisted applications can be run with elevated privilege. When necessary, the user can request elevated privilege from the IT support desk – this can be on a permanent or time-limited basis.

Last year Osirium announced a strategic technology partnership with RazorSecure to jointly deliver cybersecurity solutions specifically for the critical national infrastructure (CNI), transport and industrial internet of things markets. RazorSecure develops machine-learning-based EPM software – this builds a baseline of 'normal' activity to define what processes and applications are expected, how they are likely to use resources and therefore making it easier to identify rogue behaviour. RazorSecure's technology is used in CNI, in particular in the rail network, where it is able to detect intrusion and generate automated responses on systems that are not always connected. RazorSecure has adapted its EPM software for use by Osirium, with Osirium's new PEM solution due for official launch in Q4. The product will be licensed on a per-user basis.

As for PPA, the PEM solution can be sold independently of the PxM platform, thereby widening Osirium's addressable market. We would expect, however, that the company would initially market the solution to its existing customer base – it expects to sign its first customer by year end.

Technology roadmap

The R&D team develops enhancements to the PxM platform continuously and we would expect it to continue to develop the new PPA and PEM products as customers provide feedback. The company is developing the ability to cluster instances of Osirium servers together ('mesh') to ensure high availability, based on the concept of a Raft database.[6] This means that a much higher number of devices could be managed by an installed instance. The goal is that the servers should be able to communicate with each other to enforce the rule that there is only one instance of an ID at any one time. This should also provide fault tolerance, with the ability to reconfigure the mesh in the event of any of the clustered servers failing.

The company invests in patent applications to cover several of its key technologies. It has four active patent families with global reach, and a focus on the US and Europe. Osirium was recently granted a European-wide patent providing a wide scope of protection covering its password recovery process. US patent grant is expected in the next six to 12 months.

Direct and partner-driven sales strategy

Enterprise customers – direct sales

As well as the management team having direct relationships with enterprise and MSSP customers, the company has several telesales people and uses marketing automation tools. To help build the brand, the company has invested in the website and digital marketing, holds regular webinars and presents at industry conferences.

[6] The Raft protocol helps to maintain consensus in a distributed network of servers.

Few customers can be named owing to commercial confidentiality. In August 2016, Osirium signed up a global asset manager on a three-year contract to secure 3,000 devices – this was renewed for a further three years in May and over the last three years the contract has been expanded to cover 4,500 devices. This week, the company announced that an existing customer (a UK provider of software and IT services to the public sector) that had signed up in February to secure 250 devices for 12 months had expanded the contract to a total of 2,600 devices over three years.

Other customers include ThinkMoney (financial services), English police forces, a European car manufacturer, several NHS trusts, a multi-national defence company, a global mobile network operator, a reinsurer, several retailers (online and bricks and mortar), British universities and a professional services provider. The relationships with these direct enterprise customers give Osirium the opportunity to learn what additional features customers may require and helps shape the R&D process.

Accessing the mid-market via channel partners

The company recently hired a channel director to manage distributors and resellers, an important route to market for Osirium. A crucial part of the process is providing training and support to distributors and resellers so they are able to sell and install the software. Progress in building the channel includes:

- UK: Osirium is partnered with Progress Distribution.
- Middle East and North Africa: Osirium is partnered with Spectrami.

Osirium also runs a reseller partner programme that currently comprises 16 partners. The company is not directly targeting the US as this is a notoriously difficult market for non-US companies to crack and is the home market of the highest number of competitors. Nevertheless, Osirium software is already in use in the US and we expect penetration to increase as Osirium signs up more multi-national customers.

Sensitivities

Osirium's financial performance and share price will be sensitive to the following factors:

- **The pace of adoption of software.** This includes the rate at which new direct customers are signed up, the rate at which MSSPs expand the use of Osirium's software to their own customer bases, the rate at which distributors sell Osirium's software and the rate at which existing customers upgrade the number of devices using the software.
- **Renewal rates.** Osirium has historically had a high renewal rate (>90%); staying at this high level will be key to maintaining the high level of recurring revenues.
- **Pricing ability.** Osirium bundles several modules within one licence fee. The company intends to sell these modules separately in the future and the ability to price these appropriately will influence the adoption rate and profitability.
- **Ability to hire.** Cybersecurity engineers are in strong demand and therefore can be expensive to hire.
- **Competition.** There is already an active market for PAM software and several well-established and well-funded competitors.
- **Funding requirements.** The company will require additional funding before it reaches breakeven. This could result in dilution for existing shareholders.

Financials

Subscription-based business model

Osirium sells its software on a subscription basis. Customers typically buy a licence for 12 months and pay in full upfront. A small number of customers sign up for three years, with some paying the whole amount in advance and others billed annually. There are one or two customers paying monthly as device numbers increase. The majority of customers deploy the software on-premise, although now that the software is available on AWS and Azure, we expect cloud deployment to increase in popularity.

PxM licences are typically priced on the basis of the number of devices managed, with the minimum licence for 50 devices. Currently, the PAM and PTM modules come under one licence with PSM requiring a separate additional licence. PBM is bundled in with PAM/PTM but the company plans to make this available as a standalone module. Osirium has a 'land and expand' strategy. It typically aims to sell a licence to a customer for a minimum number of devices to resolve a specific problem; once the customer is comfortable with the technology, this can be expanded to include more devices, and additional modules such as PSM. PPA and PEM are licensed on a per-user basis.

The company generates some service-based revenues (10–15% of total revenues), but this is not a target area for substantial growth. With the channel strategy, Osirium would expect the channel partner to undertake the implementation work.

Freemium product and proofs of concept to attract new business

At the end of 2017, Osirium launched a freemium product, PxM Express. This is designed to provide the full functionality of the PxM platform to businesses with up to 10 servers or network devices. The company also enters into proofs of concept with potential customers so they can trial the software for a limited period of time. Currently, c 80% of PoCs convert to an order.

Cost base reflects investment in R&D and sales and marketing

The largest cost is staff. Included in other operating costs are premises costs (rent of headquarters in Theale), sales and marketing costs and other admin costs. The company capitalises development costs; these are amortised over a five-year period, starting in the year of capitalisation.

Review of H119 results

We recently revised our forecasts when the company issued its half-year trading update in July. Revenues grew 11% y-o-y while bookings were 69% higher y-o-y. This resulted in a 70% increase in deferred income, reflecting the number of multi-year contracts signed in the period. The company retained 100% of customers in H1. Operating expenses (excluding depreciation and amortisation) were 17% higher reflecting an increase in headcount and higher spend on marketing events. The company had a net cash position of £0.89m at the end of H119 – this does not include the £0.47m R&D tax credit that has since been received.

Exhibit 5: Half-year highlights

£k	H119	H118	y-o-y
Bookings	1030.0	608.2	69%
Deferred income	1238.8	725.0	70%
SaaS revenues	427.8	387.4	10%
Services revenues	87.6	78.9	11%
Total revenues	**515.5**	**466.3**	**11%**
Operating expenses	(1,710.8)	(1,456.9)	17%
EBITDA	**(1,195.4)**	**(990.6)**	**21%**
Depreciation & amortisation	(514.3)	(373.2)	38%
Normalised operating profit	**(1,709.6)**	**(1,363.8)**	**25%**
Share-based payments	0.0	0.0	
Reported operating profit	(1,709.6)	(1,363.8)	25%
Net interest income	(0.4)	0.6	N/A
Normalised PBT	(1,710.0)	(1,363.2)	25%
PBT	(1,710.0)	(1,363.2)	25%
Tax	334.3	205.0	63%
Reported net income	**(1,375.7)**	**(1,158.2)**	**19%**
EPS - basic & diluted (p)	(10)	(9)	11%
Net cash	**889.6**	**3,337.2**	**-73%**

Source: Osirium

Outlook and changes to forecasts

The company expects to meet market expectations for bookings in FY19. We have increased our operating cost forecast for H219, FY20 and FY21 to reflect the amount spent in H119. We forecast a shift to a net debt position by year-end. If the company is able to accelerate bookings growth ahead of our forecast, this would have a positive impact on cash flow due to the upfront billing of subscriptions. The company has noted it is planning to raise funds in H2.

Exhibit 6: Changes to forecasts

£'k	FY19e Old	FY19e New	% Change	% y-o-y	FY20e Old	FY20e New	% Change	% y-o-y
Bookings	1,601.1	1,601.1	0.0%	36.0%	2,161.5	2,161.5	0.0%	35.0%
Revenues	1,250.7	1,251.0	0.0%	30.7%	1,830.3	1,819.3	(0.6%)	45.4%
EBITDA	(1,833.3)	(2,165.5)	18.1%	22.5%	(1,516.2)	(1,879.8)	24.0%	(13.2%)
EBITDA margin	-146.6%	-173.1%	18.1%		-82.8%	-103.3%	24.7%	
Normalised operating profit	(2,830.8)	(3,179.2)	12.3%	18.9%	(2,742.7)	(3,140.6)	14.5%	(1.2%)
Normalised operating profit margin	-226.3%	-254.1%	(27.8%)		-149.8%	-172.6%	(22.8%)	
Reported operating profit	(2,830.8)	(3,179.2)	12.3%	18.9%	(2,742.7)	(3,140.6)	14.5%	(1.2%)
Reported operating margin	-226.3%	-254.1%	(27.8%)		-149.8%	-172.6%	(22.8%)	
Normalised PBT	(2,830.8)	(3,179.2)	12.3%	18.8%	(2,742.7)	(3,140.6)	14.5%	(1.2%)
Reported PBT	(2,830.8)	(3,179.2)	12.3%	18.8%	(2,742.7)	(3,140.6)	14.5%	(1.2%)
Normalised net income	(2,360.9)	(2,651.4)	12.3%	16.9%	(2,331.3)	(2,669.5)	14.5%	0.7%
Reported net income	(2,360.9)	(2,651.4)	12.3%	16.9%	(2,331.3)	(2,669.5)	14.5%	0.7%
Normalised basic EPS (p)	(17.42)	(19.56)	12.3%	7.8%	(17.20)	(19.69)	14.5%	0.7%
Normalised diluted EPS (p)	(17.42)	(19.56)	12.3%	7.8%	(17.20)	(19.69)	14.5%	0.7%
Reported basic EPS (p)	(17.42)	(19.56)	12.3%	7.8%	(17.20)	(19.69)	14.5%	0.7%
Net debt/(cash)	197.0	531.1	169.7%	(122.3%)	2,754.6	3,468.0	25.9%	553.0%

Source: Edison Investment Research

Valuation

The share price has declined over the last year, reflecting a slower pace of bookings growth than originally expected. Compared to cybersecurity peers trading on an average EV/sales multiple of 4.6x this year's revenues and 4.2x next year, Osirium is now trading at a discount (FY19e 2.4x, FY20e 1.7x). In our view, the key factors to trigger upside will be evidence of bookings growth at least in line with expectations for this year and confirmation of funds raised.

As we do not expect Osirium to reach profitability within our forecast period, we use a reverse discounted cash flow analysis to calculate the assumptions underlying the current share price. With a WACC of 11% and a terminal growth rate of 3%, we arrive at the current share price using the following assumptions for the period after our 2019–2020 explicit forecasts:

- Bookings growth of 30% in 2021, 25% per year in 2022 and 2023, reducing thereafter to 20% with 29% recognition in the year invoiced and 95% of deferred income unwinding each year.
- Revenue growth: trending down from 29% in 2021 to 20% in 2028.
- EBITDA margin: hitting positive EBITDA in 2024, rising to 35% margin by 2028. This assumes the company continues to capitalise development costs at a similar rate over the period of the analysis. We note that this equates to a terminal EBIT margin of 15%, slightly below established software vendors. It also assumes that the company does not grow its cost base significantly until it has reached break-even.
- Working capital: negative working capital requirements due to the upfront payment subscription model.
- Capex (mainly capitalised development costs): we forecast this to reduce from 75% of sales in 2021 to 23% by 2028.

Sector consolidation highlights maturing market

The table below shows selected acquisitions in the PAM market – the pace of acquisitions accelerated last year. After Bomgar's spending spree, it is now of a similar size (in revenues) as CyberArk. We view this as confirmation that PAM is now understood to be a crucial part of a company's IT security.

Exhibit 7: Recent transactions in the PAM market

Date	Acquirer	Target	Deal details	Technology acquired
Aug-15	CyberArk	Cybertinel	$20m	Threat detection
Oct-15	CyberArk	ViewFinity	$30.5m	Least privilege management & application control
Dec-15	Bomgar	Pitbull Software	N/A	Password management
Mar-16	CyberArk	Agata Solutions	$3m	Deep packet inspection
May-17	CyberArk	Conjur	$42m	Dev ops security
Jan-18	One Identity	Balabit	$100m (est); forward price/sales c 3.4x	Privileged account management
Feb-18	Bomgar	Lieberman Software	N/A	Privileged account management
Mar-18	CyberArk	Vaultive	$18m (est)	Cloud data encryption platform
Apr-18	Francisco Partners	Bomgar	Bought from Thoma Bravo	
Jul-18	Bomgar	Avecto	Revs £23.5m (+51% y-o-y); deal value N/A	EPM
Jul-18	Thoma Bravo	Centrify	Bought majority stake from VC investors	Privileged account management
Jul-18	Okta	ScaleFT	N/A	Remote access management platform
Sep-18	Bomgar	BeyondTrust	Combined entity will have revenues of $310m, 19,000 customers	Privileged account management
Jul-19	Wallix	Trustelem	€1m cash	Cloud access management
Jul-19	Wallix	Simarks	€1.3m cash	Privilege elevation & delegation management

Source: Edison Investment Research, company data

Exhibit 8: Financial summary

£'k	2013	2014	2015	2016*	2017	2018	2019e	2020e
31 October/31 December	IFRS	IFRS	IFRS	IFRS	IFRS	IFRS	IFRS	IFRS
INCOME STATEMENT								
Revenue	120.0	207.0	290.2	477.6	647.6	957.5	1,251.0	1,819.3
EBITDA	(366.7)	(327.1)	(377.9)	(1,136.7)	(1,609.4)	(1,767.3)	(2,165.5)	(1,879.8)
Normalised operating profit	(679.4)	(714.3)	(790.7)	(1,725.6)	(2,296.8)	(2,674.8)	(3,179.2)	(3,140.6)
Amortisation of acquired intangibles	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Exceptionals	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Share-based payments	0.0	(184.3)	(56.4)	(96.9)	0.0	0.0	0.0	0.0
Reported operating profit	(679.4)	(898.5)	(847.1)	(1,822.5)	(2,296.8)	(2,674.8)	(3,179.2)	(3,140.6)
Net Interest	(35.2)	5.7	(9.9)	9.7	4.2	(0.6)	0.0	0.0
Joint ventures & associates (post tax)	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Exceptionals	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Profit Before Tax (norm)	(714.6)	(708.5)	(800.7)	(1,715.9)	(2,292.6)	(2,675.4)	(3,179.2)	(3,140.6)
Profit Before Tax (reported)	(714.6)	(892.8)	(857.1)	(1,812.8)	(2,292.6)	(2,675.4)	(3,179.2)	(3,140.6)
Reported tax	137.7	134.1	121.0	453.3	409.4	407.6	527.7	471.1
Profit After Tax (norm)	(576.9)	(602.1)	(687.6)	(1,286.9)	(1,883.2)	(2,267.8)	(2,651.4)	(2,669.5)
Profit After Tax (reported)	(576.9)	(758.7)	(736.0)	(1,359.6)	(1,883.2)	(2,267.8)	(2,651.4)	(2,669.5)
Minority interests	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Discontinued operations	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Net income (normalised)	(576.9)	(602.1)	(687.6)	(1,286.9)	(1,883.2)	(2,267.8)	(2,651.4)	(2,669.5)
Net income (reported)	(576.9)	(758.7)	(736.0)	(1,359.6)	(1,883.2)	(2,267.8)	(2,651.4)	(2,669.5)
Basic average number of shares outstanding (m)	0	1	10	10	10	13	14	14
EPS - normalised (p)	N/A	N/A	(6.61)	(12.38)	(18.12)	(18.14)	(19.56)	(19.69)
EPS - normalised fully diluted (p)	N/A	N/A	(6.61)	(12.38)	(18.12)	(18.14)	(19.56)	(19.69)
EPS - basic reported (p)	(296.36)	(144.92)	(7.08)	(13.08)	(18.12)	(18.14)	(19.56)	(19.69)
Dividend (p)	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Revenue growth (%)	26.3	72.6	40.2	64.6	35.6	47.9	30.7	45.4
EBITDA Margin (%)	-305.7	-158.0	-130.2	-238.0	-248.5	-184.6	-173.1	-103.3
Normalised Operating Margin	-566.3	-345.0	-272.5	-361.3	-354.7	-279.4	-254.1	-172.6
BALANCE SHEET								
Fixed Assets	815.7	805.2	799.7	1,178.8	1,812.1	2,360.2	3,021.5	3,490.8
Intangible Assets	808.6	795.7	793.3	1,134.5	1,731.9	2,307.2	2,944.6	3,414.8
Tangible Assets	7.2	9.5	6.4	44.3	80.2	52.9	76.9	75.9
Investments & other	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Current Assets	109.3	269.2	428.1	3,953.7	1,646.4	3,134.6	288.2	(2,461.9)
Stocks	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Debtors	77.2	218.6	154.6	380.9	622.6	748.0	819.3	1,006.1
Cash & cash equivalents	32.2	50.6	273.5	3,572.8	1,023.8	2,386.6	(531.1)	(3,468.0)
Other	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Current Liabilities	(235.2)	(294.2)	(365.0)	(648.5)	(857.7)	(1,170.3)	(1,636.7)	(2,025.4)
Creditors	(235.2)	(294.2)	(365.0)	(648.5)	(857.7)	(1,170.3)	(1,636.7)	(2,025.4)
Tax and social security	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Short term borrowings	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Other	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Long Term Liabilities	(952.5)	(487.6)	(163.3)	0.0	0.0	0.0	0.0	0.0
Long term borrowings	(789.0)	(323.7)	0.0	0.0	0.0	0.0	0.0	0.0
Other long term liabilities	(163.4)	(163.9)	(163.3)	0.0	0.0	0.0	0.0	0.0
Net Assets	(262.6)	292.6	699.5	4,483.9	2,600.8	4,324.5	1,673.0	(996.5)
Minority interests	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Shareholders' equity	(262.6)	292.6	699.5	4,483.9	2,600.8	4,324.5	1,673.0	(996.5)
CASH FLOW								
Op Cash Flow before WC and tax	(366.7)	(327.1)	(377.9)	(1,136.7)	(1,609.4)	(1,767.3)	(2,165.5)	(1,879.8)
Working capital	66.3	3.8	120.7	226.8	85.5	187.2	395.1	201.8
Exceptional & other	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Tax	109.8	48.4	134.6	120.4	291.4	407.6	527.7	471.1
Net operating cash flow	(190.6)	(274.9)	(122.6)	(789.4)	(1,232.5)	(1,172.5)	(1,242.6)	(1,206.9)
Capex	(412.8)	(376.7)	(407.3)	(968.0)	(1,320.6)	(1,455.7)	(1,675.0)	(1,730.0)
Acquisitions/disposals	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Net interest	(35.2)	5.7	(9.9)	9.7	4.2	(0.6)	0.0	0.0
Equity financing	0.0	639.3	762.8	5,047.1	0.0	3,991.5	0.0	0.0
Dividends	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Other	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Net Cash Flow	(638.6)	(6.5)	222.9	3,299.3	(2,549.0)	1,362.8	(2,917.6)	(2,936.9)
Opening net (cash)/debt	118.3	756.9	273.1	(273.5)	(3,572.8)	(1,023.8)	(2,386.6)	531.1
FX	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Other non-cash movements	0.0	490.3	323.8	0.0	0.0	(0.1)	(0.0)	0.0
Closing net (cash)/debt	756.9	273.1	(273.5)	(3,572.8)	(1,023.8)	(2,386.6)	531.1	3,468.0

Source: Osirium, Edison Investment Research. Note: *14-month period.

Contact details	Revenue by geography
Theale Court, 11–13 High Street Theale, Reading Berkshire, RG7 5AH UK 0118 3242444 www.osirium.com	

Management team

CEO: David Guyatt

The management team is led by David Guyatt, co-founder of Osirium. He has over 25 years' experience in turning next-generation IT products into successful technology businesses. He is a recognised pioneer in establishing the content security software market, as co-founder and CEO of MIMEsweeper, which became the recognised world leader in content security solutions, with a 40% global market share. He was sales & marketing director at Integralis (1990–96) as it established itself as the Europe's leading IT security integrator.

CFO: Rupert Hutton

Rupert joined Osirium in 2015. He served for 12 years as finance director of AIM-quoted Atlantic Global, a cloud-based project management service, before it was sold to a US-based software company. Previously, Rupert was group financial controller of the Milton Keynes and North Bucks Chamber of Commerce. His early career and formal training took place with Grant Thornton and he has an AMBA accredited master's in business administration and is a fellow of the Association of Chartered Certified Accountants.

CTO: Andrew Harris

Andy joined Osirium in 2011. He has over 25 years' experience inventing and building unique IT networking and security products, including leading-edge technologies including IP network translation gateway, print symbiont technologies for LAN-based printers, and Disaster Master, a technique of continuously updating a backup site with mirrored data. He was technical director at Integralis and one of the co-founders and CTO of MIMEsweeper. He created the world's first content security solution, which became the default product in its sector. He went on to start WebBrick Systems, which was one of the pioneering home automation technologies, also a forerunner to what we know as IOT devices today. As engineering director Andrew has created and patented several core components in the Osirium product family.

Chairman: Simon Lee

Simon Lee is an international adviser to Fairfax Financial, where he sits on the boards of Brit Syndicates and Advent Underwriting. He is also on the Global Advisory Board to Afiniti Inc, non-executive director of TIA Technology and chairman of Hospice in the Weald. Until December 2013, Simon was group chief executive of RSA Insurance Group plc, a FTSE 100 company, operating at the time in 32 countries, employing around 23,000 people, writing c £9bn in premiums with assets of c £21bn. Previously, Simon spent 17 years with NatWest Group, working in a variety of roles including; chief executive NatWest Offshore, head of US Retail Banking, CEO NatWest Mortgage Corporation (US) and director of Global Wholesale Markets.

Principal shareholders	(%)
Octopus Investments	17.2
Canaccord Genuity Wealth Management	11.9
Harwell Capital	11.3
1798 Volantis	10.4
Unicorn Asset Management	10.2
Osirium directors and related parties	9.0
GAM London	5.6
Rathbone Investment Management	4.9
Herald Investment Management	3.7

Companies named in this report

CyberArk, Beyond Trust, Centrify, Micro Focus, Wallix

General disclaimer and copyright

This report has been commissioned by Osirium Technologies and prepared and issued by Edison, in consideration of a fee payable by Osirium Technologies. Edison Investment Research standard fees are £49,500 pa for the production and broad dissemination of a detailed note (Outlook) following by regular (typically quarterly) update notes. Fees are paid upfront in cash without recourse. Edison may seek additional fees for the provision of roadshows and related IR services for the client but does not get remunerated for any investment banking services. We never take payment in stock, options or warrants for any of our services.

Accuracy of content: All information used in the publication of this report has been compiled from publicly available sources that are believed to be reliable, however we do not guarantee the accuracy or completeness of this report and have not sought for this information to be independently verified. Opinions contained in this report represent those of the research department of Edison at the time of publication. Forward-looking information or statements in this report contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter to be materially different from current expectations.

Exclusion of Liability: To the fullest extent allowed by law, Edison shall not be liable for any direct, indirect or consequential losses, loss of profits, damages, costs or expenses incurred or suffered by you arising out or in connection with the access to, use of or reliance on any information contained on this note.

No personalised advice: The information that we provide should not be construed in any manner whatsoever as, personalised advice. Also, the information provided by us should not be construed by any subscriber or prospective subscriber as Edison's solicitation to effect, or attempt to effect, any transaction in a security. The securities described in the report may not be eligible for sale in all jurisdictions or to certain categories of investors.

Investment in securities mentioned: Edison has a restrictive policy relating to personal dealing and conflicts of interest. Edison Group does not conduct any investment business and, accordingly, does not itself hold any positions in the securities mentioned in this report. However, the respective directors, officers, employees and contractors of Edison may have a position in any or related securities mentioned in this report, subject to Edison's policies on personal dealing and conflicts of interest.

Australia

Edison Investment Research Pty Ltd (Edison AU) is the Australian subsidiary of Edison. Edison AU is a Corporate Authorised Representative (1252501) of Crown Wealth Group Pty Ltd who holds an Australian Financial Services Licence (Number: 494274). This research is issued in Australia by Edison AU and any access to it, is intended only for "wholesale clients" within the meaning of the Corporations Act 2001 of Australia. Any advice given by Edison AU is general advice only and does not take into account your personal circumstances, needs or objectives. You should, before acting on this advice, consider the appropriateness of the advice, having regard to your objectives, financial situation and needs. If our advice relates to the acquisition, or possible acquisition, of a particular financial product you should read any relevant Product Disclosure Statement or like instrument.

New Zealand

The research in this document is intended for New Zealand resident professional financial advisers or brokers (for use in their roles as financial advisers or brokers) and habitual investors who are "wholesale clients" for the purpose of the Financial Advisers Act 2008 (FAA) (as described in sections 5(c) (1)(a), (b) and (c) of the FAA). This is not a solicitation or inducement to buy, sell, subscribe, or underwrite any securities mentioned or in the topic of this document. For the purpose of the FAA, the content of this report is of a general nature, is intended as a source of general information only and is not intended to constitute a recommendation or opinion in relation to acquiring or disposing (including refraining from acquiring or disposing) of securities. The distribution of this document is not a "personalised service" and, to the extent that it contains any financial advice, is intended only as a "class service" provided by Edison within the meaning of the FAA (i.e. without taking into account the particular financial situation or goals of any person). As such, it should not be relied upon in making an investment decision.

United Kingdom

This document is prepared and provided by Edison for information purposes only and should not be construed as an offer or solicitation for investment in any securities mentioned or in the topic of this document. A marketing communication under FCA Rules, this document has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research.

This Communication is being distributed in the United Kingdom and is directed only at (i) persons having professional experience in matters relating to investments, i.e. investment professionals within the meaning of Article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005, as amended (the "FPO") (ii) high net-worth companies, unincorporated associations or other bodies within the meaning of Article 49 of the FPO and (iii) persons to whom it is otherwise lawful to distribute it. The investment or investment activity to which this document relates is available only to such persons. It is not intended that this document be distributed or passed on, directly or indirectly, to any other class of persons and in any event and under no circumstances should persons of any other description rely on or act upon the contents of this document.

This Communication is being supplied to you solely for your information and may not be reproduced by, further distributed to or published in whole or in part by, any other person.

United States

The Investment Research is a publication distributed in the United States by Edison Investment Research, Inc. Edison Investment Research, Inc. is registered as an investment adviser with the Securities and Exchange Commission. Edison relies upon the "publishers' exclusion" from the definition of investment adviser under Section 202(a)(11) of the Investment Advisers Act of 1940 and corresponding state securities laws. This report is a bona fide publication of general and regular circulation offering impersonal investment-related advice, not tailored to a specific investment portfolio or the needs of current and/or prospective subscribers. As such, Edison does not offer or provide personal advice and the research provided is for informational purposes only. No mention of a particular security in this report constitutes a recommendation to buy, sell or hold that or any security, or that any particular security, portfolio of securities, transaction or investment strategy is suitable for any specific person.

Frankfurt +49 (0)69 78 8076 960
Schumannstrasse 34b
60325 Frankfurt
Germany

London +44 (0)20 3077 5700
280 High Holborn
London, WC1V 7EE
United Kingdom

New York +1 646 653 7026
1,185 Avenue of the Americas
3rd Floor, New York, NY 10036
United States of America

Sydney +61 (0)2 8249 8342
Level 4, Office 1205
95 Pitt Street, Sydney
NSW 2000, Australia