Osirium Technologies

Securing growth through PAM innovation

Osirium reported H118 results in line with management expectations. Revenue growth of 78% and bookings growth of 37% provide good support to our FY18 forecasts. Heightened M&A activity in the privileged access management (PAM) market highlights the growing importance of PAM technology in IT security and the greenfield opportunity for Osirium. The company continues to invest in R&D to maintain its innovative edge, with the next generation of its task automation software due for release early next year and a technology partnership with RazorSecure bringing endpoint privilege management to the portfolio.

Year end	Revenue (£m)	EBITDA* (£m)	EPS* (p)	DPS (p)	P/E (x)	EV/Sales (x)
12/16**	0.48	(1.14)	(12.4)	0.0	N/A	32.7
12/17	0.65	(1.61)	(18.1)	0.0	N/A	24.1
12/18e	0.92	(2.00)	(18.4)	0.0	N/A	16.9
12/19e	1.41	(1.82)	(17.4)	0.0	N/A	11.1

Note: *EBITDA and EPS are normalised, excluding amortisation of acquired intangibles, exceptional items and share-based payments. **14-month period ended 31 December 2016.

H118 results on track

In H118 Osirium reported revenue growth of 78%, bookings growth of 37% and an EBITDA loss of £0.99m, compared to a £0.91m loss a year ago. So far this year, Osirium's largest UK and international customers have renewed their contracts and the company has added new customers in the retail sector and the NHS. In total, 13 proofs of concept were underway by the end of H118. Net cash at the end of H1 stood at £3.3m. We have made small increases to our cost estimates to reflect the headcount added in H1.

Increasing focus on PAM market

Market analysts have put the spotlight on PAM as a priority for IT security, and recent acquisition activity has confirmed the relevance of the technology. Osirium invested in additional R&D headcount during H118 to continue to enhance its technology and in particular to ensure its task automation software remains ahead of the competition. A recent partnership with RazorSecure will give Osirium access to endpoint privilege management technology, widening its product offering. The company approaches the market with a parallel strategy of direct sales for enterprise customers combined with channel partnerships to serve the mid-market.

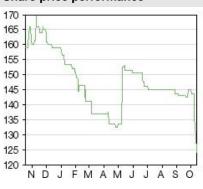## Valuation: Bookings progress the key driver

As an early-stage company showing revenue growth ahead of its peer group, Osirium is trading at a premium to peers on an EV/sales basis. 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 annual bookings growth of 24% for FY21–27, break-even EBITDA in FY23, average EBITDA margins of 12.8% for FY21–27 and a terminal EBITDA margin of 36.5%. In our view, bookings growth will be the key driver of share price performance.

Investment summary

Innovative PAM software vendor with land and expand strategy, moving into the mid-market

Osirium's privileged access management software helps protect critical IT infrastructure from unauthorised use of privileged IT accounts, whether from hacking or internal threats. Osirium's PxM software platform consists of four software modules and 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 management team has worked together for many years and has experience in commercialising cybersecurity software. Osirium is following a land and expand strategy – selling licences to enterprise customers to help resolve pain points, and then expanding licences to cover a larger number of end devices and additional modules. 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 PAM software than enterprises, so this is a market ripe for development. The company has distributors covering the UK, German-speaking European countries, the Middle East and North Africa, with orders already received via some of these partners. To support partners, Osirium has business development directors in those regions, and to support customers has 24/7 global technical support in place.

H118 on track; forecast changes reflect headcount investment

H118 results confirmed that bookings and revenues grew in line with expectations. The company had a net cash position of £3.3m at the end of H118. We have made minor changes to our forecasts, mainly to reflect the timing of headcount increases in H118. Our EBITDA forecast reduces from a loss of £1.85m to a loss of £2.00m in FY18 and from a loss of £1.65m to a loss of £1.82m in FY19. We forecast a net cash position of £2.49m at the end of FY18.

Valuation: Bookings progress the key driver

As an early-stage company showing revenue growth ahead of its peer group, Osirium is trading at a premium to peers on an EV/sales basis. 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 24% for FY21–27, break-even EBITDA in FY23, average EBITDA margins of 12.8% for FY21–27 and a terminal EBITDA margin of 36.5%. In our view, bookings growth will be the key driver 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 PAM software. While 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. The company is now 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 privileged access management 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 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 44.

Strategy: Expand into the mid-market

The 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, but where companies may not have the same level of IT resource to manage this risk. 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 privileged access management 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; Rupert served as CFO of AIM-listed Atlantic Global for 12 years.

Privileged access management

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 access and typically each device and application requires a separate user name and password for this (privileged account). 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, further extending the number of privileged account holders.

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 these 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[1] in 2018 estimated that 28% of attacks were perpetrated by insiders.

---

[1]   Verizon Data Breach Investigations Report, 2018

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) was adopted by the European Parliament in 2016 with full adoption by member states since May 2018; the UK has adopted the directive despite Brexit. Member states have until November 2018 to identify the relevant operators, ie operators of essential services (OES) in critical national infrastructure and digital service providers (DSPs). The directive requires OESs and 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.

Market forecasts are for strong growth

Gartner estimates that 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 of security priorities for CISOs[2] and named PAM as the number one priority. It is developing a Magic Quadrant for PAM (expected later this year), where previously it has only looked at the wider access management market, which is dominated by identity access management.

Competition

There is a well-established market for PAM software, with a number of competitors with a focus 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 since 1999, and is Osirium's biggest competitor in the enterprise market. In the mid-market space, Osirium traditionally competed more with smaller players Thycotic, Bomgar, BeyondTrust and Wallix. Over the last year, consolidation has accelerated with Bomgar buying several PAM vendors (see page 14) – it is now of a similar size to CyberArk. Customer numbers per Exhibit 2 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.

---

[2] Chief Information Security Officers

Exhibit 1: Competitive environment

Company	Ownership	Annual revenues	No. employees	HQ	Products	No. customers
PAM focused vendors						
CyberArk	Nasdaq: market cap $2.6bn	FY17 $262m, FY18e $323m	1,077	US	Privileged Account Security Solution	>4,000
Bomgar	Francisco Partners	Post acquisitions: $310m		US	Privileged Access, Password Vault, PowerBroker PAM platform, Secure Privileged Access Management*	19,000
Centrify	Thoma Bravo (majority stake)	FY17 $103m	c 500	US	Privileged Access Security	>5,000
Thycotic	Private; includes Insight Venture Partners	$26.6m		US	Secret Server, Privilege Manager	>10,000
Wallix	Euronext: market cap €127m	FY17 €11.5m	83	France	Wallix Bastion	577
Broad-based vendors						
CA Technologies	Nasdaq: market cap $18bn	FY18 $4.2bn	11,300	US	Privileged Access Manager	
Micro Focus	LSE: market cap £5.8bn	FY17 $1.38bn of which $207m from Identity, Access & Security	16,000	UK	Privileged Account Manager	
ManageEngine	Zoho Corporation (private)	N/A	4,000	US	Password Manager Pro	

Source: Edison Investment Research. Note: *Incorporates products from Bomgar, BeyondTrust and Lieberman Software.
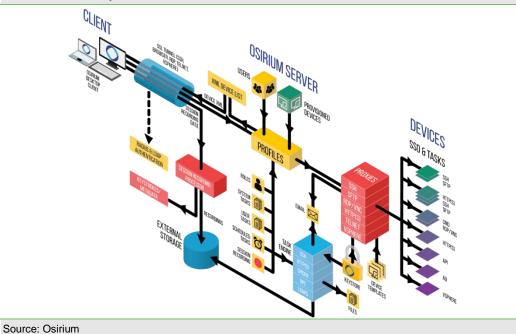
As Osirium is still at an early stage in terms of revenue generation, it has not featured heavily in the market research reports from Gartner and KuppingerCole. However, last year Gartner named Osirium a Cool Vendor in Identity and Fraud Management, in particular because of its approach to task automation. Gartner defines Cool Vendors as disruptive vendors that are helping companies to solve long-established problems and stay ahead of the competition in a rapidly changing world.

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.

Osirium's PxM platform

Exhibit 2 shows the platform architecture.

Exhibit 2: Osirium platform architecture
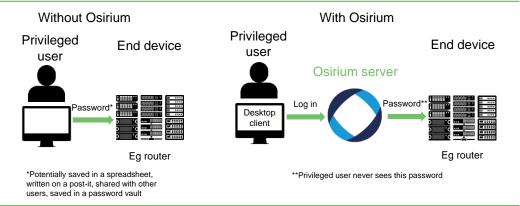

Source: Osirium

Osirium's PxM 6.1.0 platform offers four modules: privileged access management (PAM), privileged task management (PTM), privileged session management (PSM) and privileged behaviour management (PBM). The solution consists of software loaded on to a server (Osirium server) and an application that is loaded onto 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 company has also made its software available on AWS and Azure for cloud deployment.

Privileged access management (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

Without Osirium

Privileged user — End device

Password*

Eg router

*Potentially saved in a spreadsheet, written on a post-it, shared with other users, saved in a password vault

With Osirium

Privileged user — Osirium server — End device

Desktop client — Log in — Password** — Eg router

**Privileged user never sees this password

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 onto 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.

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 onto 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 that 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

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 that 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.

PSM

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

This is Osirium's newest module. The idea is that privileged user behaviour is monitored 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).

Technology roadmap

The R&D team develops enhancements to the PxM platform on a continuous basis. Over the last year, this has included further development of the MAP solution for legacy software, introducing Elastic Stack to reduce the processing load on a customers' infrastructure generated by behaviour analytics undertaken by the PBM module, and adding 'App-less' access for third parties (a web access gateway). This provides a web connection between a third party (typically an outsourcer) and the customer's infrastructure such that the third party does not need to run the customer's applications on their own infrastructure.

Other significant projects that are underway include:

- **Project OPUS:** this is the development of the next generation of task automation. This will add the ability to deal with tasks that go wrong during run-time, eg the expected firewall has been swapped out for a different supplier so the task does not complete. Osirium is working to develop software that would identify the issue and automatically update the task. The company is aware that in many companies, developers are writing their own tasks in a multitude of different languages. The company is developing software that rates the security of this code, and suggests improvements to it to make it more secure and more effective.

- **Endpoint privilege management (EPM)**. Osirium recently 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 endpoint privilege management 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 is also going to adapt its EPM software for use by Osirium, who will resell it as part of its PxM platform. EPM functionality has been requested by customers and this relationship will bring it to Osirium's product range faster than if Osirium were to develop it in-house.

■ **Multi-factor authentication**. Osirium is working to expand the number of multi-factor authentication companies its software can integrate with.

■ **Clustering**. The company is developing the ability to cluster instances of Osirium servers together to ensure high availability, based on the concept of a Raft database[3]. This should mean 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.

In January 2016, the company filed three patents in the area of privileged access and related automation innovation in the UK, Europe and the US; it is hard to predict when the final decision will be made whether to grant the patents – the process can take up to five years from filing.

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. The company recently hired a new marketing director, Chris Heslop, who has previously worked with the team at MIMEsweeper and more recently held senior positions in field marketing for Vocollect and Honeywell.

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 has been renewed twice since the original contract and expanded to cover a larger number of devices. Other customers include ThinkMoney (financial services), two 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) 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 has signed up distributors in key geographies. A crucial part of the process is providing training and support to distributors and resellers so that they are able to sell and install the software. Business development directors have been hired in the Middle East, Asia-Pacific and Germany. Progress in building the channel includes:

■ UK: Osirium partnered with Progress Distribution from the start of 2018.

■ Middle East and North Africa: Osirium is partnered with Spectrami.

■ Germany: Osirium is partnered with Adyton to cover the DACH region (Germany, Switzerland, and Austria).

Osirium also runs a partner programme, and by the end of H118 this comprised 12 partners in the UK. The company is not directly targeting the US. This is a notoriously difficult market for non-US

---

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

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 may 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 being billed annually. There are one or two customers paying on a monthly basis 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.

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.

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.

Early days for freemium product

At the end of last year, Osirium launched a freemium product, PxM Express. This is designed to provide the full functionality of the PxM platform to businesses with up to 25 servers or network devices. It can also be deployed by larger organisations looking to test the software prior to making

a wider investment decision. It has 17 customers using this product – it is too soon to ascertain the conversion rate to the paid product.

Cost base reflects investment in R&D

The largest cost is for staff; having added headcount during H118, the company does not expect to increase headcount materially from this point. 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 H118 results

Osirium traded in line with management expectations in H118. Bookings increased 37% y-o-y and revenues increased 78% over the same period. Within that SaaS software revenues increased 87% and revenues from services 46%. As indicated when the company raised funds in March, it has increased headcount to support product development, customer support and sales and marketing. This has resulted in an increase in operating expenses (excluding depreciation and amortisation) of 25% y-o-y. The EBITDA loss was marginally higher y-o-y at £991k. The company capitalised development costs of £589k in H118 and amortised £353k. The company closed H118 with a net cash position of £3.3m, benefiting from the March fundraise which netted proceeds of £4.0m.

Exhibit 4: Half-yearly results			
£k	H118	H117	y-o-y
Bookings	**608.2**	**445.2**	**37%**
Deferred income	646.3	459.6	41%
SaaS revenues	**387.4**	**207.4**	**87%**
Services revenues	**78.9**	**54.2**	**46%**
Total revenues	**466.3**	**261.6**	**78%**
Operating expenses	(1,456.9)	(1,168.5)	25%
EBITDA	**(990.6)**	**(906.9)**	**9%**
Depreciation & amortisation	(373.2)	(277.4)	35%
Normalised & reported operating profit	(1,363.8)	(1,184.3)	15%
Net interest income	0.6	2.4	-76%
Normalised & reported PBT	(1,363.2)	(1,181.9)	15%
PBT	(1,363.2)	(1,181.9)	15%
Tax	205.0	175.0	17%
Normalised & reported net income	(1,158.2)	(1,006.9)	15%
EPS - basic & diluted (p)	(9)	(11)	-18%
Net cash	**3,337.2**	**2,015.9**	**66%**

Source: Osirium. Note: *14-month period ended 31 December 2016.

Outlook and changes to forecasts

We have made minimal changes to forecasts post H118 results. We have increased our operating cost forecast for H218, FY19 and FY20 to reflect the pace of hiring in H118. We estimate that the company has sufficient cash to fund the business until FY20. If it 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.

Exhibit 5: Changes to forecasts

£000s	FY18e Old	FY18e New	Change	y-o-y	FY19e Old	FY19e New	Change	y-o-y	FY20e Old	FY20e New	Change	y-o-y
Bookings	1314.5	1,314.5	0.0%	50.0%	1840.3	1,840.3	0.0%	40.0%	2484.4	2,484.4	0.0%	35.0%
Revenues	902.6	922.6	2.2%	42.5%	1,404.7	1,406.7	0.1%	52.5%	1,957.7	1,957.9	0.0%	39.2%
EBITDA	(1,845.2)	(1,995.5)	8.1%	24.0%	(1,645.3)	(1,816.0)	10.4%	(9.0%)	(1,257.9)	(1,432.6)	13.9%	(21.1%)
EBITDA margin	*-204.4%*	*-216.3%*	*5.8%*		*-117.1%*	*-129.1%*	*10.2%*		*-64.3%*	*-73.2%*	*13.9%*	
Normalised operating profit	(2,758.7)	(2,759.0)	0.0%	20.1%	(2,775.2)	(2,775.8)	0.0%	0.6%	(2,596.8)	(2,581.6)	(0.6%)	(7.0%)
Normalised operating profit margin	*-305.7%*	*-299.1%*	*6.6%*		*-197.6%*	*-197.3%*	*0.2%*		*-132.6%*	*-131.8%*	*0.8%*	
Reported operating profit	(2,758.7)	(2,759.0)	0.0%	20.1%	(2,775.2)	(2,775.8)	0.0%	0.6%	(2,596.8)	(2,581.6)	(0.6%)	(7.0%)
Reported operating margin	*-305.7%*	*-299.1%*	*6.6%*		*-197.6%*	*-197.3%*	*0.2%*		*-132.6%*	*-131.8%*	*0.8%*	
Normalised PBT	(2,756.7)	(2,757.0)	0.0%	20.3%	(2,774.2)	(2,774.8)	0.0%	0.6%	(2,596.8)	(2,581.6)	(0.6%)	(7.0%)
Reported PBT	(2,756.7)	(2,757.0)	0.0%	20.3%	(2,774.2)	(2,774.8)	0.0%	0.6%	(2,596.8)	(2,581.6)	(0.6%)	(7.0%)
Normalised net income	(2,343.2)	(2,343.5)	0.0%	24.4%	(2,358.1)	(2,358.6)	0.0%	0.6%	(2,207.3)	(2,194.3)	(0.6%)	(7.0%)
Reported net income	(2,343.2)	(2,343.5)	0.0%	24.4%	(2,358.1)	(2,358.6)	0.0%	0.6%	(2,207.3)	(2,194.3)	(0.6%)	(7.0%)
Normalised basic EPS	(18.37)	(18.38)	0.0%	1.4%	(17.42)	(17.42)	0.0%	(5.2%)	(16.30)	(16.21)	(0.6%)	(7.0%)
Normalised diluted EPS	(18.37)	(18.38)	0.0%	1.4%	(17.42)	(17.42)	0.0%	(5.2%)	(16.30)	(16.21)	(0.6%)	(7.0%)
Reported basic EPS	(18.37)	(18.38)	0.0%	1.4%	(17.42)	(17.42)	0.0%	(5.2%)	(16.30)	(16.21)	(0.6%)	(7.0%)
Net debt/(cash)	(2,465.4)	(2,494.9)	1.2%	143.7%	(65.9)	(28.1)	(57.3%)	(98.9%)	1,863.2	1,972.6	5.9%	N/A

Source: Edison Investment Research

Valuation

As we do not expect Osirium to reach profitability within our three-year 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 2018–2020 explicit forecasts:

■ Bookings growth of 30% per year from 2021 to 2023, reducing thereafter to 15% by 2027 with 25% recognition in the year invoiced and 90% of deferred income unwinding each year.

■ Revenue growth: trending down from 33.7% in 2021 to 18.7% in 2027.

■ EBITDA margin: hitting positive EBITDA in 2023, rising to 36.5% margin by 2027. 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 19.3%, in line with 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: we forecast this to reduce from 56% of sales in 2021 to 17% by 2027.

PAM-related acquisitions accelerate in 2018

The table below shows selected acquisitions in the PAM market – the pace of acquisitions has accelerated this year. After Bomgar's spending spree, it is now of a similar size (in revenues) as CyberArk.

Exhibit 6: 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	Endpoint privilege management
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

Source: Edison Investment Research

Exhibit 7: Financial summary

£'k	2013	2014	2015	2016*	2017	2018e	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	922.6	1,406.7	1,957.9
EBITDA	(366.7)	(327.1)	(377.9)	(1,136.7)	(1,609.4)	(1,995.5)	(1,816.0)	(1,432.6)
Normalised operating profit	(679.4)	(714.3)	(790.7)	(1,725.6)	(2,296.8)	(2,759.0)	(2,775.8)	(2,581.6)
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)	(2,759.0)	(2,775.8)	(2,581.6)
Net Interest	(35.2)	5.7	(9.9)	9.7	4.2	2.0	1.0	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)	(2,757.0)	(2,774.8)	(2,581.6)
Profit Before Tax (reported)	(714.6)	(892.8)	(857.1)	(1,812.8)	(2,292.6)	(2,757.0)	(2,774.8)	(2,581.6)
Reported tax	137.7	134.1	121.0	453.3	409.4	413.6	416.2	387.2
Profit After Tax (norm)	(576.9)	(602.1)	(687.6)	(1,286.9)	(1,883.2)	(2,343.5)	(2,358.6)	(2,194.3)
Profit After Tax (reported)	(576.9)	(758.7)	(736.0)	(1,359.6)	(1,883.2)	(2,343.5)	(2,358.6)	(2,194.3)
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)	(2,343.5)	(2,358.6)	(2,194.3)
Net income (reported)	(576.9)	(758.7)	(736.0)	(1,359.6)	(1,883.2)	(2,343.5)	(2,358.6)	(2,194.3)
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)	(18.38)	(17.42)	(16.21)
EPS - normalised fully diluted (p)	N/A	N/A	(6.61)	(12.38)	(18.12)	(18.38)	(17.42)	(16.21)
EPS - basic reported (p)	(296.36)	(144.92)	(7.08)	(13.08)	(18.12)	(18.38)	(17.42)	(16.21)
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	42.5	52.5	39.2
EBITDA Margin (%)	-305.7	-158.0	-130.2	-238.0	-248.5	-216.3	-129.1	-73.2
Normalised Operating Margin	-566.3	-345.0	-272.5	-361.3	-354.7	-299.1	-197.3	-131.8
BALANCE SHEET								
Fixed Assets	815.7	805.2	799.7	1,178.8	1,812.1	2,464.9	2,921.4	3,188.8
Intangible Assets	808.6	795.7	793.3	1,134.5	1,731.9	2,358.4	2,788.5	3,029.6
Tangible Assets	7.2	9.5	6.4	44.3	80.2	106.5	132.9	159.2
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	3,161.3	829.8	(1,048.9)
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	666.3	801.6	923.7
Cash & cash equivalents	32.2	50.6	273.5	3,572.8	1,023.8	2,494.9	28.1	(1,972.6)
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)	(1,376.0)	(1,859.6)	(2,413.6)
Creditors	(235.2)	(294.2)	(365.0)	(648.5)	(857.7)	(1,376.0)	(1,859.6)	(2,413.6)
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	4,250.2	1,891.6	(273.8)
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	4,250.2	1,891.6	(273.8)
CASH FLOW								
Op Cash Flow before WC and tax	(366.7)	(327.1)	(377.9)	(1,136.7)	(1,609.4)	(1,995.5)	(1,816.0)	(1,432.6)
Working capital	66.3	3.8	120.7	226.8	85.5	480.1	351.0	432.0
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	409.4	413.6	416.2
Net operating cash flow	(190.6)	(274.9)	(122.6)	(789.4)	(1,232.5)	(1,106.0)	(1,051.5)	(584.4)
Capex	(412.8)	(376.7)	(407.3)	(968.0)	(1,320.6)	(1,416.3)	(1,416.3)	(1,416.3)
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	2.0	1.0	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)	1,471.2	(2,466.8)	(2,000.7)
Opening net (cash)/debt	118.3	756.9	273.1	(273.5)	(3,572.8)	(1,023.8)	(2,494.9)	(28.1)
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)	(2,494.9)	(28.1)	1,972.6

Source: Osirium, Edison Investment Research, Note: *14 months ended 31 December 2018.

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 Plc, 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 space. 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 advisor to Fairfax Financial, where he sits on the boards of Brit Syndicates Ltd and Advent Underwriting Ltd. 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	17.3
Harwell Capital	11.3
Canaccord Genuity	8.5
Lombard Odier	8.0
David Guyatt	7.5
Rathbone Brothers	5.5
Herald Investment Management	3.8

Companies named in this report

CyberArk, Wallix