

Osirium Technologies

Keeping your secrets

Osirium Technologies' software protects critical IT infrastructure from the unauthorised use of privileged IT accounts, bringing an innovative approach to the privileged access management (PAM) software market. Having established its credentials in the enterprise market, it is now seeking to expand into the mid-market where the simplicity of its technology makes it attractive. Bookings growth, new channel partners and new customers signed up will be the key metrics to track in the short to medium term.

Year end	Revenue (£000s)	Bookings (£000s)	PBT* (£000s)	EPS (p)	DPS (p)	P/E (x)
10/13	120.0	143.9	(714.6)	N/A	0.0	N/A
10/14	207.0	239.3	(708.5)	N/A	0.0	N/A
10/15	290.2	267.7	(800.7)	(6.6)	0.0	N/A
12/16*	477.6	540.8	(1,715.9)	(12.4)	0.0	N/A

Note: *PBT and EPS are normalised, excluding amortisation of acquired intangibles, exceptional items and share-based payments. *14 month period

Securing the keys to the IT kingdom

Osirium designs software to secure privileged accounts; these are the accounts with enhanced access used by IT system administrators and developers and are a key target for hackers as they grant access to a higher volume of data and users. Securing the perimeter is no longer enough; with increasing cloud adoption the IT perimeter is becoming blurred, and companies are also at risk from internal threats. Combined with increased regulatory pressure, these factors are driving strong growth in the PAM software market. Gartner forecasts a CAGR of 27% from 2015-20 to reach a market size of \$2.2bn. Osirium's PxM platform has four software modules designed to manage account access, automate commonly performed tasks, record active sessions and monitor behaviour. Innovative concepts such as the virtual airgap (which keeps passwords out of users' hands) and task automation (which delegates actions rather than privilege) offer an alternative to established PAM vendors' solutions.

Expanding into the mid-market

Osirium's subscription-based software has been adopted by a number of enterprise and managed security service provider (MSSP) customers. The company is now keen to take its technology to the mid-market, where its simplicity of deployment and use and subscription-based business model should prove attractive. To drive customer growth, management has invested in sales and marketing, is building out a distribution channel and has put in place a global technical support infrastructure.

Tracking progress

With its product developed and investment made in direct sales and the channel, the company is now accelerating commercial roll out. At this early stage in the business's progress, we are not in a position to initiate forecasts. Instead key performance indicators to track the progress of the strategy will include revenues, bookings, new channel partners signed up, new customers, customer renewals/upsells, proofs of concept and software evaluations installed.

Initiation of coverage

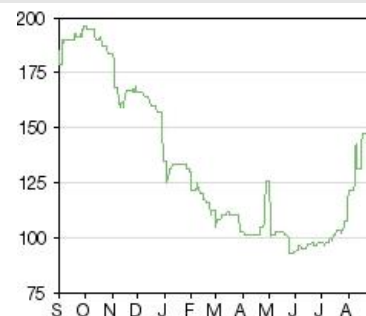
Software & comp services

30 August 2017

Price **141.5p**
Market cap **£15m**

Net cash (£m) at end FY16	3.6
Shares in issue	10.4m
Free float	85%
Code	OSI
Primary exchange	AIM
Secondary exchange	N/A

Share price performance



%	1m	3m	12m
Abs	31.6	52.2	(26.9)
Rel (local)	32.3	56.3	(32.2)
52-week high/low		196.5p	93.0p

Business description

UK-based Osirium Technologies designs and supplies subscription-based cyber security software. It has four products: privileged access management (PAM), privileged task management (PTM), privileged session management (PSM) and privileged behaviour management (PBM).

Next events

H117 results	25 September 2017
--------------	-------------------

Analysts

Katherine Thompson	+44 (0)20 3077 5730
Bridie Barrett	+44 (0)20 3077 5700

tech@edisongroup.com

[Edison profile page](#)

**Osirium Technologies is a
research client of Edison
Investment Research Limited**

Investment summary

Company description: Innovative PAM software vendor

Osirium's privileged access management software helps protect critical IT infrastructure from unauthorised use of privileged IT accounts, whether from hacking or internal threats. The current technology was developed in response to customers' issues with privileged access management; based around its PxM software platform it consists of four software modules and introduces innovative concepts such as the virtual air gap (to prevent passwords from making it onto users' workstations) and task automation (to delegate actions rather than privilege). The management team has worked together for many years and has experience in commercialising cybersecurity software. The company is based in Theale, UK, and has 34 direct employees and six contractors.

Growth strategy: Land and expand, move into the mid-market

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. In addition, management believes the time is right to take Osirium's technology to the mid-market. Designed with simplicity in mind, 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 recently boosted the sales and marketing team with senior hires and, since the beginning of the year, the company has been building out the channel. It now has distributors covering the UK, German-speaking European countries, the Middle East and North Africa, and APAC, with orders already received via some of these partners. To support partners, Osirium has hired business development directors in those regions, and to support customers has put in place 24/7 global technical support.

Subscription-based business model

Osirium sells its software on a subscription basis, with contracts typically signed for 12 to 36 months and cash paid upfront for at least 12 months in advance. Licences are sold on the basis of the number of end devices secured by the software. In FY16 (14 months to 31 December 2016), Osirium reported revenues of £478k, with subscription licence revenues of £440k, and an operating loss of £1,822k. Bookings received during the period totalled £540k with deferred income at the end of FY16 of £276k. All contracts expiring in FY16 were renewed, with many expanded in scope. The company had a net cash position of £3.6m at the end of FY16. At this point, we are not initiating forecasts. To track performance, the company monitors the following KPIs: revenues, bookings, new channel partners signed up, new customers, retaining and growing customer renewals, number of proof of concepts and software evaluations installed.

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 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 the company maintaining a high level of recurring revenues. The mix between direct and channel sales will influence the rate of revenue growth. Funding requirements could result in dilution for existing shareholders.

Company description: Privileged access software

Osirium is a UK-based provider of privileged access management (PAM) software. While small from a revenue perspective, the company has signed up a number of blue-chip enterprises and managed security service providers (MSSPs), providing validation for its innovative, subscription-based software. With recent investment in sales and marketing and R&D, the company is now positioned to build its customer base and expand 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 Privileged Access Management module and the Privileged Task Management 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. The company is based in Theale, UK, and has 34 direct employees as well as six contractors.

Strategy: Expand into the mid-market

The technology has been developed to meet the exacting demands of enterprise customers, and the company now believes the time is right to expand 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 shorter term, the company has been working to meet the targets in place at the time of the IPO (see Exhibit 1), where it is making good progress. 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. The company 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).

Exhibit 1: Progress since IPO

IPO targets	Progress	Comment
Build out senior management team	✓	Hired sales and marketing directors
Build pipeline, particularly in the mid-market	Ongoing	First bookings from partners achieved
Transition sales to channel-led mid-market fulfilment	✓	Distribution partners signed, business development directors hired in target regions
Build marketing team, evolve the brand	Ongoing	Stephen Roberts hired as head of marketing
Refocus R&D on strategic direction	Ongoing	R&D team now at 23 (12 at IPO)
Build out tech support and infrastructure	✓	24/7/365 support now available
Get patents approved	Ongoing	

Source: Osirium, Edison Investment Research

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 Limited in 2002. David joined Clearswift as a non-executive director in 2002, and became 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 Plc for 12 years. After the IPO, the management team was bolstered by the hires of Stephen Roberts in November 2016 as marketing director (previously at PAM vendor Wallix) and Tim Ager as sales director in January 2017 (previously at Celestix Networks, secure remote access and identity management solutions).

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 in order 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 access (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 in order 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 in order 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 in order 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 Verizon¹ in 2017 estimated that 25% 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) was adopted by the European Parliament last year. Member states have until May 2018 to transpose the directive into their national laws; the UK has said it will adopt it despite Brexit. Member states then have another six months 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: Privileged account management (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 \$521m in 2014, rising to \$690m in 2015 (+33%). 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.

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 competes more with smaller players Thycotic, Bomgar, BeyondTrust and Wallix. Customer numbers per Exhibit 2 reflect

¹ Verizon Data Breach Investigations Report, 2017

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 2: Competitive environment

Company	Ownership	Estimated revenues	No. employees	HQ	Product description	No. customers
PAM focused vendors						
CyberArk	Nasdaq; market cap \$1.4bn	FY16: \$216.6m	823	US	Privileged Account Security Solution	>3,350
Lieberman Software	Private	N/A	N/A	US	Secure Privileged Access Management	N/A
BeyondTrust	Veritas Capital (private equity)	N/A	N/A	US	PowerBroker PAM platform	>4,000
Bomgar	Thoma Bravo (private equity)	>\$70m	c 300	US	Privileged Access, Password Vault	>12,000
Centrify	Private	FY17: >\$100m	c 500	US	Privileged Access Security	>5,000
Thycotic	Private; funding from Insight Venture Partners	N/A	N/A	US	Secret Server	>7,500
Wallix	Euronext; market cap €68m	FY16: €7.3m	71	France	Wallix Bastion	>400
Broad-based vendors						
CA Technologies	Nasdaq; market cap \$13.5bn	FY17: \$4bn	c 11,800	US	Privileged Access Manager	
Micro Focus	LSE; market cap £4.9bn	FY17: \$1.38bn of which \$207m from Identity, Access & Security	c 4,500	UK	Privileged Account Manager	
ManageEngine	Zoho Corporation (private)	N/A	N/A	US	Password Manager Pro	

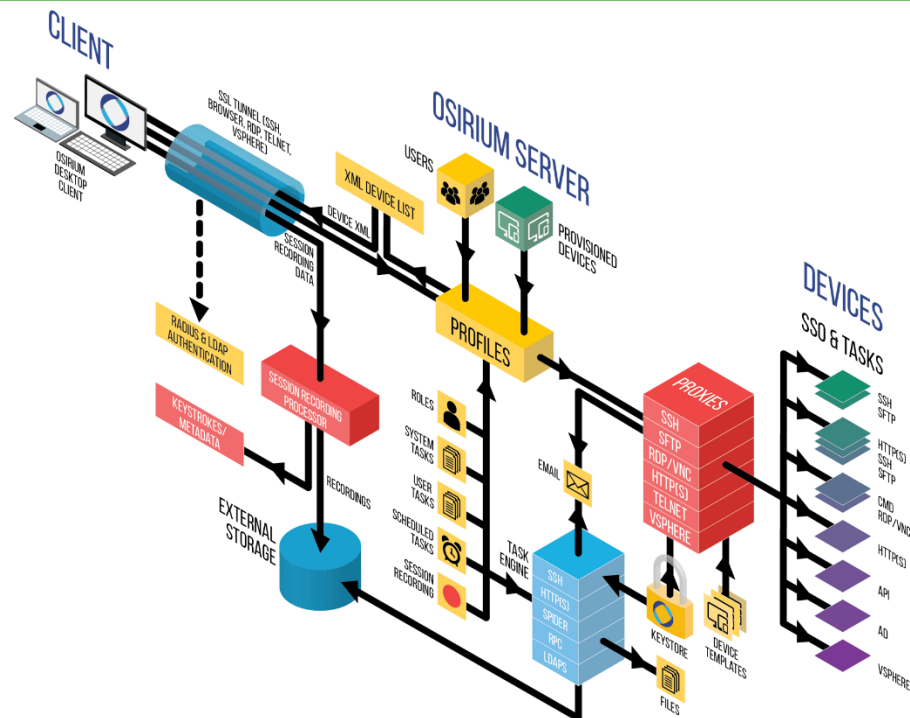
Source: Edison Investment Research

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, in June 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.

In the June 2017 KuppingerCole report, analysts recognised that Osirium's innovative features (virtual air gap, automated tasks) take a different approach than its competitors and therefore make it hard to assess on a like-for-like basis, but also highlighted that these features may be exactly what is required by the customer.

Osirium's PxM platform

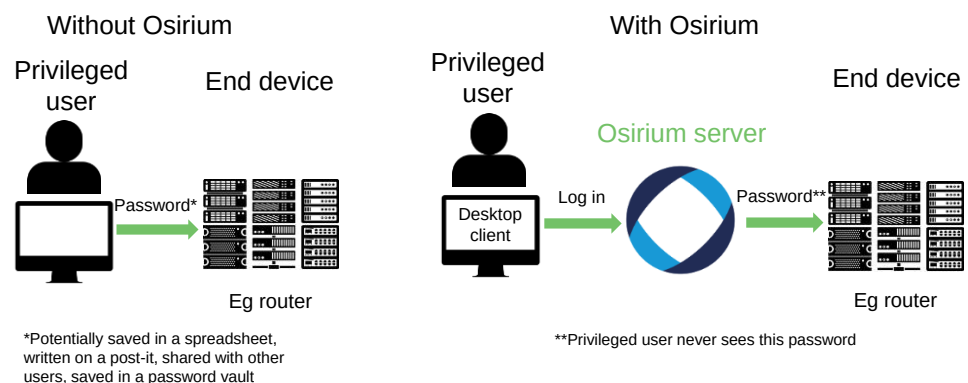
The diagram in Exhibit 3 shows the platform architecture. Osirium's PxM 2.0 platform currently offers four modules: PAM, PTM, PSM and PBM. The solution consists of software loaded onto a server ("Osirium server") and an application that is loaded onto the desktop of privileged users. The Osirium server 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, load balancers and UPSs. 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.

Exhibit 3: Osirium platform architecture


Source: Osirium

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 that 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 4: 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 onto the Osirium server using the customer's preferred method, eg user password, two-factor authentication (for example, Osirium's platform is integrated with SailPoint identity access management software). 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 are able to access all of 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 that 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.

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.

Privileged task management (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 as 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 to perform the task, 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.

Privileged session management (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 that 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.

Privileged behaviour management (PBM)

This is Osirium's newest module. The idea is that privileged user behaviour is monitored over time 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 has been expanded significantly since IPO, with two teams of six developers (12 in total) growing into four teams making up a total of 23 developers. Areas and features that the company is looking to develop include:

- Distributed privileged behaviour management – using Elastic Stack to reduce the processing load on a customers' infrastructure generated by behaviour analytics.
- Further development of the MAP solution for legacy software.
- Further development of the task engine.
- "App-less" access for third parties. 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.

The company filed three patents in January 2016 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. The patents cover the following functions:

1. Password maintenance in computer networks
2. Controlling access to remote devices
3. Password recovery

Direct and partner-driven sales strategy

Enterprise customers – direct sales

At the time of IPO Osirium had 13 direct customers. We estimate that this has increased to more than 20, with around 50 corporate users of the software including direct and indirect customers.

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.

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 substantially implemented. Other customers include ThinkMoney (financial services), two English police forces, a European car manufacturer, a multi-national defence company, a global mobile network operator, a reinsurer 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 is signing up distributors in key geographies. A crucial part of the process is providing training and support to distributors so that they are able to sell and install the software. Business development directors have been hired in the Middle East, Asia-Pacific (two) and Germany.

Progress in building the channel includes:

- UK: Osirium signed up UK distributor Distology at the beginning of this year. Through Distology, the company has already received orders, including from a UK infrastructure provider and a global insurer.
- Middle East and North Africa: Osirium signed up Spectrami in March.
- Singapore: Osirium signed up CHJ Technologies in March.
- Germany: Osirium signed up Ectacom in July. Ectacom covers Germany, Switzerland, Austria and Poland.

The company is not directly targeting the US. 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.

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. 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 currently bundled in with PAM/PTM but the company plans to make this available as a standalone module.

The company generates some service-based 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.

Positive revenue and bookings trends

In Exhibit 4, we show the revenues and bookings reported to date. The monthly bookings rate increased significantly in FY16. 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.

Exhibit 5: Revenues and bookings				
£k	FY13	FY14	FY15	FY16*
Reported subscription revenues	101.0	153.0	252.4	440.6
Services	19.0	54.0	37.7	37.0
Total revenues	120.0	207.0	290.2	477.6
<i>Growth rates</i>				
Reported subscription revenues		51.5%	65.0%	74.5%
Services		184.2%	-30.1%	-1.9%
Total revenues		72.5%	40.2%	64.6%
Bookings (invoiced sales)	143.9	239.3	267.7	540.8
Monthly bookings rate	12.0	19.9	22.3	38.6
Growth in monthly bookings		66.3%	11.9%	73.2%
Source: Osirium. Note: *14-month period ended 31 December 2016.				

Cost base to level off in FY17

Exhibit 6: Costs and operating losses				
£k	FY13	FY14	FY15	FY16*
Staff costs – gross			620.0	1,561.0
Capitalised development costs			(276.9)	(755.5)
Staff costs – net	141.2	414.4	343.1	805.5
Other operating costs	345.5	119.7	324.9	808.8
Depreciation	5.1	6.0	6.0	14.6
Amortisation	307.6	381.2	406.8	574.3
Share-based payments	0.0	184.3	56.4	96.9
Total costs	799.3	1,105.5	1,137.3	2,300.1
Operating loss	(679.4)	(898.5)	(847.1)	(1,822.5)
Cash flow from operations	(190.6)	(274.9)	(122.6)	(789.4)
Capitalised development costs	(410.1)	(368.4)	(404.4)	(915.5)
Average headcount	7	9	11	21
Source: Osirium Technologies. Note: *14-month period ended 31 December 2016.				

In the exhibit above, we summarise the key cost lines for the business. The largest cost is for staff: at IPO the company had 18 direct employees and three contractors; this has now risen to 34 direct employees and six contractors (including regional business development directors). In the short term, the company does not expect to increase headcount materially. 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 – in FY16 close to half of staff costs were capitalised. These are amortised over a five-year period, starting in the year of capitalisation.

At the end of FY16, Osirium had a gross/net cash position of £3.6m. The company is likely to require additional funding before it reaches breakeven. This could result in dilution for existing shareholders.

Track performance via KPIs

At this stage in the company's life, we are not introducing forecasts. The company tracks its performance through progress of the following KPIs: bookings, revenue, new channel partners signed up, new customers, retaining and growing customer renewals, number of proof of concepts and software evaluations installed. The company will report interims on 25 September when we expect to see an update on progress against these KPIs.

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%) – maintenance at this high level will be key to maintaining the high level of recurring revenues.
- **Pricing ability.** Osirium currently 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 is likely to require additional funding before it reaches breakeven. This could result in dilution for existing shareholders.

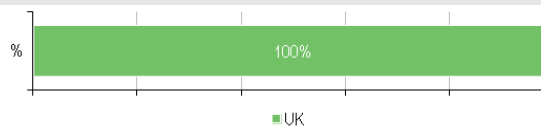
Exhibit 7: Financial summary

	£k	2013	2014	2015	2016
Year end 31 October (FY13-FY15)/31 December (FY16)		IFRS	IFRS	IFRS	IFRS
INCOME STATEMENT					
Revenue		120.0	207.0	290.2	477.6
EBITDA		(366.7)	(327.1)	(377.9)	(1,136.7)
Normalised operating profit		(679.4)	(714.3)	(790.7)	(1,725.6)
Amortisation of acquired intangibles		0.0	0.0	0.0	0.0
Exceptionals		0.0	0.0	0.0	0.0
Share-based payments		0.0	(184.3)	(56.4)	(96.9)
Reported operating profit		(679.4)	(898.5)	(847.1)	(1,822.5)
Net Interest		(35.2)	5.7	(9.9)	9.7
Joint ventures & associates (post tax)		0.0	0.0	0.0	0.0
Exceptionals		0.0	0.0	0.0	0.0
Profit Before Tax (norm)		(714.6)	(708.5)	(800.7)	(1,715.9)
Profit Before Tax (reported)		(714.6)	(892.8)	(857.1)	(1,812.8)
Reported tax		137.7	134.1	121.0	453.3
Profit After Tax (norm)		(576.9)	(602.1)	(687.6)	(1,286.9)
Profit After Tax (reported)		(576.9)	(758.7)	(736.0)	(1,359.6)
Minority interests		0.0	0.0	0.0	0.0
Discontinued operations		0.0	0.0	0.0	0.0
Net income (normalised)		(576.9)	(602.1)	(687.6)	(1,286.9)
Net income (reported)		(576.9)	(758.7)	(736.0)	(1,359.6)
Basic average number of shares outstanding (m)		0	1	10	10
EPS – basic normalised (p)		N/A	N/A	(6.61)	(12.38)
EPS – diluted normalised (p)		N/A	N/A	(6.61)	(12.38)
EPS – basic reported (p)		N/A	N/A	(7.08)	(13.08)
Dividend (p)		0.00	0.00	0.00	0.00
Revenue growth (%)		26.3	72.6	40.2	64.6
EBITDA Margin (%)		-305.7	-158.0	-130.2	-238.0
Normalised Operating Margin		-566.3	-345.0	-272.5	-361.3
BALANCE SHEET					
Fixed Assets		815.7	805.2	799.7	1,178.8
Intangible Assets		808.6	795.7	793.3	1,134.5
Tangible Assets		7.2	9.5	6.4	44.3
Investments & other		0.0	0.0	0.0	0.0
Current Assets		109.3	269.2	428.1	3,953.7
Stocks		0.0	0.0	0.0	0.0
Debtors		77.2	218.6	154.6	380.9
Cash & cash equivalents		32.2	50.6	273.5	3,572.8
Other		0.0	0.0	0.0	0.0
Current Liabilities		(235.2)	(294.2)	(365.0)	(648.5)
Creditors		(235.2)	(294.2)	(365.0)	(648.5)
Tax and social security		0.0	0.0	0.0	0.0
Short term borrowings		0.0	0.0	0.0	0.0
Other		0.0	0.0	0.0	0.0
Long Term Liabilities		(952.5)	(487.6)	(163.3)	0.0
Long term borrowings		(789.0)	(323.7)	0.0	0.0
Other long term liabilities		(163.4)	(163.9)	(163.3)	0.0
Net Assets		(262.6)	292.6	699.5	4,483.9
Minority interests		0.0	0.0	0.0	0.0
Shareholders' equity		(262.6)	292.6	699.5	4,483.9
CASH FLOW					
Op Cash Flow before WC and tax		(366.7)	(327.1)	(377.9)	(1,136.7)
Working capital		66.3	3.8	120.7	226.8
Exceptional & other		0.0	0.0	0.0	0.0
Tax		109.8	48.4	134.6	120.4
Net operating cash flow		(190.6)	(274.9)	(122.6)	(789.4)
Capex		(412.8)	(376.7)	(407.3)	(968.0)
Acquisitions/disposals		0.0	0.0	0.0	0.0
Net interest		(35.2)	5.7	(9.9)	9.7
Equity financing		0.0	639.3	762.8	5,047.1
Dividends		0.0	0.0	0.0	0.0
Other		0.0	0.0	0.0	0.0
Net Cash Flow		(638.6)	(6.5)	222.9	3,299.3
Opening net debt/(cash)		118.3	756.9	273.1	(273.5)
FX		0.0	0.0	0.0	0.0
Other non-cash movements		0.0	490.3	323.8	0.0
Closing net debt/(cash)		756.9	273.1	(273.5)	(3,572.8)

Source: Osirium Technologies accounts

Contact details

Theale Court,
11-13 High Street
Theale, Reading
Berkshire, RG7 5AH
UK
0118 3242444
www.osirium.com

Revenue by geography

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.

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.

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.

Chairman: Simon Lee

Simon Lee is an international advisor to Fairfax Financial, global advisor to SATMAP 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	15.4
Harwell Capital	14.7
David Guyatt	9.8
Lombard Odier	9.2
Dalton Investments	6.9
Investec	6.7
Unicom Asset Management	6.2

Companies named in this report

CyberArk, Wallix

Edison is an investment research and advisory company, with offices in North America, Europe, the Middle East and AsiaPac. The heart of Edison is our world-renowned equity research platform and deep multi-sector expertise. At Edison Investment Research, our research is widely read by international investors, advisers and stakeholders. Edison Advisors leverages our core research platform to provide differentiated services including investor relations and strategic consulting. Edison is authorised and regulated by the [Financial Conduct Authority](#). Edison Investment Research (NZ) Limited (Edison NZ) is the New Zealand subsidiary of Edison. Edison NZ is registered on the New Zealand Financial Service Providers Register (FSP number 247505) and is registered to provide wholesale and/or generic financial adviser services only. Edison Investment Research Inc (Edison US) is the US subsidiary of Edison and is regulated by the Securities and Exchange Commission. Edison Investment Research Limited (Edison Aus) [46085869] is the Australian subsidiary of Edison and is not regulated by the Australian Securities and Investment Commission. Edison Germany is a branch entity of Edison Investment Research Limited [4794244]. www.edisongroup.com

DISCLAIMER

Copyright 2017 Edison Investment Research Limited. All rights reserved. This report has been commissioned by Osirium Technologies and prepared and issued by Edison for publication globally. 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. Opinions contained in this report represent those of the research department of Edison at the time of publication. The securities described in the Investment Research may not be eligible for sale in all jurisdictions or to certain categories of investors. This research is issued in Australia by Edison Aus and any access to it, is intended only for "wholesale clients" within the meaning of the Australian Corporations Act. The Investment Research is distributed in the United States by Edison US to major US institutional investors only. Edison US is registered as an investment adviser with the Securities and Exchange Commission. Edison US 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. As such, Edison does not offer or provide personalised advice. We publish information about companies in which we believe our readers may be interested and this information reflects our sincere opinions. The information that we provide or that is derived from our website is not intended to be, and should not be construed in any manner whatsoever as, personalised advice. Also, our website and 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 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. This document is provided 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. Edison has a restrictive policy relating to personal dealing. 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. Edison or its affiliates may perform services or solicit business from any of the companies mentioned in this report. The value of securities mentioned in this report can fall as well as rise and are subject to large and sudden swings. In addition it may be difficult or not possible to buy, sell or obtain accurate information about the value of securities mentioned in this report. Past performance is not necessarily a guide to future performance. 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. 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 (ie 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. To the maximum extent permitted by law, Edison, its affiliates and contractors, and their respective directors, officers and employees will not be liable for any loss or damage arising as a result of reliance being placed on any of the information contained in this report and do not guarantee the returns on investments in the products discussed in this publication. FTSE International Limited ("FTSE") © FTSE 2017. "FTSE" is a trade mark of the London Stock Exchange Group companies and is used by FTSE International Limited under license. All rights in the FTSE indices and/or FTSE ratings vest in FTSE and/or its licensors. Neither FTSE nor its licensors accept any liability for any errors or omissions in the FTSE indices and/or FTSE ratings or underlying data. No further distribution of FTSE Data is permitted without FTSE's express written consent.