IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with Mark Warren

Carol Baker

With the move to remote working during COVID, staff members were often granted local admin rights on their laptops so they could get working without help from IT. Unfortunately, this meant that IT lost visibility and control over those devices. Following the pandemic, businesses have had to adapt security processes to address the quick fixes and temporary measures they put in place and prepare for a more permanent adoption of remote and flexible working. However, many organizations and individuals have become complacent with a number of aspects of cybersecurity, explains Osirium's Product Specialist and Marketing Director, Mark Warren.

***Mark Warren** is Osirium's Marketing Director and Product Specialist, (https://www.osirium.com), and has over 30 years of experience in product development and marketing leadership at global software organizations.*

At Osirium, he leads the Marketing team, focusing on field and product marketing and demand generation, and developing the Osirium brand and market presence.

Before Osirium, Mark worked in different industry sectors at international organizations including SITA, 1E, Perforce Software, Serena, and Micro Focus.

Mark blogs at https://www.osirium.com/resources/blog

Why is Privileged Access Management (PAM) so crucial to the foundation of any cybersecurity strategy?

Osirium is known as the Privileged Access Management (PAM) Innovator. For a small company, we have a phenomenal list of customers ranging from major public organizations and global investment banks through to SMEs, across every industry sector. The key differentiator that sets us apart from our competitors is the ease of deployment of Osirium's products. A lot of our customers come to us after having failed deployments with some of the big international players.

Time and time again we hear, "The price was OK with your competitor, but there was no white glove service, they were never available when we needed them. Whereas with Osirium you are always available, and always give good advice." We pride ourselves in delivering a superior experience for all our customers.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Some of the core functionality of PAM is largely consistent across all the vendors – it's about protecting admin credentials – but with Osirium, it's also about the secure automation of the work that needs PAM.

PAM controls how a user connects to an IT system. They don't have direct access to credentials, but have to go through some central point that can control connection to those back end systems. The PAM system itself monitors what a user is doing, and can record the sessions while they're connected, and therefore controls how the user connects. While connected, the system is watching what the user is doing to make sure they only do the things they should.

We first introduced automation in our PAM solution to allow the IT team to write scripts which could be executed on a remote node on a remote device or system in a secure way. So, the credentials are always protected and never returned to the user, and neither could the user interfere with the processes. This ensures that the right thing is done in the right way – and it's usually a lot quicker than the manual processes.

But many IT tasks have to touch multiple systems. A common task for IT teams is resetting an account after somebody forgot their password, or provisioning accounts for a new employee. It is also moving their accounts as they move around the organization or disabling their accounts when they leave. Creating accounts for a new starter when they join the business involves, for example, creating an Active Directory account and an Office 365 account. If they're in the Marketing department they will need to log into the CRM system, or if they're in Finance, they will need to log in to Xero, Sage, or whatever financial system is in use in the business. They must also be able to log into all productivity tools, and a typical new employee could easily need to have ten or more accounts created before they can really be productive in their work.

Traditionally, someone in HR, or maybe the hiring manager, would need to send a request to IT. The IT department would raise perhaps a whole bunch of tickets to each of the relevant teams to create a new user in Workday, create a new user in Active Directory, create a new user in the CRM system, for example. At some point, each of those teams would come back hopefully saying they've completed that task.

But IT teams can be busy, and whilst some might say, "Yeah, I'm in there. I'll just do it now quickly, and I'm done", others will say, "Yeah, I'll do it tomorrow". Then suddenly tomorrow, there's a server crash, or a subscription breach and all of a sudden the ticket goes to the bottom of the queue and doesn't get actioned. This results in only half of the required accounts being done, or the user needing to wait weeks or months to get everything done. So, there are opportunities for better automation that can securely automate a task or tasks which touch multiple systems.

If you can securely connect to each of those systems, you can easily encode the operation to write a playbook or write a script to do the necessary updates and ensure that you've got an audit trail. It then becomes much easier for somebody,


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

perhaps the frontline helpdesk engineer or even the HR person themselves, to create accounts for this new user, or disable accounts when someone has just left the business. With automation the tasks can be actioned all in one go, in minutes rather than weeks or months. We call this Privileged Process Automation or PPA.

Could you give us an example of how this works in practice?

Earlier this year we announced a deal with the NHS Midlands and Lancashire Commissioning Support Unit (MLCSU). They are kind of a Managed Service Provider (MSP) to NHS Trusts. They provide IT services – everything from acquiring desktop hardware to managing HR systems – on the trust's behalf, and they saw an opportunity to focus on primary care settings. Traditionally, IT in the NHS has focused around acute care, for example, hospitals and ambulance trusts – which are big organizations with IT staff with big IT infrastructure. But if you look around, there's a much bigger population of primary care providers such as GP surgeries.

Some GP surgeries are pretty big businesses these days, but many of them are quite small: they may have a practice manager and a couple of admin people, plus clinical staff, and they rely on IT systems, but they don't have any kind of local IT presence. So, they go through the whole scenario, submitting a request to MLCSU to, say, create accounts for a new team member, or remove and disable all accounts when a team member leaves, and typically the request is sent at five o'clock on a Friday afternoon.

Now, those requests would get into the queue with every other request that the helpdesk is getting, amongst all the general IT firefighting they're doing, and it could be that somebody leaves on a Friday and all their accounts are still open a week later – and clearly, that's not a good place to be.

So MLCSU saw an opportunity that if they could automate more of this work, they could delegate it out to the primary care organizations and let them do more of this for themselves – and with Osirium's help, that's exactly what they are doing.

MLCSU has just started rolling out automation to GP practices, starting in the Birmingham and Solihull area, where the office manager or grant cycle operations manager at a practice can do those account creation, resetting and disabling operations themselves. Originally it was a four week pilot, and when it came towards the end, GP practices were saying "Don't take this away – we depend on this." It's a wonderful example of how an organization has come to depend on automation, and is a real big push for digital transformation in the healthcare sector.

But it's not just healthcare. Think about hotels. For example, at every Premier Inn there are a couple of admin staff and a bunch of checking-in terminals, and a backup system, but they don't have any IT staff on site.

The same applies in many other industries, for example, in the vehicle hire sector, or in retail where every shop has POS terminals and PCs, but no IT staff. Automation would see that shift where the end user gets what they need faster.


IT for CEOs & CFOs is published by House of Words Media Limited.
The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The business can focus on the business, the IT helpdesk or the MSP can focus on higher value tasks – and the whole business is better because it can be sure that the right processes are being performed in the right way, plus there's a full audit trail.

Privileged process automation is different from traditional Robotic Process Automation (RPA) scripting, which can be either too weak in security, or too heavyweight to build automation; you can spend weeks and months building scripts. But with Osirium our environment uses a kind of low code environment. It's very easy to build these scripts, and we have a very large and growing library of free playbooks as a starting point – it's a real sweet spot that suits the way that IT teams work.

Why have businesses become complacent when it comes to cybersecurity?

The move to remote working during the pandemic saw remote workers being granted local admin rights on their laptops so that they could get working quickly without the help of the IT department. But this meant the IT department lost visibility and control over those laptops, and remote workers could easily be duped into installing infected software, even if they'd had the best cybersecurity awareness training.

Following the pandemic, many businesses have yet to adapt their security processes to address the quick fixes and temporary measures they put in place and prepare for a more permanent adoption of remote and flexible working. This is particularly important when it comes to the security of endpoint devices, especially those with shared usage.

In addition to ensuring employees use strong passwords and MFA, an approach that we call Privileged Endpoint Management (PEM) should be used to allow staff to run approved applications with elevated privileges. They can then do their work without having the wide-open access that attackers are looking for to install their malware.

With tools such as PEM deployed and active, businesses can balance productivity and security. Users can do the work they need with fewer calls to the Helpdesk. IT gets fewer interruptions and can focus on more valuable work, and auditors can see who had access to which applications due to logs that show the actual users, not just an arbitrary administrator account, ensuring security and compliance regs are met.

For example, if we look at academia, organizations need to know what is going on at the endpoints. Universities in particular are concerned about controlling servers and their databases, especially when students are connecting laptops. Universities were some of the earliest adopters of IT, and a lot of their IT systems have evolved over a very long period of time, often without any structure or planning. They tend to be a bit of a mess, especially when it comes to the Active Directory – and it becomes challenging to know when to lock permissions down when you don't know who's got what, where, and when.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

The ethos of universities is around collaboration, the sharing of knowledge and experiences and having the freedom to investigate and research, but they still need to be able to lock systems down to keep the university secure. The weakness comes when the IT team gets a lot of requests from students to install software, add a printer driver, update a system, or even change the wallpaper on the desktop. This ties up IT staff time, so they give users either local admin permissions on their account or a shadow account that has local admin rights. This means when they try to install a piece of software, they get a pop-up user access control (UAC) prompt whereby Windows asks them to revalidate to show they are who they say they are, and that they have permission to make that change.

You then get a bunch of shadow accounts, otherwise the IT department gets constant requests such as “Can you upgrade my Chrome please? Or can you let me have permissions just for an hour while I run a network sniffing tool?”.

To overcome this, Osirium has introduced a Privileged Endpoint Management (PEM) solution that removes local admin rights from users in a way that is as unobtrusive as possible.

PEM can be run in learning mode for a period of time – this might be a couple of weeks, or a month, and over that time PEM is watching to see which apps get run with administrative privileges. Interestingly, as we’ve been doing this, we’ve found a number of scenarios where requests are a little bit more subtle than the normal “I’d love to be able to add a new program”.

For instance there are tools such as AutoCAD, which is used by product designers and architects, and which has a whole bunch of plugins to do all sorts of things. This could be stress calculations, or it could be models for objects to place in a design, for example, and every one of those plugins wants to be able to update itself whilst it’s being used. So you need to have administrative privilege to enable the software install to happen.

Now, if you’re in the middle of a piece of work, and you must halt it because AutoCAD just said you can’t continue working, that’s not good. So, what PEM can do is learn which apps are being used, review those apps, and make sure that they’re an approved version.

For example, a company might have a policy to say Chrome 101 is its approved version of Chrome. So, anybody who’s using something older will need to be upgraded to 101 before they’re allowed to do anything else; that is a good hygiene factor. But also, we can fingerprint the installer for Chrome 101 to show that it hasn’t been infected by malware.

These then become a set of proof policies which can be rolled out to say ‘these are approved applications of this particular version’ so that a group of users can install them or run them with elevated privilege. At that point, the local admin accounts can be removed, and now the user carries on working. It means that when the UAC prompt comes up, and the user gives their normal user account details, it is just the process that gets elevated permissions, not the whole user.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

What is next for Osirium PAM?

PAM is always developing. Now that businesses realize how critical PAM is for giving access to backend infrastructure, the threat of ransomware is getting more attention. The largest part of PAM is protecting the systems that help you get back in: the recovery systems. We've now introduced a high availability option in Osirium PAM which means you could have multiple PAM servers and if one of them falls out for hardware failure, for instance, the system can quickly switch to another and carry on running – because if you want PAM to be the gateway to all IT systems, you do everything to make sure it's available. The difference with the way that Osirium does it is that we don't have any dependencies on external databases. You don't have to go and buy an upgrade to SQL Server or whatever to make this work.

Neither do we ask for any strange network architecture that some of the other vendors do. There is an additional cost as a kind of platform to get to add on, but it's very scalable. You can have as many servers as you like – there's no cost per server – so it's very predictable costing.

We continue to develop PAM. The latest release of Osirium PAM v8.0 focuses on two critical new and enhanced capabilities that make it easier for businesses to adopt zero-trust security strategies: scheduled and approved access to administrator accounts, and built-in multi-factor authentication (MFA).

Osirium PAM minimizes the risk of privilege misuse, as access to privileged accounts is only granted as and when needed and then removed as soon as access is no longer required; in line with best-practice recommendations from the National Cybersecurity Centre.