PAM in use with multi-dependency IT estates

OSIRIUM REPORTS

It is a fair estimate that 60–80% of all DevOps effort goes in to maintaining 'legacy' applications. Of course this depends entirely on how one defines legacy, but for the purpose of this article we'll use the definition: 'All software older than the current "official" release'.

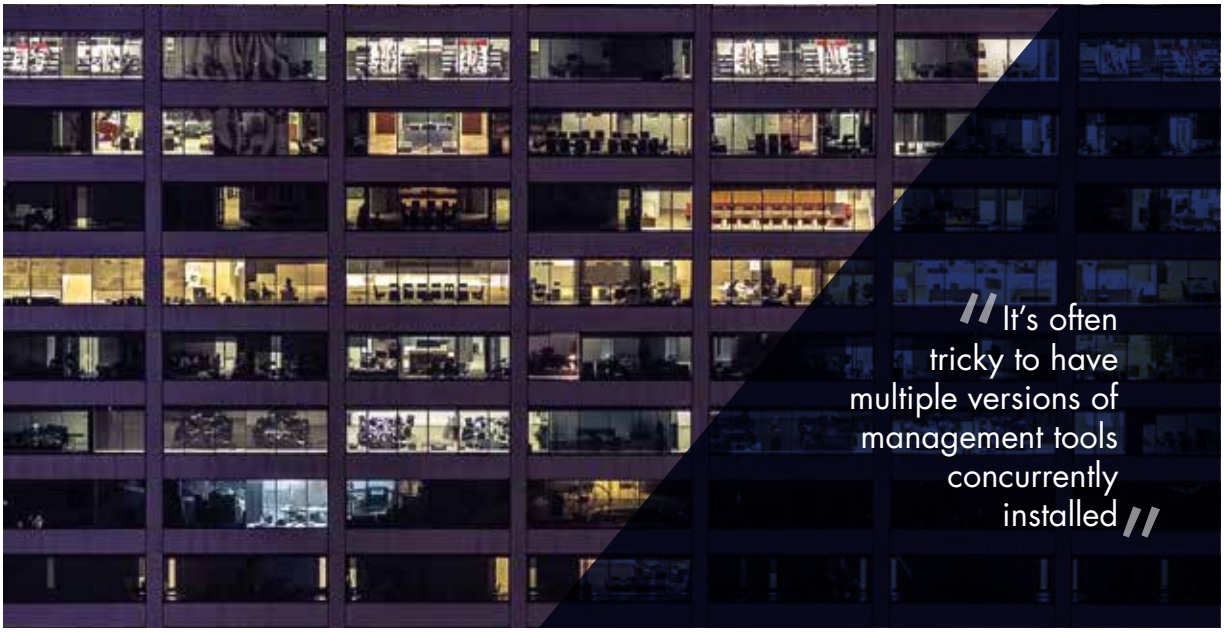
At the time of writing, VMware is at version 6.0 yet we're aware that many customers and prospects are running systems on 4.1 and older. Here's the problem with management applications or 'thick clients' as they are sometimes called: they all have dependencies, sometimes it's their own DLLs but most likely it's versions of .NET and Java. This means it's often tricky or impossible to have multiple versions of some management tools concurrently installed.

So SysAdmins and DevOps are forced to bounce back and to between different versions or install specific versions on 'jump boxes' and then bounce through those. Of course the 'jump boxes' come with their own desktop and get shared across team members. Then your team members have to remember which jump box had what client on. So that's a built-in inconvenience and a Privileged Access Management problem – dealing with the shared accounts.

We've dealt with these issues with our PxM Platform; we've built MAP servers to handle all those fat legacy clients, project only the application window to your desktop *and* handle

cont. overleaf

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password lifecycle management, and then hand the pre-prepared session back to the incoming request ready for system management. The session can be recorded, subject to time windows and device group separation. We have delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.



all the account mapping and enterprise class password lifecycle management. All the DevOp or SysAdmin need to do is select the system they need to connect to. The PxM Platform works out which version of the application they need and which MAP server to project it from. Then the PxM Platform does single sign on using either known, personalised or mapped accounts. It's comforting to know that the device credentials never enter the workstation environment – this gives full protection from malware and phishing.

It also means that multiple users can have access to the same account to get access to systems yet still retain the ability to know who did what, where and when. With the PxM Platform, the users arrive as an identity and leave as a role, whether that role maps to a shared administrator/root style account, a personalised account, or a privileged version of their normal account. As the connections are made, the PxM Platform syslogs all this data to SIEM systems and can be set to record sessions. By record sessions, we mean just the part of the session that deals with the interaction with the end system, device or application. The PxM Platform records just that window, it doesn't capture all the google searches etc. that the user makes when deciding what to do to a system.

These days of less people needing to do more make our PxM Platform even more relevant to DevOps teams; for example, we integrate with ticketing systems. In this way, you can add the bar of needing a change or incident ticket to access a system, but when the user does, the PxM Platform helps them find the system quickly, connect using the right version of the management application and log the connection and ticket for them!

This kind of access can be mapped through to third parties and outsourcers. The PxM Platform has a profile scheme where systems are added also with a defined access role, time windows can be defined along with a profile enable/disable condition. One can add and delete third parties to these profiles as required - the access is granted and revoked in real time.