Secure Your Cloud and Outsourced Business with Privileged Identity Management
Table of Contents

Executive Summary........................................................................................................3
Understanding Privilege.............................................................................................3
Do All Service Providers “Get It”?.............................................................................5
Managing Privilege ‘Everywhere’ With CyberArk....................................................7
Executive Summary

Privilege is everywhere. Outsourcing, from traditional managed and hosted services to the cloud, extends the complex relationships of privileged accounts, users, data, systems and services, which are so critical to assessing and reducing corporate risk, well beyond enterprise boundaries.

Understanding and managing privilege is perhaps the most critical component of bringing risk under control, yet it is often poorly understood and inadequately addressed within the organization’s IT environment. That being the case, how are enterprises to address privilege when they put external parties in control of applications, processes, services, systems and data in the hands of cloud service providers and their administrators?

As outsourcing and the various representations of cloud-based services become increasingly essential to business operations, enterprises need to find ways to exercise governance over their critical assets and operations by extending control over privilege, both internally and externally. Service providers, for their part, must be prepared to address their clients' privilege/risk management requirements to maintain a strong competitive position in the market. This paper reviews the “10 steps for securing the extended enterprise”.

Whether the IT ownership in a particular area is internal or ceded to one or more of the outsourcing models discussed, the organizations liability remains constant.

Understanding Privilege

Privilege is generally, if not universally, understood in terms of controlling users who have high levels of authorization to, and control over, corporate IT systems, information assets and applications. In that important, but somewhat narrow context, poor control over privileged user accounts is an all too common source of risk, both from a security and compliance perspective. Ineffective privileged account and privileged user management is the bane of many organizations. Access to these accounts is commonly shared by multiple users, issued outside of corporate security policies and procedures, rarely if ever, revoked when its longer needed, and inadequately tracked. Poorly secured and managed privileged user accounts undermine organizational security and make individual accountability for errors and incidents all but impossible. Undocumented, poorly managed accounts make audit and regulatory compliance difficult at best. But enterprises are loathed to tackle the issue for fear of disrupting critical business operations.

However, privilege is a far more sweeping and complex concept than managing privileged accounts and must be evaluated in the multitude of contexts in which users, accounts, data, applications and processes interoperate.

From this perspective, an account or process is not necessarily intrinsically privileged, but may have privileged status because of its relationship within a given context. So for example, performing maintenance on a database may carry a privileged context based on the sensitivity of the data (e.g., credit card numbers or patient health records) rather than the maintenance process or the level of authorization required to perform the task. (For a detailed discussion of privilege and associated risk, see “Take Control of Your Business with Privilege Centric Risk Assessment” http://www.cyberark.com/constants/whitepapers.asp)
Privilege permeates your business: people, policies, processes, applications and data. Nevertheless, they are not always your people, or your infrastructure, your development platform, or your applications. As corporations outsource to managed service, hosting and cloud providers, they progressively cede direct control to someone else’s privileged users, who apply privileged processes and procedures to other people’s data – your data.

This understanding is at the core of privilege-centric risk management, as enterprises balance the business benefits of increased outsourcing, especially in cloud environments, and the challenges of entrusting high value business data and operations into the hands of third party entities.

**Extending Risk, Losing Control**

Enterprises must take a holistic view of privilege, risk and control across their IT environment wherever it is – from the corporate data center to software-as-a-service. The need for privilege-centric risk management persists throughout, but companies surrender direct control to some degree, depending on the service model.

In every case, the service introduces administrators who are not your employees. You typically do not know who they are and cannot monitor their activity. Depending on the service model, you may not know where your data resides or what applications are accessing it; you cannot impose appropriate risk-based controls based on the privilege context.

Broadly speaking, we can summarize IT environments as:

- **Internal** - corporate data centers, networks, databases, file shares, computers, etc. The company can and should exercise privilege-based risk assessment within the organization and implement appropriate policies, procedures and controls to effectively manage risk.

- **Managed services** - company relinquishes some degree of control over specified operations, such as firewall management. The company still retains the ability to determine privilege based on the applicable contexts and set appropriate policies and procedures for privilege management. However, the service provider’s administrators are outside direct corporate control and the company should determine how or if the provider will meet its security and regulatory requirements based on its risk assessments.

- **Hosting** - the client company relinquishes some control in return for a dedicated service or services, such as MS Exchange, network management and data center hosting, being located and managed offpremise. Privileged users will fall outside the control of the company.

In cloud service environments, it can be difficult to establish attribution and enforcement of privileged account controls. This is especially true in public cloud environments, where an organization is purchasing services from a provider, as opposed to selecting and implementing controls and monitoring themselves.

Public cloud services, in turn, are divided into three broad types where enterprises can exert control to a decreasing degree:

- Infrastructure-as-a-service (IaaS) provides virtual server instances and storage on demand. A company pays for the capacity it needs as required.

The service provider is responsible for physical and virtualization security, while the customer organization is responsible for securing the operating system, applications and data. So, you retain important control. You are still responsible, for example, for managing the operating system and still need to delegate and manage privileged accounts in your organization. Client organizations can still manage privileged accounts, root accounts, even though the infrastructure is hosted.
Platform-as-a-service (PaaS) offers software and product development tools hosted that allow developers to create applications on the provider’s platform. In PaaS environments, the provider is responsible for securing the platform, but securing the applications and their development is the customer’s responsibility.

This is something of a middle ground between IaaS and SaaS in terms of corporate ability to exercise security control. It is often a troublesome area when developers take advantage of the easy access to this type of service without following corporate security policies.

Software-as-a-service (SaaS) allows the user to simply consume the application through a front end portal. The provider owns the infrastructure and the software product and interacts with the user through the portal.

In this case, the vendor has total responsibility for security controls throughout the stack, from the physical layer through the applications and data. The enterprise is free of any direct operational responsibility for security, but still holds the organizational responsibility for security and compliance.

The lower you go down the stack, from SaaS to IaaS, the more responsibility for security falls to the enterprise and less to the provider.

But whether the IT ownership in a particular area is internal or ceded to one or more of the outsourcing models discussed, the organization’s liability remains constant. It does not diminish as the service provider takes on some or all of the operational responsibility.

This is why it remains critical either for the organization to exercise control over privilege, directly or through enforceable obligations on the part of the service provider. At its foundation, this requires a consistent policy and process-driven approach to evaluating and enforcing privilege control.

**Do All Service Providers ‘Get It’?**

It is the enterprise’s responsibility to ensure that it implements a privilege-centric risk management program at the core of its IT operations. It is no less important to extend that program to its service providers, rewarding those that can meet its requirements with their business. For their part, forward-thinking service providers recognize privilege control as an increasingly important business differentiator.

Not all service providers see it that way, particularly those higher up in the cloud stack. The Cloud Security Alliance (CSA) observes that introducing strong security controls, such as privileged user management, is often perceived as making the provider more rigid. Therefore, security, particularly the stringent requirements of an enterprise with a privilege-centric risk management program, may not fit the provider’s current business model.

A provider, for example, may well walk away from a potential customer that asks if it has a demonstrable privilege management program and/or offers to negotiate a contract that will help to develop one.

The situation is analogous to the evolution of application development. For a long time, getting the application out and into production took complete precedence over application security. In time, as greater threats emerged and the industry began to mature, the lines between “get it out at any cost” and security began to cross. Now, increasingly, organizations are baking security into their software development life cycles, emphasizing getting a secure application out in timely fashion.

So, too, savvy service providers are realizing they are leaving a lot of business on the table if they cannot demonstrate strong privilege control policies and processes that are consistent with those of mature organizations — their potential customers — who take a risk-based approach to IT operations.
“IT security is the most important inhibitor to public cloud for large companies,” says a service line manager for outsourcing for a global provider of IT services. “Public cloud providers need to change. You must demonstrate you have proper privilege management, demonstrate that you have proper processes that are tuned for public cloud.”

A service provider that is not even familiar with the fact that enterprises are solving privileged access in their own environments is hardly in a position to convince potential customers that they can be trusted with their most critical assets. They will be unable to demonstrate any comparable level of assurance and are far from the point that they can offer privilege-centric risk management.

It is increasingly in the best interest of the enterprise to leverage outsourcing services everywhere. Over time, organizations are trusting more and more of their IT operations to managed service providers, hosted services and the various types of cloud services. By the same token, those service providers that can convince large organizations that they can manage the business critical components of their IT operations securely will be positioned to gain new business and steal a march on the competition.

Before committing critical or sensitive assets to a service provider, organizations must assess the risk to the business if something goes wrong. So, let us examine the key steps enterprises should be taking to assure that risks of outsourcing are properly addressed.

**10 Steps to Securing the Extended Enterprise**

1. **Put privilege first** - implement a privilege-centric risk management program for internal IT operations, so that the enterprise can insist that the service provider follow policies, processes and practices that are consistent with its requirements. This should be grounded in a recognized standard, such as ISO 27002.

2. **Policy follows the user** - make sure that the enterprise has privileged management policies, processes and tools are applied to internal users leveraging outside services. For example, if you are licensing 100 UNIX machines from a cloud vendor, you still need to use privileged identity management to make sure privileged accounts are recycled, that user access is audited and that access adheres to policy.

3. **Provider is in sync** - make sure the service provider has privileged identity policies and processes are consistent with those of the organization. Ideally, both your program and your provider’s will be ISO-based.

4. **Reality check** - review and evaluate the service provider security structure and processes as part of the vetting process. Make sure they are not “paper policies.” In particular, look for privileged identity management tools that support and automate their policies and processes.

5. **Put it in writing** - privileged identity management policies and processes, audit and report requirements and use of appropriate technologies should be written into contracts and service level agreements.

6. **Define roles** - insist on policies that limit privileged user access and authorization. The service provider must be able to demonstrate clear separation of duties, especially for privileged users.

7. **No hidden passwords** - there should be no use of hardcoded embedded application passwords that grant database access. Select privileged identity management tools, such as CyberArk’s Privileged Identity Management Suite, which can assure this.

8. **Measure success** - the service provider’s program must demonstrate continuous control and monitoring. There should be clear metrics, mutually agreed upon, to show that security policies are being applied and that privilege control is continuously improving. CSA recommends that these metrics be written into contracts and service level agreements.
9. **Log and report** - all privileged user accounts, privileged asset access and privileged process activity, should be logged and audited. Service providers should issue weekly or monthly reports that give the enterprise visibility into its operations. This visibility is critical, particularly as contracted services move up the stack to SaaS.

10. **It is in the details** - depending on the service model — more so, for managed and hosted services, less so for higher level cloud services — reports should include detailed reporting on each time a service provider used privileged accounts on the enterprise’s systems.

**Managing Privilege ‘Everywhere’ With CyberArk**

CyberArk’s concept of privilege applies universally, as the enterprise IT environment exists not only internally but also across multiple service providers at all layers of the outsourcing stack.

All the things that would make you use PIM in your own data center become more important when the data center is exposed to the Internet. The same benefits and the same reasons, the same risk reductions of inhouse implementations of a data center apply when moving to cloud, with even more importance.

This will be increasingly practical as enterprises adopt a privilege-centric approach to risk management, and employ privileged identity management tools such as CyberArk’s to translate their policies into a comprehensive, automated, transparent, auditable and secure process form, prioritizing and managing risk associated with high-level accounts and passwords.

Built around its centerpiece, Enterprise Password Vault, CyberArk’s Privileged Identity Management (PIM) suite empowers enterprises to ensure secure access around privileged applications, systems, business processes and information. As the organization builds policy and establishes privilege-centric priorities based on potential impact to the business, CyberArk supplies the necessary tools to build a sustainable program, overcoming the practical obstacles to success.

The CyberArk PIM suite tools — Enterprise Password Vault, Application Identity Manager, Privileged Session Manager and OnDemand Privileges Manager — provide granular control over privileged business activity. All products in the suite are built upon the Digital Vault, a hardened and encrypted repository for managing highly sensitive data such as privileged access information.

“Without CyberArk, you cannot be sure that your people have proper access and authorizations,” says a service line manager for outsourcing for a global provider of IT services, a CyberArk PIM user. “If your people delegate control, authorization can quickly get out of control.”

“Industry-caliber solutions are also necessary for proper inventory of privileged passwords,” he adds. “You can have a privileged identity management process with homegrown tools, but this is not measurable. With CyberArk, you can measure your process and demonstrate that the process is really executed.”

Enterprises must appreciate that the need for a privilege-centric approach to risk takes on even greater importance as they consume managed and hosted services, and commit more and more of their IT environment to the cloud. As service providers develop mature practices around privileged identity management, enterprises will be able to demand and expect, if not the same level of control, a level of assurance commensurate with the criticality of the business assets they are willing to entrust.
“I want to put the best security in place for my environment, and I want to find the vendors who are doing the same,” said Adam Bosnian, CyberArk executive vice president of Americas and corporate strategy. “If you are a vendor and know enterprises are looking for providers who practice privilege based security, you need to bring it top of mind, not just to make your environment more secure, but gain the trust of potential customers.”