SSH

How MSPs can reduce access management risk, complexity, and costs in customer environments

White paper

Index

Introduction

Outsourcing IT and cybersecurity responsibilities to third parties is certainly not a new trend. However, the emergence of the as-a-service model has brought a new dimension to the whole story. **Enterprises can now outsource their entire IT infrastructure to Managed Service Providers (MSPs)** who will then run and maintain the infrastructure, provide 24/7 support if needed, and in general, offer expertise not all companies have in-house.

This evolution has led to **MSPs getting access to highly valuable targets in the customer environments**, typically using what are called *privileged accounts*.

Privileged accounts are used by IT admins, DevOps teams and application support, to name a few, to gain administrative access to critical customer infrastructure and applications, including:

- Windows, Linux, and UNIX servers
- Hypervisors & container management systems
- Firewalls & Network Switches
- Databases
- System Controllers
- Mainframes
- Cloud Administration Consoles
- Operational Technology (OT) devices

The Cloud Hopper case (2017) is a dire example of why securing, managing, and restricting privileged credentials is important. A hacker group infiltrated MSP systems to gain access to their customers' applications network and infrastructure. The group stole legitimate administrator credentials that granted access the MSP and its customer's shared infrastructure. Such credentials allowed the group to laterally move in client's network, penetrating the system even deeper.

There are other variables as well. **The customer environments MPSs host can be very dynamic**, meaning that the target environment is in a constant state of change as servers are spun up and down as needed. Moreover, experts performing remote monitoring and management in these environments come from all corners of the globe and still should only have the minimal amount of access required (principle of least privilege) to get the job done.

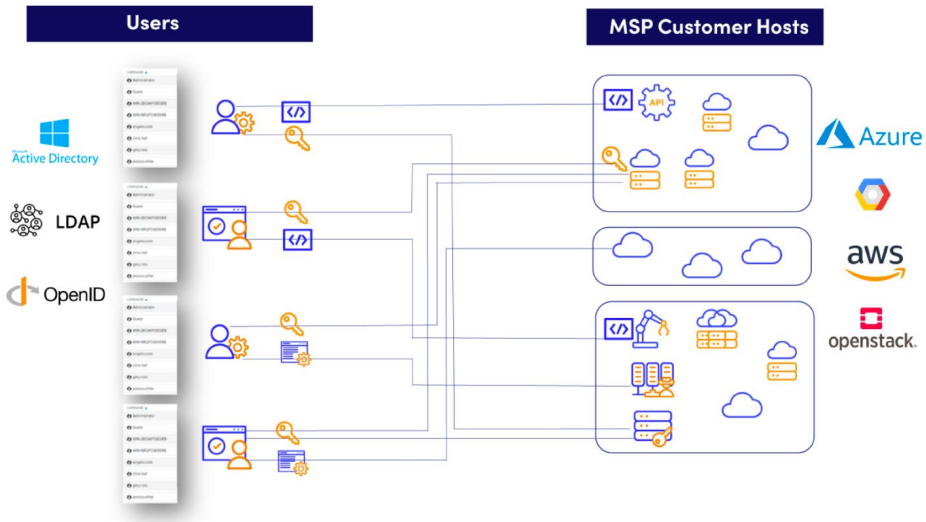
All this has implications to risk management, regulations, customer demands, operational efficiency, and potential new business for MSPs.

Let's look at the challenges first.

Access challenges and risks MSPs face in customer environments under management

Managing many targets creates complexity for MSPs

The variety of targets, the dynamic nature of the hybrid cloud environments, and the spectrum of technologies required to get access to them can be a challenge to many MSPs. How can MSPs ensure that secure access to critical targets does not become too complex, increase risks, or add costs?



An example of a complex customer environment managed by an MSP.

Customers require security and auditability

The growing awareness of supply chain risks (examples include the Solarwinds or the Colonial Pipeline cases) has led and will lead to customers being more selective of the partners they choose to run their critical operations. Most companies require that the partner they select can demonstrate sound security policies, a solid audit trail of activities, and proper management of privileged credentials that allow access to their valuable data or targets.

Regulations require robust access controls

Authorities around the globe are taking steps to ensure safer infrastructures for all. The EU has revised the Directive on Security of Network and Information Systems (NIS 2 Directive) and in the States, the President has issued an Executive Order on improving the nation's cybersecurity. Both publications put special emphasis on private and public organizations to demand proper security controls from the partners and vendors they use.

The spotlight is on credentials and their management

Every time someone or something (machines have IDs too!) accesses a target, there are credentials involved. The credentials used for privileged accounts are highly sought after by hackers to gain access to customer data, intellectual property, and critical infrastructure. As well as the risk of data theft and

malicious service outages, some privileged accounts are also used by cyber threat actors distributing ransomware and malware.

The extent to which ransomware can encrypt data is related to the account that the ransomware is executed under. The higher the privilege of the account, the greater the extent of the problem. The monetary impact and reputational damage of malicious access to these privileged accounts can be devastating.

Some sobering statistics from Verizon Data Breach Investigation Report 2024:

- 62% of financially motivated incidents involved ransomware or extortion, and ransomware was a top threat across 92% of industries.
- Around 50% of breaches started wth misused/breached credentials.

No centralized way to control access

Every cloud service provider (Azure, AWS, GoogleCloud), database, network switch or sensor has their own proprietary tool to access them. Learning to use so many different tools, switching between them and trying to produce a consistent audit trail can prove to be a huge operational bottleneck for MSPs.

According to the study 'Re-Thinking Privileged Access Management in the Age of Hybrid Cloud' by VansonBourne, IT professionals admitted that:

- 52% would consider bypassing security controls if needed to meet a deadline.
- 71% experience issues with cloud access management solutions that slow down their daily work.
- 85% share account credentials, even though most of them (70%) know and understand this is an issue.

Fortunately, there are ways for MSPs to overcome these security, credential risk, and regulatory enforcement challenges without sacrificing operational efficiency. In fact, with the right approach, MPSs can reduce complexity from their managed environments, turn security into a competitive advantage, and even adopt new business models with their customers. We call these WIN, WIN, WIN scenarios.

WIN #1: Improve secure access to customer environments

Mitigating credential and compliance risk

As MSPs grow and take on more customers, naturally the associated risk will increase, including becoming prime targets of cyber threats. By compromising MSP access, bad actors can gain entry to many customers' infrastructure, intellectual property, and data. Therefore, **it is imperative that MSPs treat their own admin access into customer networks as privileged**. If a data breach for a key customer is attributed to MSP access, this will cause severe reputational and long-term revenue impacting damage to the MSP.

MSPs need to adhere to the compliance and regulatory requirements (like the already-mentioned NIS 2.0 and the US Presidential Executive Order) to retain and win new customers. **Providing audit trails, session recordings, and reports to show exactly who did what, with what rights, and when is essential.** Additionally, proving that you have controls in place around providing, modifying, and removing access to privileged accounts is a must-have for many customers.

PAM tools are purpose-built to manage access to critical targets and manage privileged credentials. It is no surprise that Gartner has placed PAM projects as the second most important for business to deliver adequate controls. Additionally, Gartner have stated that businesses will mostly move away from using password based access by 2022. **Deploying effective PAM solutions is proven to be one of the most impactful projects to undertake in terms of reducing cybersecurity risk.**

Reducing the number of secrets to manage

Using passwords and keys to provide MSP access to customer environments can be reduced by **adopting modern solutions that use Just-In-Time (JIT) certificates for authentication**. The certificates are created on the fly upon establishing the privileged connection and automatically expire after the authorization, leaving no credentials behind for misuse. Futhermore, the secrets needed for authentication are baked into the certificate which the user never sees or handles.

This approach reduces the risk of password compromise and the implied dangers mentioned earlier (reputational damage, service outage or data theft). Analysts agree:

"It's an innovative approach but one that does bring functional and security advantages – access is faster, onboarding and offboarding of privileged users is quick and there are not passwords to issue or lose, since there are no permanent, leave-behind credentials."

– Paul Fisher, Senior Analyst, KuppingerCole

Adopting an effective access management model for access to customer environments should give MSPs peace of mind that they are able to meet the compliance and regulatory needs of any new or existing customer.

WIN #2: Simplify access administration

An effective MSP access management environment should not only improve the security of providing access to customer environments, it should also simplify the processes around access administration and customer onboarding.

One UI to rule them all

A centralized, easy-to-use, intuitive web-based UI makes it much easier to launch connections to customer environments rather than using a variety of different clients or proprietary software with different user experiences. The UI is also the go-to place to see what accounts and targets MSP admins have access to. The UI also allows managing access to new accounts with minimal amount of effort and manual work.

Stay in sync with joiners, movers and leavers

Privileged access associated with MSP admins needs to be easily administered. The joiner-mover-leaver process of MSP admins should be built into the access governance processes: add, modify, and remove associated privileged access automatically without having to use multiple registries or manual steps, easily providing multi-factor authentication (MFA) to certain admins or for access to specific systems for added security is also a big plus.

Auto-discover hosts in hosts under management

New customers and associated hosts should be easily on-boarded. Automatic discovery of hosts can reduce the time and effort taken to onboard new customers and provide access to their IT environment. As new assets (servers, switches, apps) are provisioned, MSPs should be able to be easily keep in sync with the changing IT landscape under management.

Reduce the complexity of credential management

Typically, MSPs have been provided access to customer environments using passwords or keys. These keys or passwords are often exposed to the MSP admins and need to be managed at significant risk, time, and effort.

A modern way to reduce the secrets management effort is to avoid using passwords or keys for authentication where possible. Access methods that are based on Just-In-Time (JIT) certificates for authentication not only eliminate the need for credential exposure, but also remove the need for their rotation and distribution. As mentioned, JIT certificates simply authenticate the user, after which they expire automatically. This is not only more secure but also a big boost to operational efficiency and a way to keep the environment under management lean and clean.

Vault when needed

Where passwords and keys are still necessary (some environments don't support passwordless authentication), they should be controlled based on roles in a multi-tenant vault. Customers should be able to update the vaulted passwords or keys without exposing the credentials to the MSP admins. Where vaulted passwords or keys are still used, the MSP admins should be able to use vaulted passwords without being able to see them.

Go beyond VPNs and firewalls

A common approach for MSPs to access customer environments is through the management of many VPN or firewall configurations. Customer VPNs are commonly overloaded, particularly with the dramatic increase in remote work in recent years.

Additionally, VPNs and firewalls can grant access to MSPs that is much broader than the access required to do their tasks. Reverse proxy-based technology can eliminate the need to use multiple VPNs altogether and provides a more secure, least privilege driven and granular level of access to the MSP admins.

WIN #3: Increase MSP revenue opportunities

MSPs can offer to run a managed on-premise PAM service or a cloud-based PAMaaS to existing and new customers. **When done right, a PAM service which is fully integrated with customer deployment, service desk ticketing, and user provisioning workflows becomes an incredibly sticky solution.**

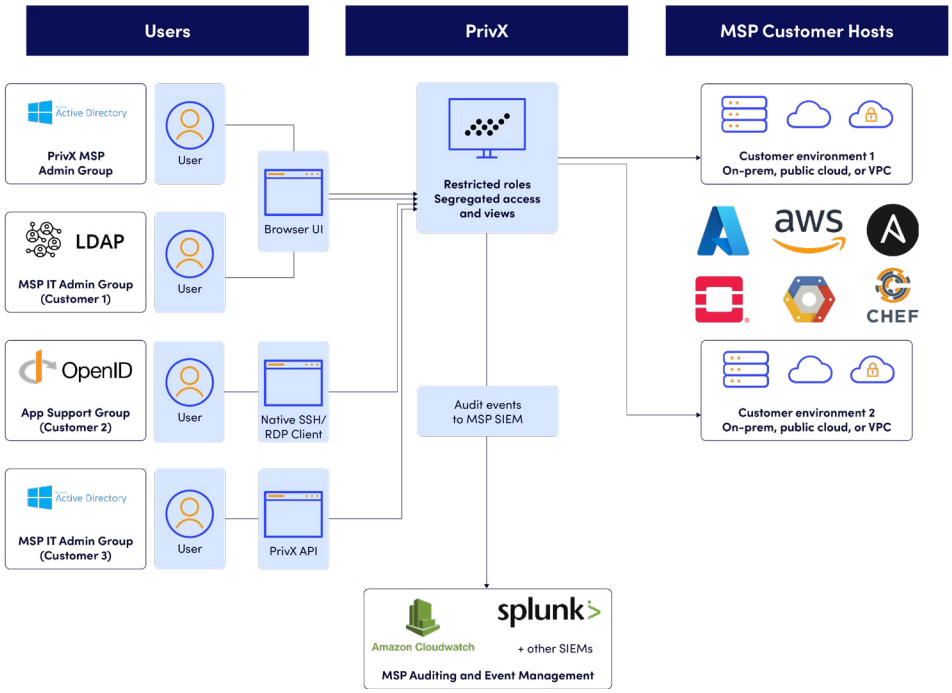
With the right selection of a PAM solution, this can lead to significant, long-term service revenue opportunities. We have successfully worked with Global System Integrators to develop their own cloud hosted PAMaaS solution for their customers.

In order to maximize revenue, an MSP will need to select a PAM solution with low TCO (Total Cost Of Ownership). This is not merely in terms of licensing, but also deploying and maintaining the service. A PAM solution with high levels of automation capability (user/server/customer on/off-boarding) certainly helps reduce TCO, which can lead to higher profit margins for MSPs.

MSPs offering a multi-cloud supporting, cloud-native PAM solution are able to use this deployment to offer additional consultancy services assisting their customers with moving workloads to cloud. New service offerings and revenue opportunities can also be built around cloud migration strategies.

Why PrivX® MSP Edition is a perfect PAM solution for MSPs

At SSH Communications Security, we developed a truly unique PAM solution, which we believe is perfectly suited to MSPs.



Auditing, session recording, and reporting

MSPs can connect to a wide range of target servers using SSH, RDP, HTTPs, or VNC encrypted protocols as required. Every MSP admin session is authenticated to an individual User Identity which the MSP can manage independently. Role-based access can be provided to privileged users on customer IT systems. Reports for compliance readiness and internal auditors can be easily produced to send to customer internal auditors when required.

Audit events can be passed to MSP SIEM (Security Incident & Event Management) system for alerting purposes. Each session will record the user identity, start time, end time, role used, authentication method used, target account, target server, and whether files were transferred. Full session recordings can be replayed and provided to auditors for forensic analysis.

Enforce Zero Trust for access to customer environments

Ensure only authorized admins have access to customer systems. Integrated directly with MSP User Directory, privileged access for MSP admins can be kept tightly coordinated with MSP joiner-mover-leaver processes. Access is granted and removed automatically. Additionally, MFA can be easily added for access to the most critical systems.

Versatile authentication methods to customer infrastructure & multi-tenant vault

MSPs must deal with many customers with various requirements how to authenticate to their environments. PrivX offers unique passwordless authentication for SSH and RDP connections, reducing risk of password compromise and the overhead of password management.

Additionally, authentication to targets can be made with vaulted passwords, user provided passwords, or SSH keys. Customers also can update passwords in the vault to be used without being exposed to MSP admins.

Cloud native deployment

Adopting a PAM solution that can easily be deployed to major cloud providers has compelling and major benefits for MSPs. Cloud-native services such as load balancers, availability zones, auto-scaling, and database services allow to easily build a highly available and auto-scaling solution.

This is particularly important so that MSPs can take on new business without concern of not being able to handle the load. With this in mind, PAM solutions with a micro-service architecture and cloud-native tooling will ensure that the PAM service can always meet the needs of the MSP. PrivX MSP Edition additionally has strong high-availability capabilities, making it ideal for demanding customer environments.

Multi-cloud capable – secure access into any cloud major provider & hybrid environments

Many large customers are adopting a multi-cloud strategy as they identify which workloads they wish to move to different cloud platforms. This, coupled with MSPs working with customers that will adopt various cloud platforms and strategies, means that the PAM system adopted by an MSP really needs to be able to work across all the major cloud providers (Google, AWS, Azure, OpenStack).

PrivX MSP Edition has the added advantage of being able to auto-discover cloud hosts and use cloud host-tagging functionality to manage access to servers without making changes to target host.

Accessing restricted environments

PrivX Extender Components offer a unique reverse proxy capability to connect to restricted customer environments such as VPCs, DMZs, or connecting to customer perimeter.

Case study: Fujitsu using PrivX in customer managed environments

FUJITSU

Securely connecting to customer managed environments

Fujitsu built a multi-tenant PAM solution based on PrivX to provide secure access for Fujitsu IT admins to connect into customer managed environments. This PAM solution provides fully audited and secure access for over 4500 admins to over 1000 customers across Europe.

PrivX did not only offer advanced technology and simplicity of management for Fujitsu, but also superior Total Cost of Ownership: PrivX TCO was 30% when compared to a previous traditional PAM solution used by Fujitsu.

Privileged Access Management as a Service

PrivX is now being fully utilised by our partner Fujitsu to deliver PAMaaS offering to its customers across Europe, Middle East, and Africa.

Fujitsu offers a true cloud-hosted PAM as a Service. Architected across multiple availability zones in AWS (Sweden, UK and Dublin), this service can be easily spun up and provided to customers instantaneously and auto-scaled as service. A full project and managed service offering is built around this PAMaaS to ensure high levels of customer satisfaction as well as long-term managed service revenue and project-based revenue for Fujitsu.

Conclusion

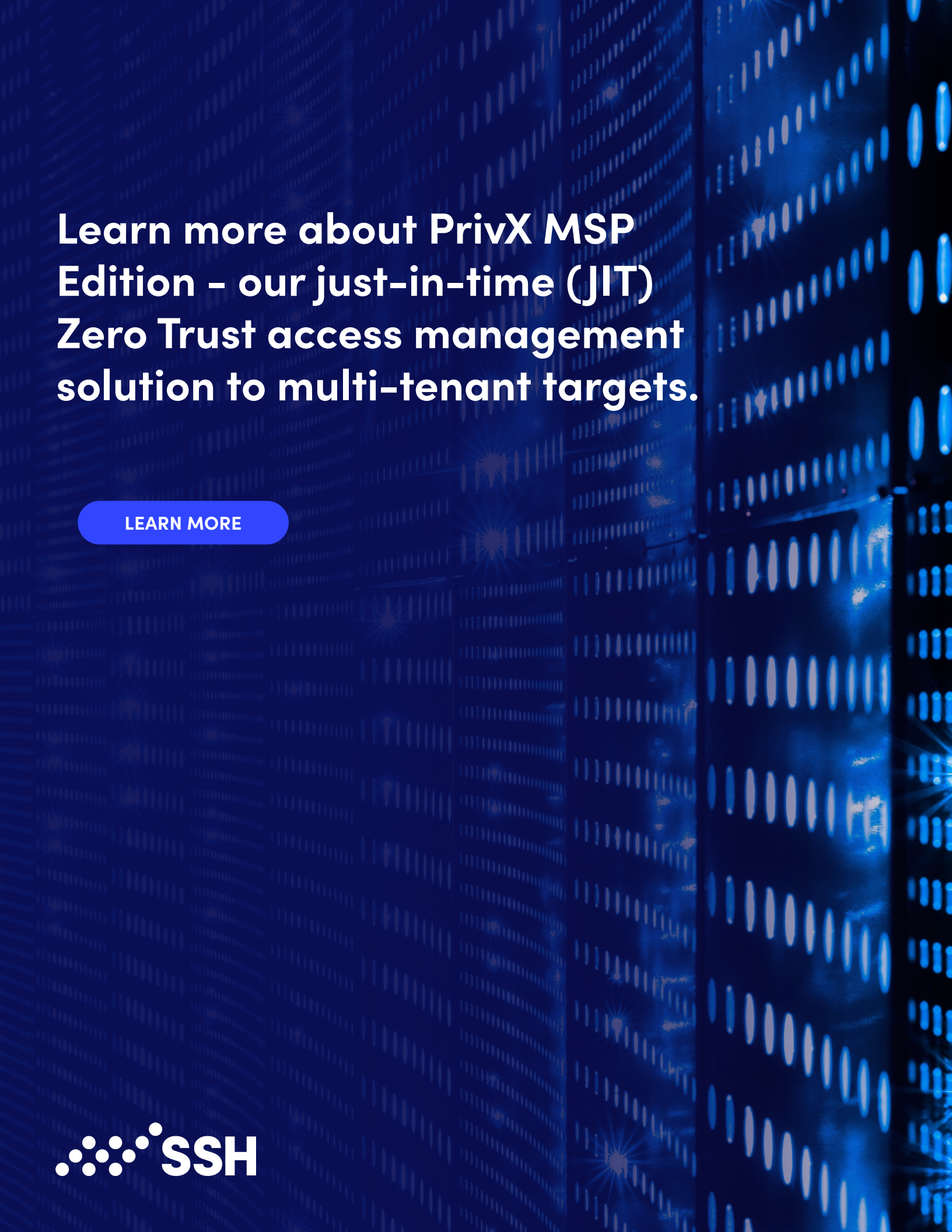
Any respectable company operating in customer environment should take security seriously. Fortunately, with the right type of Privileged Access Management solution, any company can achieve:

- Secure remote access
- Managing required privileged credentials while reducing their numbers
- Reducing overall system complexity
- Automating onboarding of both hosts and users
- Ease-of-use and fast deployment
- Fast Return on Invesment (ROI) and a low Total Cost of Ownership (TCO)

After all, robust cybersecurity and proper access controls are not only ways to ensure your reputation and business continuity with your customers, they open doors to new business opportunities and new business models (like PAMaaS) for MSPs.

Our PrivX MSP Edition makes securing environments under management easy and productive for MSPs.

SSH


Learn more about PrivX MSP Edition - our just-in-time (JIT) Zero Trust access management solution to multi-tenant targets.
LEARN MORE
SSH

We'd love to hear from you!

Get in touch with our experts around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH Communications Security Oyj
Karvaamokuja 2D
00380 Helsinki
Finland
Tel. +358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH Communications Security Inc.
66 Hudson Blvd E, Suite 2308
New York, NY, 10001
USA
Tel: +1 (212) 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Singapore

SSH CommSec Pte. Ltd.
6 Raffles Boulevard, Marina Square, #03-308
Singapore 039594
Singapore
Tel. +65 6338 7160
sales.asia@ssh.com

SSH