Fujitsu Secures Admin Connections to European Customer Managed Environments

Case study

Summary

Fujitsu uses their CME environment to govern and manage access to customers' environments. Fujitsu has multiple large customers in their managed environment, providing hosting, network management, application services, SOC (Security Operations Centre) & SIEM (Security Incident & Event Management) services and development.

Previously deployed traditional PAM solution required managing jump hosts and maintaining manual configurations to environments under management. This was particularly **demanding and time-consuming in dynamic, multi-cloud customer environments** and while granting different levels of privilege to admins who manage those environments.

With **PrivX MSP by SSH Communications Security**, Fujitsu can ensure governed, controlled, audited access in a Just-In-Time manner and without the risk of leave-behind credentials. This improved security and operational efficiency and lowered the cost of providing their services to customers.

Fujitsu was also able to leverage their own IDM solution for identities simply by interfacing PrivX with it. PrivX automatically syncs identities with the right privileged roles no matter how often the identities change or are revoked.

Customer Background

Fujitsu is a global IT service provider and IT equipment manufacturer with several thousand customers across the globe, 27B+ € turnover, and around 125 000 employees.

Fujitsu (Europe) provides IT managed services to 1000+ Customer Managed Environments (CMEs) across their Northwest Europe Division, spanning the UK, Ireland, Nordics, and Benelux.

Challenge

Fujitsu has 4500+ IT admins to provide their managed services to 1000+ customers, covering 30 000+ servers under management.

The admins need to securely connect to customer environments – it is often mandated by the customers that the admin sessions must be recorded and granted access must be secure, fully audited, and tighly controlled.

Previously deployed traditional Privileged Access Management (PAM) solution required managing multiple jump hosts and maintaining manual configurations to environments under management to meet customers' requirements. This was particularly demanding and time-consuming in dynamic, multi-cloud customer environments and while granting different levels of privilege to admins who manage those environments.

Fujitsu's goal was to find a solution with low Total Cost of Ownership (TCO) that is cloud-native by design and highly automatable to ensure high operational efficiency. After comparing the available PAM tools on the market, Fujitsu selected PrivX MSP from SSH Communications Security.

Solution Overview

PrivX is used for privileged access within Fujitsu's CMEs. The solution provides **a unique and modern approach to PAM, particularly suited to enterprises that have a hybrid of on-premise and cloud infrastructure** and need to operate a secure Zero Trust environment.

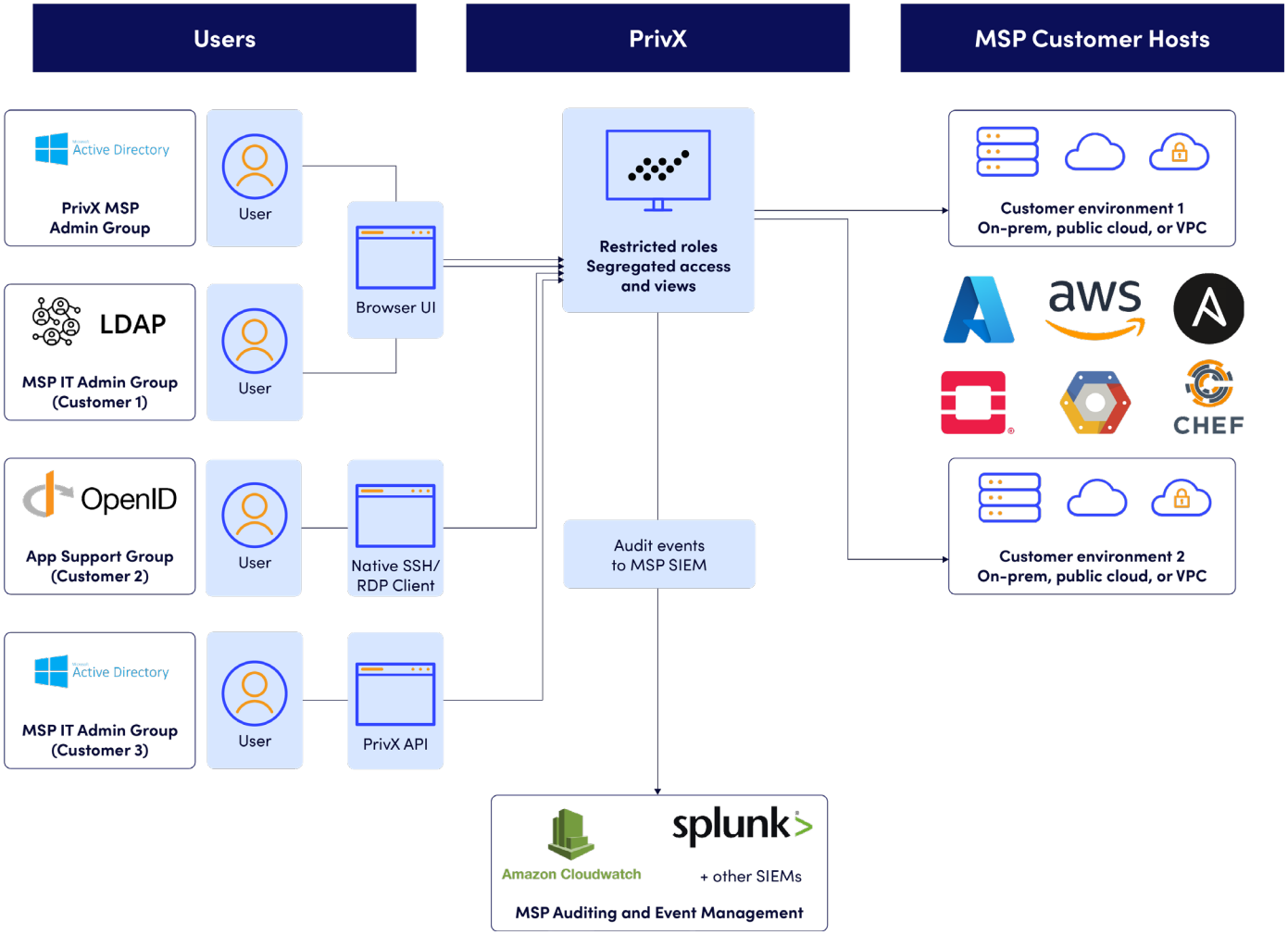
Fujitsu can now ensure **governed, controlled, audited access in a Just-In-Time manner and without the risk of leave-behind credentials**. This improved security and operational efficiency and lowered the cost of providing their services to customers.

Fujitsu was also able to leverage their own IDM solution for identities simply by interfacing PrivX with it. PrivX automatically syncs identities with the right privileged roles no matter how often the identities change or are revoked.

SSH

About PrivX MSP

↓ *An example deployment of PrivX into a CME environment.*



PrivX MSP is a (privileged) access management solution that is simple to maintain and advances your security control by using the principle of least privileges and allowing Just-in-Time connections, with just-enough access, only for the amount of time necessary.

It removes the dependency on passwords (and keys), controlling access to both cloud-hosted and on-premise systems/applications. PrivX eliminates the risk of credential theft, removing the greatest security risk in PAM, as the access to endpoints is provisioned using on-demand short-lived (ephemeral) certificates that are valid for only a few minutes, never stored to disk, and never exposed to end-users.

Additionally, PrivX interfaces directly with your identity management system so that your Joiner-Mover-Leaver processes can seamlessly align with associated access management rights.

SSH

Solution Deployment (into AWS) & Usage

PrivX can be architected for a large MSP environment as follows:

- PrivX environments can be deployed into different AWS availability zones (e.g. Ireland, UK, Sweden) across various public cloud environments.
- Connections to PrivX UI controlled by AWS Application Load Balancer
- Architected with AWS native-cloud services for Elastic File System and RDS
- Auto-scaling based on demand with new Privx instances spun up as computing capacity is required
- PrivX Extender components can be deployed into the customer (often restricted) networks to provide a reverse proxy connection to the customer servers from the central Privx instance
- Customer admins have role-based access control (RBAC) to specific customer environments using AD groups
- Ad-hoc access to customer environments can be requested using Privx in-built workflows
- Multi-factor authentication (MFA) can be enforced if required

Fujitsu enabled their 4500+ admins to access 1000+ customer managed environments via PrivX over 18-month-long period:

- All customer environments migrated to be accessed via PrivX
- PrivX configuration centrally managed by Fujitsu Service Security team
- Separate audit role created to provide access to review audit logs and session recordings only
- Admins only allowed to access specific customer environments (AD membership controlled)
- Customers can be provided audit logs of all activities when required
- On- and off-boarding new customer environments is highly automated with low TCO

Fujitsu Project Roll-Out

Fujitsu Service Delivery team have built up the PrivX infrastructure and successfully migrated 1000+ customer environments to be connected via using PrivX infrastructure.

Environment	Month, year	# of CMEs	Estimated users
Ireland, Pre-prod	November 2020	20	10
Sweden Prod	January 2021	50	400
Ireland Prod	May 2021	85	430
UK onboarding	July 2021	155	2000
	September 2021	225	
DSPU onboarding	December 2021	750	2500
Finland onboarding	June 2022	1000+	4500+

Usage Information (PrivX Environments)

PrivX instance	Purpose	Users	CMEs	Average concurrent RDP sessions	Maximum concurrent RDP sessions	Average concurrent web sessions	Maximum concurrent web sessions
AWS London	UK & Ireland Prod	2000	200	250	500	50	100
AWS Stockholm	Nordics Prod	500	50	50	200	10	50
AWS Dublin	Pre-prod	100	50	20	100	10	50

Hardware Specifications (PrivX Environments)

Component	Type	Count	London			
			Instance/node	CPU	Memory	Storage
PrivX Server	EC2 instance	2	c4.2xlarge m5.xlarge	8vCPUs 4vCPUs	15360MB 16GB	20GB
PrivX Database	AWS RDS		db.t3.medium	2vCPUs	4096MB	100GB
PrivX Redis Cache	AWS ElastiCache		cache.t2.small		1.5GB	
PrivX Carrier	EC2 instance	4	m4.2xlarge	8vCPUs	32GB	60GB
PrivX Web Proxy	EC2 instance	4	c5.large	2vCPUs	4096MB	10GB
Audit Trail Storage	AWS EFS					

Component	Type	Count	Stockholm			
			Instance/node	CPU	Memory	Storage
PrivX Server	EC2 instance	2	c4.xlarge m5.xlarge	4vCPUs 4vCPUs	7680MB 16GB	20GB
PrivX Database	AWS RDS		db.t3.medium	2vCPUs	4096MB	100GB
PrivX Redis Cache	AWS ElastiCache		cache.t2.small		1.5GB	
PrivX Carrier	EC2 instance	4	m4.xlarge	4vCPUs	16GB	30GB
PrivX Web Proxy	EC2 instance	4	c5.large	2vCPUs	4096MB	10GB
Audit Trail Storage	AWS EFS					

Component	Type	Count	Dublin			
			Instance/node	CPU	Memory	Storage
PrivX Server	EC2 instance	2	c4.large m5.large	2vCPUs 2vCPUs	3840MB 8GB	20GB
PrivX Database	AWS RDS		db.t3.medium	2vCPUs	4096MB	100GB
PrivX Redis Cache	AWS ElastiCache		cache.t2.small		1.5GB	
PrivX Carrier	EC2 instance	4	m4.xlarge	4vCPUs	16GB	30GB
PrivX Web Proxy	EC2 instance	4	c5.large	2vCPUs	4096MB	10GB
Audit Trail Storage	AWS EFS					