SSH.COM

CASE STUDY

A Fortune 500 Company Secures SSH connections to Container Environments with Zero Trust Privileged Access Management

Customer in a nutshell

- Multinational Fortune 500 corporation
- Operates primarily in the cloud and offers services purely on-line
- Large container estate with Kubernetes orchestration in place
- Operations in more than 30 countries
- Has a strong drive to be at the cutting edge of technology

Background

The customer is a global Fortune 500 company that has a sizable container estate in-house and their developers are using Docker to speed up and accelerate their application development. To orchestrate their containers, the customer is using Kubernetes - a popular solution to automate computer application deployment, scaling, and management.

While the customer was planning to further expand the use of containerization in the organization, they soon realized that while their container and their orchestration setup was a great fit for their agile development and production lifecycles (like continuous integration/continuous development (CI/CD) pipelines), it could use improvements in one particularly critical area: secure access management.

Taking their cybersecurity needs seriously, the customer started looking for solutions that could help them manage access in a secure fashion in such a modern environment. A further requirement from the customer was that they wanted to run their Kubernetes orchestration in-house, so the solution should support on-prem installations while offering the highly dynamic and automated functions native to container solutions, like auto-scaling and the granularity of microservices.

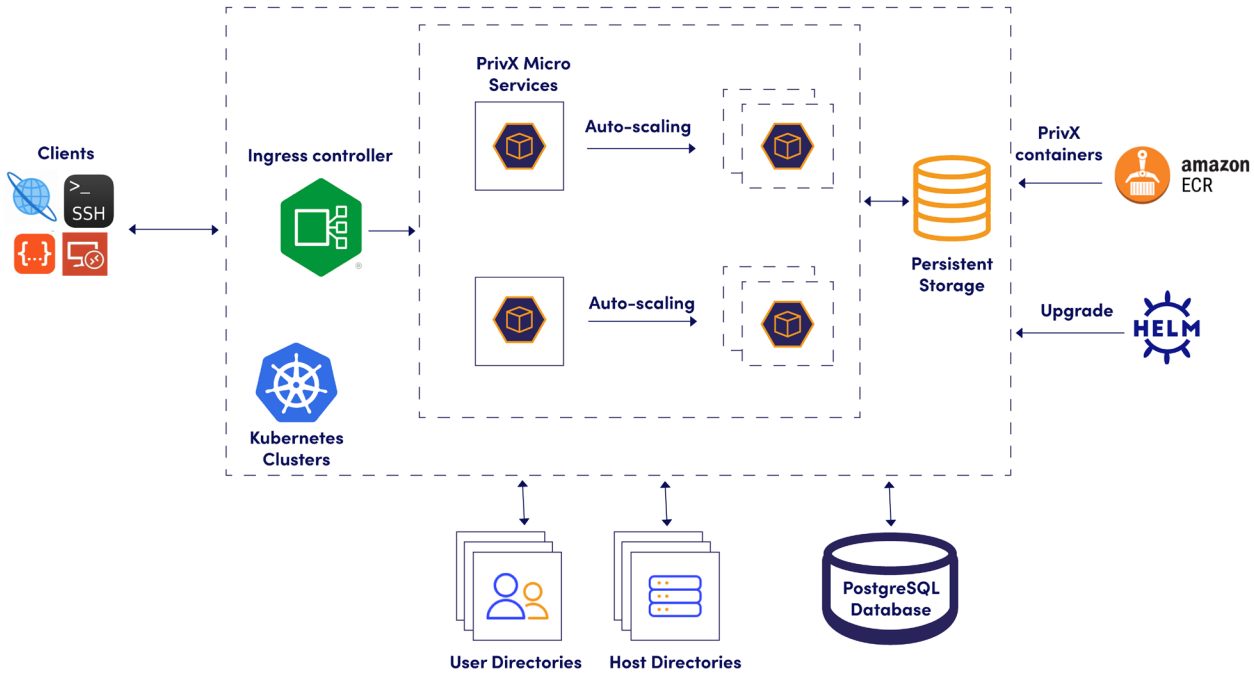
The customer identified privileged access management (PAM) as the category of solutions to investigate further. After all, managing DevOps engineer, administrator and superuser access with a proper audit trail of activities, ensuring access secrets are secured and segregation of duties (SoD) is followed, was considered important. This is exactly what PAM solutions do.

However, it soon become clear to the customer that most solutions on the market were simply not technologically mature enough to support their container and Kubernetes ambitions. Most PAM solutions on the market have been built using legacy technology that was not an optimal fit for their future-driven goals.

PrivX Just-in-Time Zero Trust PAM with microservices for Kubernetes

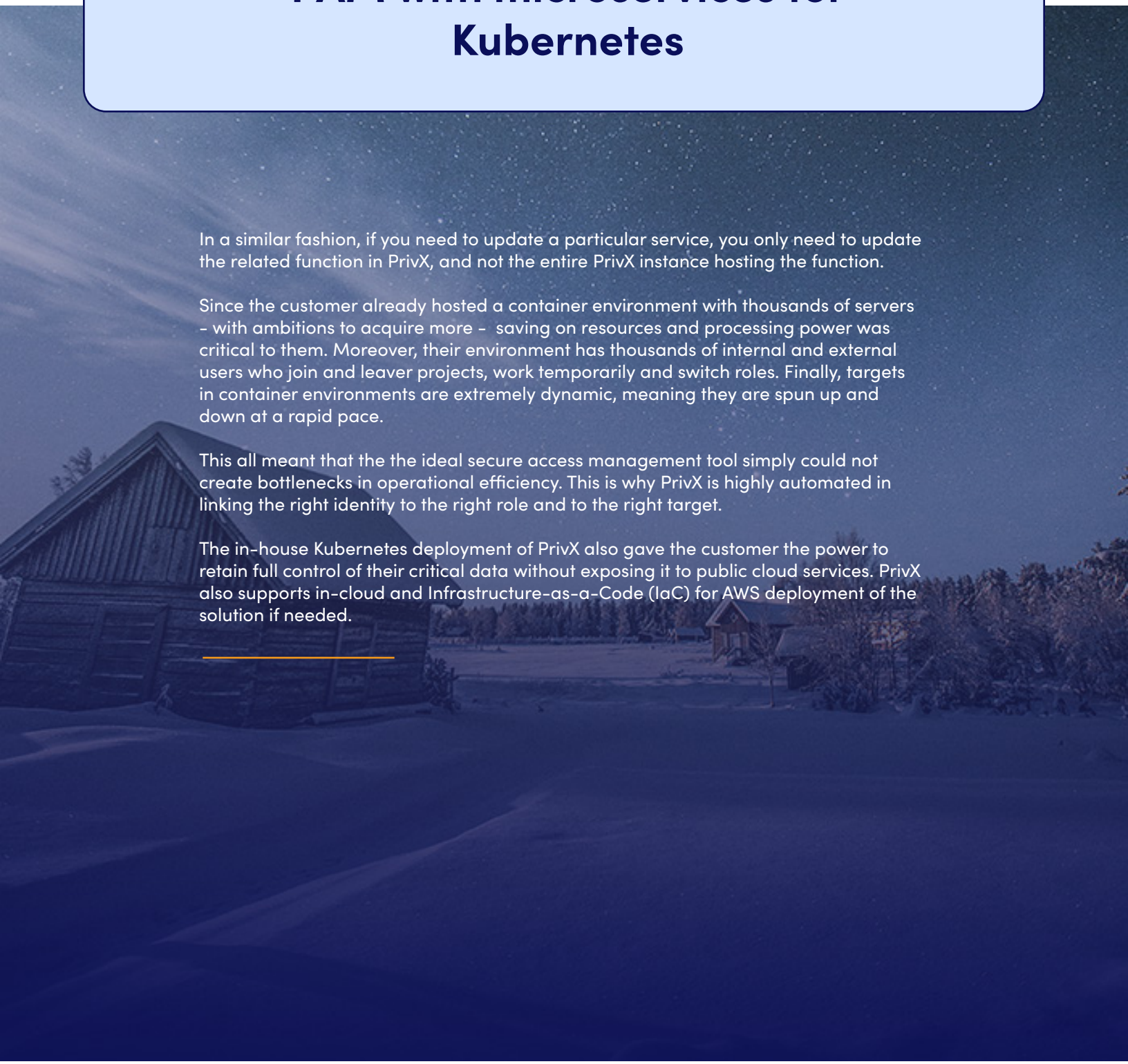
The customer selected SSH.COM's PrivX to solve their critical access management needs. Since PrivX is natively built on modern microservices architecture, running the solution on Kubernetes allows the customer to run their PAM at the same speed, scalability and level of automation as they were accustomed to with their DevOps development lifecycle and using their container orchestration tools.

For example, in microservices architecture the idea is to scale only the function you need at a particular time, instead of trying to scale an entire instance. So let's say that a group of developers have a temporary need for a specific service, and to access that resource, they need more Secure Shell (SSH) connections. PrivX can scale up the function required to establish SSH connections (the PrivX SSH proxies) without the need to scale the entire PrivX instance or set up a new one. This saves resources considerably and allows instant and very dynamic scalability.



SSH.COM

PrivX Just-in-Time Zero Trust PAM with microservices for Kubernetes



In a similar fashion, if you need to update a particular service, you only need to update the related function in PrivX, and not the entire PrivX instance hosting the function.

Since the customer already hosted a container environment with thousands of servers - with ambitions to acquire more - saving on resources and processing power was critical to them. Moreover, their environment has thousands of internal and external users who join and leaver projects, work temporarily and switch roles. Finally, targets in container environments are extremely dynamic, meaning they are spun up and down at a rapid pace.

This all meant that the the ideal secure access management tool simply could not create bottlenecks in operational efficiency. This is why PrivX is highly automated in linking the right identity to the right role and to the right target.

The in-house Kubernetes deployment of PrivX also gave the customer the power to retain full control of their critical data without exposing it to public cloud services. PrivX also supports in-cloud and Infrastructure-as-a-Code (IaC) for AWS deployment of the solution if needed.

Flexibility of the solution and industry expertise appreciated

One of the key customer requirements was that they wanted to maintain the target information in the Forgerock Identity management system (IDM). System for Cross-domain Identity Management (SCIM) is a standard used to automate the transfer user identity information between identity domains, or IT systems - another important customer requirement.

Now SCIM is used to update the information to PAM – in PrivX in this case. The result is that the users get access to the target based on a role and that the IDs, roles and target information are always in sync.

What's more, PrivX allowed the customer to use a PAM solution in a rather unconventional way. In some contexts, many privileged users don't even see PrivX but log in through Open ID Connect (OIDC) to verify their identity and then they simply use native Secure Shell (SSH) connections to access targets. All sessions are still verified, tracked and audited – and recorded if needed.

The customer was impressed not only with the solution itself but the team behind it: the level of expertise and the technical support that the customer received from SSH.COM during the negotiation period factored heavily into the decision to choose PrivX.

Last but not least, the customer appreciated the passwordless and keyless security approach in PrivX.

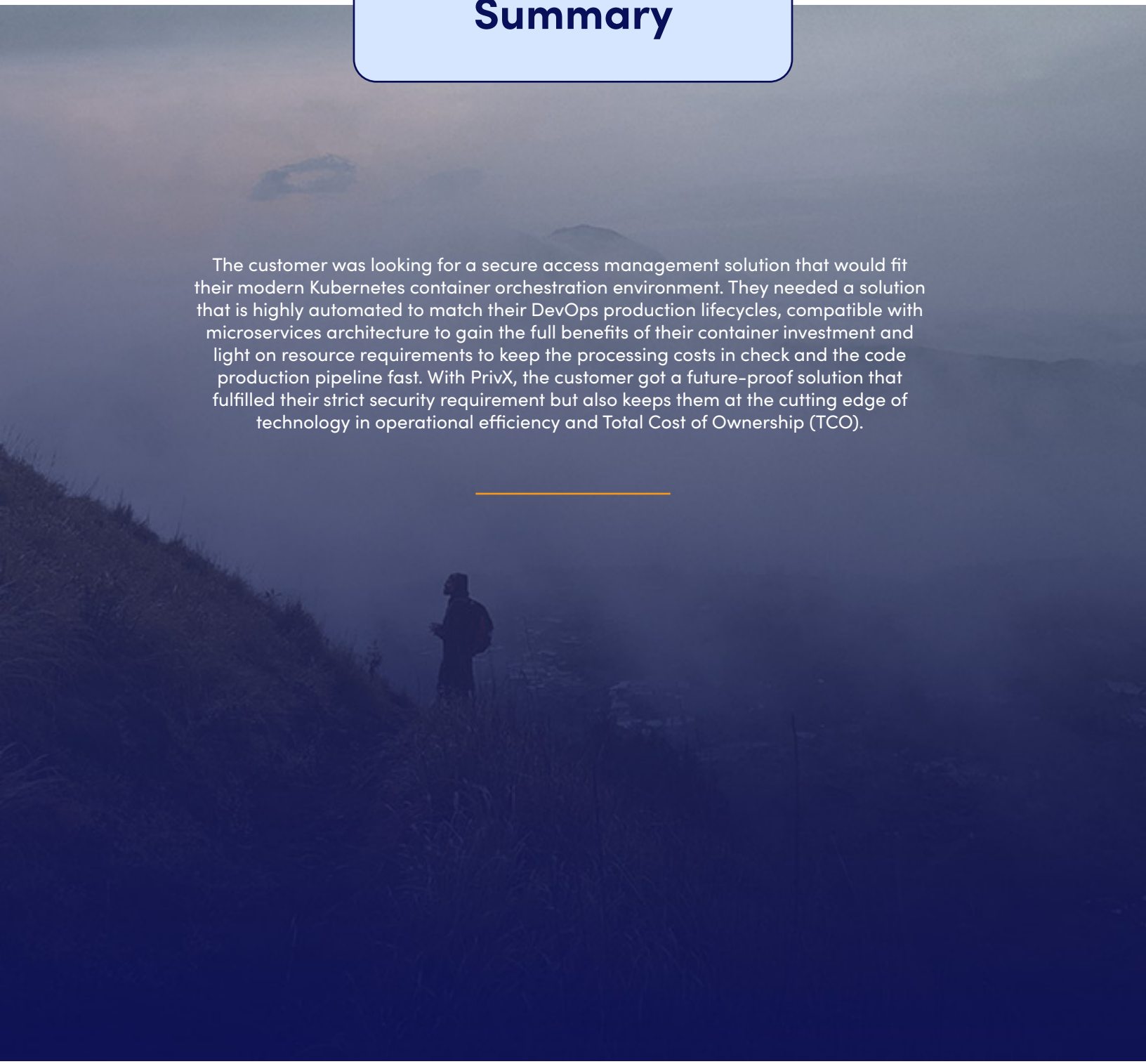
With PrivX, the user never handles or sees any credentials or keys at any point of the process. Instead, upon establishing the connection, PrivX creates a just-in-time (JIT) short-lived ephemeral certificate invisible to the user. The certificate contains all the secrets needed to establish the connection but it expires automatically after the connection is established.

This ensures there are no secrets left behind to steal, lose or misuse which improves security and aligns perfectly with the Zero Trust framework (never trust, always verify).

Furthermore, JIT and certificate based access eliminates the need to vault or rotate passwords or keys, since they simply disappear after the authentication. The customer was happy to hear this, since the approach reduces the complexity and a great amount of processes required in rotation and vault-bases solutions.

Again, eliminating extra processes and keeping the changes to the environment minimal was a key customer requirement.

Summary



The customer was looking for a secure access management solution that would fit their modern Kubernetes container orchestration environment. They needed a solution that is highly automated to match their DevOps production lifecycles, compatible with microservices architecture to gain the full benefits of their container investment and light on resource requirements to keep the processing costs in check and the code production pipeline fast. With PrivX, the customer got a future-proof solution that fulfilled their strict security requirement but also keeps them at the cutting edge of technology in operational efficiency and Total Cost of Ownership (TCO).

Global headquarters
Helsinki

SSH Communications Security Corporation

Karvaamokuja 2 B 00380
Helsinki, Finland
+358 20 500 7000
info.fi@ssh.com

US headquarters
New York

SSH Communications Security, INC

434 W 33rd Street, Suite 842
New York, NY, 10001, USA
+1 781 247 2100
info.us@ssh.com

APAC headquarters
Hong Kong

SSH Communications Security LTD

35/F Central Plaza, 18 Harbour Road
Wan Chai Hong Kong
+852 2593 1182
info.hk@ssh.com