SSH

CASE STUDY

# A Global Manufacturer Secures SSH Connections for the Future with Zero Trust Approach

# Background

## Customer information

- A global manufacturer with headquarters in Europe
- +10B € turnover
- Around 50k employees
- +6500 servers

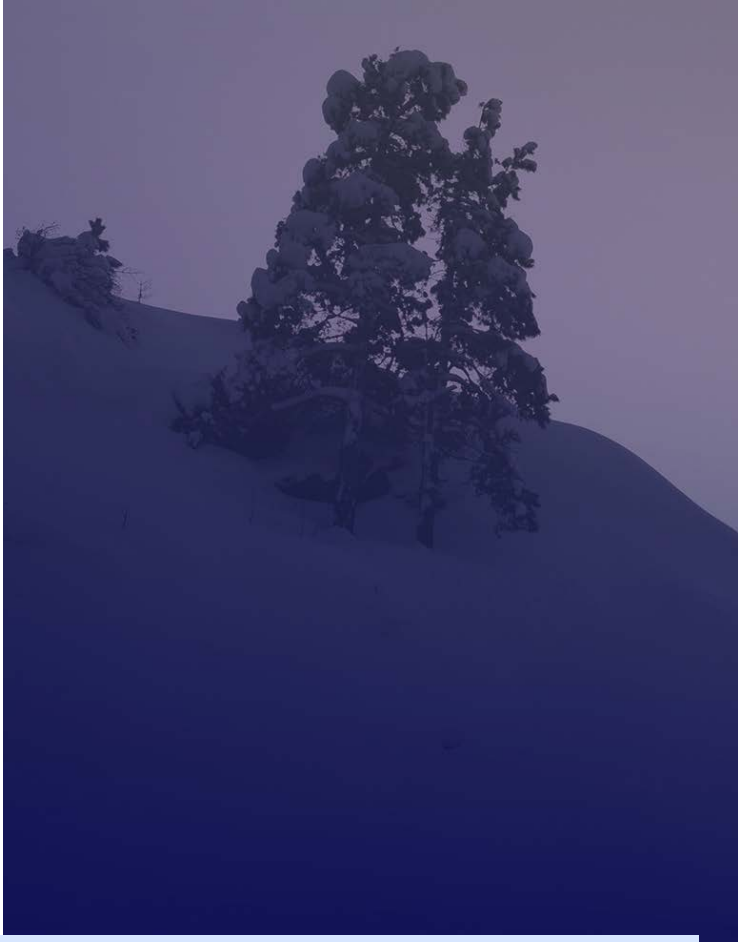
The customer is a global manufacturing business with a turnover of more than 10 billion euros. They have a strong presence and manufacturing sites not just in Europe, where their headquarters are, but all over the world. The company is a global giant with around 50 000 employees, thousands of partners, and even more customers. The company also has an estate of more than 6500 servers - to manage secure access to and between their servers, they use SSH keys.

With this number of employees, third-party partners, manufacturing centers, and servers all around the globe, secure access management is of utmost importance. Therefore, the customer has a privileged access management (PAM) solution in-house.

However, this solution is managing only part of their SSH keys. Specifically, it is managing connections between jump hosts and the rest of the network, but not between the rest of the interconnected servers. This setup only accounts for around 20% of all their SSH connections even with a PAM solution in place. The rest of the keys went unmanaged, without the customer's insight into the issue.

When the company failed one of their internal compliance audits because of rogue SSH keys, they knew that they must inspect the issue carefully and find a solution as fast as possible.

# From unmanaged keys to keyless approach



The company took the situation extremely seriously and decided to map their SSH status thoroughly. After a comprehensive assessment of their large server estate, they discovered that they have over 80 000 SSH keys (out of which 66 000 keys are public and 14 000 keys are private), most of them unmanaged.

## A Structured Approach to SSH Keys Discovery

Thanks to their discovery process, the customer gained a deep understanding of the scope and complexity of the challenge and recognized that they would not be able to manage the issue in-house. There were just too many keys - they were too decentralized across the hybrid IT environment and without anyone having ownership of them.

Therefore, they set out on a search for an external solution provider with the extensive expertise they required. They also needed a solution that would smoothly integrate and cooperate with their existing legacy PAM while adding the necessary Enterprise Key Management capacity.

Additionally, the customer was worried about the accumulating number of SSH keys in their environment and was looking for the most efficient way to solve the challenge.

This led the customer to explore solutions that would allow them to manage their current challenge, but would do so with the least management effort possible.

In the process, they learned about Zero Trust key management that allows shifting away from key management towards a more efficient, future-proof way of SSH access control. Their future vision was not to be content with just managing keys, but to find a solution that would allow them to migrate to keyless approach.

# UKM Zero Trust Just-in-Time (JIT) SSH Access Management

The customer selected the Universal SSH Key Manager (UKM) Zero Trust solution by SSH, as they valued the experience, expertise, and innovative position that SSH holds in the industry. As the name suggests, the company is the inventor of the Secure Shell (SSH) protocol.

To deliver the SSH access project, the company also collaborated with one of our Global Systems Integration Partners, Tech Mahindra.

The UKM Zero Trust solution helps with:

## 1 Mapping of SSH keys

UKM finds all customer's SSH keys and creates a complete 'web of trust' formed by keys between servers. It also reports which keys are uncompliant, violating policies, or providing access outside the company.

## 2 Centralized management of SSH keys

With UKM, companies can manage thousands of keys from a single pane of glass. It constantly monitors the keys and their validity. It streamlines the key management by alerting the IT admins every time a key expires or is due for renewal. Old or rogue keys can also be easily and safely removed without disrupting critical connections.

## 3 Automation

With many keys and complex infrastructures, typical for modern IT environments, efficient and timesaving SSH access management is crucial. UKM can be used to automate the full lifecycle of SSH keys, including all processes such as keys discovery, monitoring, renewal, revocation, and provisioning.

## 4 Migration to keyless JIT access

UKM makes it possible to radically reduce the number of SSH keys to manage. Instead, UKM supports the transition towards keyless SSH access through short-lived, ephemeral certificates.

Ephemeral certificates are issued just-in-time (JIT) on making the SSH connection, and they contain the key pairs needed to authenticate the connection. After the connection has been established, the certificates expire automatically, leaving no keys behind to manage. When a new connection is made, the process is repeated. This makes the solution Zero Trust proof, since it verifies each connection every time it is made without granting permanent authorization to anyone.

All this is invisible to individual users, since they never see or handle the keys at all, improving the security posture of the company.

After the initial implementation of UKM Zero Trust, the customer knew that UKM is exactly what they wanted. It integrates smoothly with the customer's PAM, as they required from the chosen solution. The PAM solution takes care of password vaulting and session management, and UKM manages access control and migration from key-based to certificate-based connections.

In the end, the customer fully adopted the keyless, JIT access. With UKM's hybrid approach, they still needed to manage a certain amount of SSH keys while reducing the management overhead with certificate-based access. Eliminating SSH keys completely and using certificate-based access was the next logical step for the company to ensure that their secure access management is truly future-proof.

# Summary

After a failed audit, the global manufacturing business dived deep into discovering the scope of their SSH keys management issue. They soon realized that their PAM solution is not sufficient to manage their whole SSH keys estate, which spans over more than 6500 servers.

During the discovery process, the company also came to the conclusion that finding a solution just to manage their SSH keys is not enough. Their ultimate goal was to find a future-oriented solution that would help them manage the current SSH keys challenge and, at the same time, it would support migration towards keyless, certificate-based SSH connections. Based on these and additional requirements, the customer selected Universal SSH Key Manager (UKM) Zero Trust by SSH.

UKM Zero Trust helped the customer to solve their current challenge by mapping, managing, and automating their SSH keys access. On top of that, thanks to UKM's hybrid approach, the customer was able to adopt the future-proof keyless approach to SSH access management.


## Finland

SSH Communication Security Oyj
Karvaamokuja 2 B 00380 Helsinki
www.ssh.com
+358 20 500 7000
info.fi@ssh.com

## USA

SSH Communication Security, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001 USA
www.ssh.com
+1 781 247 2100
info.fi@ssh.com

## Hong Kong

SSH Communication Security LTD.
35/F Central Plaza, 18 Harbour Road
Wan Chai
Hong Kong
www.ssh.com
+852 2593 1182
info.fi@ssh.com