

The logo for SSH.COM, featuring a cluster of black dots of varying sizes to the left of the text "SSH.COM" in a bold, black, sans-serif font.

SSH.COM

The logo for MOST Digital, featuring a stylized blue and white circular graphic to the left of the text "MOST Digital" in a black, sans-serif font.

MOST  
Digital

A stylized illustration of a blue robot with a red cap and a black visor, holding a globe. The robot is positioned in front of a large computer monitor displaying a globe. The background is a mix of red and grey tones with various mechanical gears and a person working at a computer.

# CASE STUDY

Secure access  
for robots  
to critical  
customer data

# Secure access for robots to critical customer data

*So much of the workday is taken up by rote, manual tasks – filing reports, sending routine emails, updating documents – that could easily be handled by a machine instead. MOST Digital is focused on finding and automating these tasks. The technology consultancy provides robotics-as-a-service (RaaS), examining bottlenecks in a customer's business processes to identify and automate small processes normally done by humans. From finance, to human resources, to sales, to production, there are many parts of the business that can benefit from software robotics automation, which runs 24/7 and makes fewer errors than humans. MOST Digital has built these solutions for more than 200 major companies.*

## Brief background

In the course of their work, MOST Digital's developers must interact with multiple cloud-based systems across owned and client IT environments, plus handle sensitive customer data. The company traditionally used VPN tunnels and jump hosts to connect to customer environments but found this system too awkward and difficult to manage. So, they decided to evaluate a simpler, easier to manage secure access solution. PrivX was the answer.

## Efficient and compliant replacement of customer-specific jump hosts

Microsoft Azure forms the backbone of MOST Digital's IT infrastructure. They use Azure to run the robots' Python-based code objects, and to host sophisticated data warehousing, processing, modeling and machine learning capabilities. However, all client data remains stored in the customer's own IT environment.



As a result, MOST Digital must orchestrate access for its own staff, for its robots, and sometimes third parties, to customer architecture, accessing only the required target systems.

“Customer data can be in a different cloud provider like Google Cloud or AWS,” said Sami Säisä, Director, Head of Strategic Development, MOST Digital. “And then there is the possibility that a customer is using a hybrid environment, or might only have on-site infrastructure in place. This means that our robots will have to connect to all different kinds of environments.”

**“Customer data can be in different cloud providers like Google Cloud or AWS. And then there is the possibility that a customer is using a hybrid environment, or might only have on-site infrastructure in place. This means that our robots will have to connect to all different kinds of environments.”**

Sami Säisä, Director, Head of Strategic Development MOST Digital.

MOST Digital developers rely on Python 3, Github and open source APIs to connect to customer enterprise resource planning (ERP) software and other back office systems. Additionally, VPN gateways and customer-specific jump hosts were used to connect to client virtual machines. However, managing all of the user accounts and access rights attached to these unique jump hosts is inefficient.

As a result, a key requirement for any new secure access solution would be to make it easier for MOST Digital’s software developers to get the access they need quickly.

“At MOST Digital, we employ passionate and talented programmers,” said Mr. Säisä. “We want to provide them the best environments and best tools available.”

Security would also be critical.

“We are handling very sensitive customer data,” he added. “We are using machine learning and robots to access the customer environment. And this means that security is a key priority for us.”



## Granting robots secure access to customer data

MOST Digital had several considerations during the evaluation process. Chief among them was earning the trust of client decision makers, operational staff and internal auditors who might be skeptical of cloud-based secure access solutions.

A new solution would also need to address several challenges:

- There is major segregation of duties challenge, particularly with troubleshooting robotization. MOST Digital would have to find a way to grant and control access for machine identities to the production environment.
- Robots could only have access to internal client systems, which meant restricting access to external gateways.
- MOST Digital would have to account for the user interfaces of enterprise back office systems, which can be slow and easily susceptible to critical errors.
- MOST Digital would need a way to grant extended access to key client systems and multi-source data to third-party partners.

## Single sign-on for robots, control and compliance

In a test, MOST Digital found that PrivX, the lean agile privileged access management solution for multi-cloud environments, was the best solution for its needs.

**“When we started using PrivX, it took us four hours to set up the test environment from start to finish.”**

Sami Säisä, Director, Head of Strategic Development, MOST Digital.

“When we started using PrivX, it took us four hours to set up the test environment from start to finish,” said Sami Säisä. “And the amazing part was when we connected to Azure, we could retrieve all the VMs that were part of the testing environment right away without any kinds of hassle.”

Now, MOST Digital relies on PrivX as an advanced site-to-site gateway to all different kinds of client environments, whether it’s the cloud, hybrid or on-premises.

“At the moment, we use PrivX to provision access to customer-specific environments in MOST platforms,” he said. “However, PrivX can also be used to grant SSO access for robots into customer-owned environments.”

MOST Digital is able to apply policies to robot access similarly as they are applied to humans. Machine and software identities, Active Directory accounts and user accounts are all mapped to access roles.



As for security, PrivX provides the automated reporting and auditing capabilities that MOST Digital needs to prove to customers that no unauthorized access has occurred during their work.

“As a managed service provider, it is very important to have the customer’s trust that we are handling their data appropriately,” Mr. Säisä said. “We have to demonstrate to the customer proof of what we have done in their systems and with their data. PrivX gives us the perfect tool to show this. And it also gives peace of mind to our programmers that they don’t have to run their own audit trails.”

**“We have to deliver the customer proof of what we have done in their systems and with their data. PrivX gives us the perfect tool to show this.”**

Samu Säisä, Director, Head of Strategic Development, MOST Digital.

## Just-in-time access for just-in-time business processes

Just as MOST Digital’s robots eliminate redundant work for their customers, PrivX has been able to simplify and speed up redundant work for MOST Digital. Now, the company has an easy way to facilitate access to client systems so they can conduct their evaluations, without having to waste time on multiple access requests or having to provision access on the fly.

“PrivX has provided us with a hassle-free tool to provide ad-hoc access to customer production environments without the need for cumbersome ticketing systems and approval processes,” Samu Säisä said.

Ironically, robotics-as-a-service is a very human discipline with focus on motivation, productivity, quality and the customer’s underlying values. MOST Digital success stories typically come from robots supporting staff, increasing their productivity, and enabling people to focus their core specialties.

This experience is mirrored in MOST Digital’s own use of PrivX, bringing complex security, access and audit processes for multiple end-customers into an intuitive centralized console.

“PrivX allows our core programmers to focus on programming. They don’t have to worry about security.”





### **Finland**

SSH Communications Security Oyj

Kornetintie 3, 00380 Helsinki

[www.ssh.com](http://www.ssh.com)

+358 20 500 7000

[info.fi@ssh.com](mailto:info.fi@ssh.com)

### **USA**

SSH Communications Security, Inc.

460 Totten Pond Road

Waltham, MA 02451

(781) 247-2100

[info.us@ssh.com](mailto:info.us@ssh.com)

### **Hong Kong**

SSH Communications Security Ltd.

51/F Hopewell Centre

183 Queen's Road East

Wan Chai, Hong Kong

+852 3602 3072

[info.hk@ssh.com](mailto:info.hk@ssh.com)