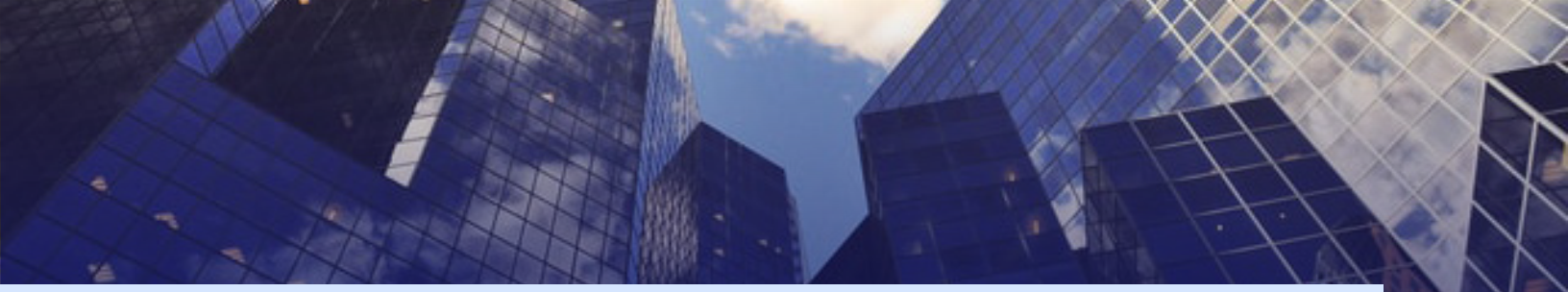
SSH.COM

CASE STUDY

# Quick-to-deploy Privileged Access Management To Meet Tight Deadlines



# Telecom solutions provider rely on PrivX to manage third-party IT access

The customer is one of the largest networking providers throughout the entire APAC region. The company suports residential and enterprise consumers across Asia with innovative solutions like a consumer product and mobile app that allows users to manage and configure their home wireless service from any device. It's a popular service used by many customers.

## Brief background

The customer turned to its third-party system integratorto help design, develop, manage and maintain their wireless network solution. Naturally, that means the third-party, as well as other vendors and partners, required access to key IT resources within the enterprise IT infrastructure. A privileged access management (PAM) solution seemed a logical fit, and it needed to offer access that is secure, fast and easy to manage. The partner suggested one of their favorite tools: PrivX, from SSH.COM, the lean cloud PAM solution.

## System passwords posed a security risk

Creating any sort of major consumer application often means bringing together a number of different partners. In this case, the customer would need to grant frequent IT access not only to the third party, but also to other software developers, network operators, and customer-facing operations teams, in order to complete the development process and support maintenance.

**Without a PAM solution, all those partners would directly log in to the customer's virtual servers using simple user accounts and passwords.**

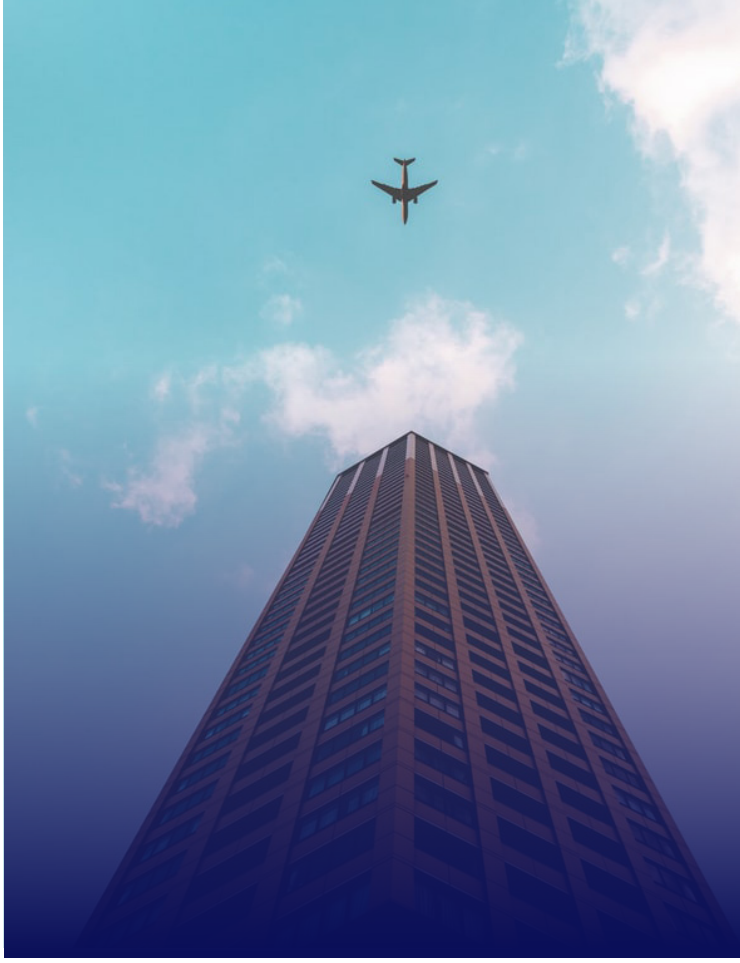
The company's IT infrastructure is composed mainly of Windows and Linux platforms built on Microsoft Azure. Without a PAM solution, all those partners would directly log in to the customer's virtual servers using simple user accounts and passwords.

This sort of direct access created a few problems: one, server passwords can easily be shared among team members, and shared passwords are a significant security risk. Secondly, frequent password sharing cannot be easily monitored, meaning the customer did not know who had privileged access to their sensitive IT infrastructure, including the ability to make changes.

Given the number of different parties involved in the development of the customer's solution and the potential that a privileged account could fall into the wrong hands, it was clear that the customer needed a stronger secure access solution.

Additional pressure came in the form of a tight implementation deadline: developers would need to develop and launch the solution within a window of just a few months.

Fortunately, the partner had the answer



## PrivX: The easy choice

The partner recommended PrivX, the lean PAM solution from SSH.COM

Access through PrivX can offer one-click access into any IT environment, drastically simplifying the privileged access workflow

The partner had already had positive experiences using PrivX to manage access to its other client environments. They appreciated its reputation for security, and the fact that access through PrivX can offer one-click access into any IT environment, drastically simplifying the privileged access workflow.

PrivX would be the perfect solution for the customer for several reasons.

First, PrivX enables rapid deployment. It integrates with corporate directories like Active Directory, LDAP and OpenID (OIDC), or with identity management software (IAM). In this case, the customer admin:

1. Integrated PrivX with Active Directory.
2. Used PrivX to define the roles and mapped the identities/authorizations to the roles that match the required level of access. The admin simply reuses the identities and their authorizations that have already been de- fined in Active Directory without duplicating any information.

It's a simple one-time process.

## PrivX stays in sync with any updates in the identities or their authorizations

After that, PrivX stays in sync with any updates in the identities or their authorizations so that roles and their entitlements are always up to date. That's Joiners, Movers and Leavers process made easy.

PrivX automatically discovered the cloud hosts from the customer environment. The admin deployed the roles to the cloud environment using orchestration and automation tools, like Ansible or Chef, and mapped the roles to the user accounts on the hosts.

This was another process that needed to be done only once. After this stage, PrivX automatically updates with any changes in the cloud estate, for example, as hosts are spun up or down.

PrivX also delivered the best value of any PAM solution, since it was up and running within the customer's environment in just three days, ensuring development could stay on deadline.

## PrivX eliminated the risk of password sharing for one simple reason – the developers or admins no longer handle privileged passwords or other permanent credentials.

The customer felt that other PAM tools were either too expensive or would take too much time to offer any benefits

PrivX eliminated the risk of password sharing for one simple reason – the developers or admins no longer handle privileged passwords or other permanent credentials, such as SSH keys, or handle any secrets.

Instead, when establishing an SSH or RDP connection, PrivX relies instead on ephemeral certificates, which are short-lived access credentials that exist for only as long as they are needed to authenticate and authorize privileged connections.

Ephemeral certificates automatically expire and are one-time use only, meaning there is no password to share or misplace. Furthermore, there is no need to worry about revoking access when a third party leaves the project.

For software developers, this meant that they log in to PrivX using single sign-on (SSO), and then they have access to only their available servers – and nothing more.

PrivX also offers added security through features like two-factor authentication, which are available at no extra cost. Engineers logging into PrivX are also asked to type in a one-time token alongside their Active Directory password, which limits the chance that unauthorized users are able to access PrivX.

Role-based access also solved the risk of excessive access. The customer no longer had to worry about who had access to their most sensitive IT resources, since access could be provided or restricted based on the user's role within the organization with the right level of privilege for the task at hand.

Every session is audited and logged for accountability. Additionally, PrivX offers a session recording feature that provide advanced security. As a result, they can see when access was granted, identify the users who received access, and troubleshoot any problems that arise along the way.

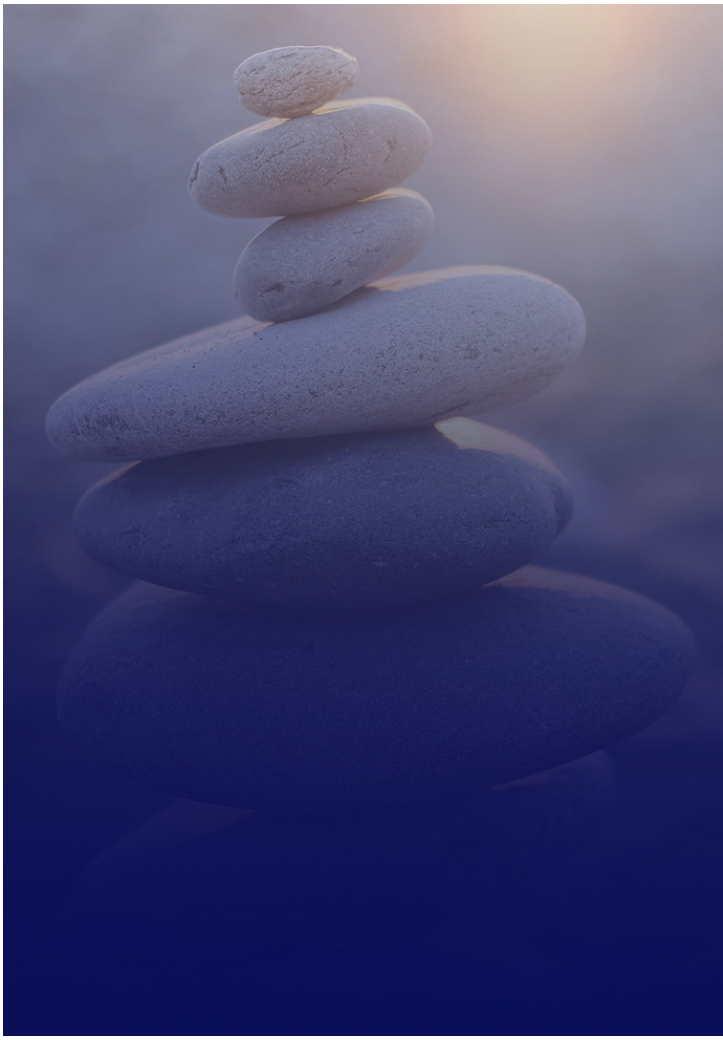
**PrivX can manage RDP and SSH access on both on-premises and cloud platforms such as Amazon Web Services, Microsoft Azure and Google Cloud. It's the ideal solution for hybrid or multi-cloud environments.**

Importantly, PrivX is purpose built for the cloud, making it the perfect solution for the customer's Azure-based IT infrastructure. PrivX can manage RDP and SSH access on both on-premises and cloud platforms such as Amazon Web Services, Microsoft Azure and Google Cloud. It's the ideal solution for hybrid or multi-cloud environments.

## Easier collaboration makes for a better product

PrivX improved collaboration between the customer and its team of partners and vendors. Faster secure access makes for easier work, and a stronger end- product.

It's also no surprise then that the partner has deployed PrivX within their own environment. The partner relies on PrivX to grant secure access to tools like Microsoft Teams connectors, which they use each day to design and develop product features based on Microsoft Teams.
PrivX ultimately makes life easier for both IT admins who need to ensure secure access to sensitive IT resources, as well as developers who need to move quickly even in environments that require extra security steps.





SSH.COM


## 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