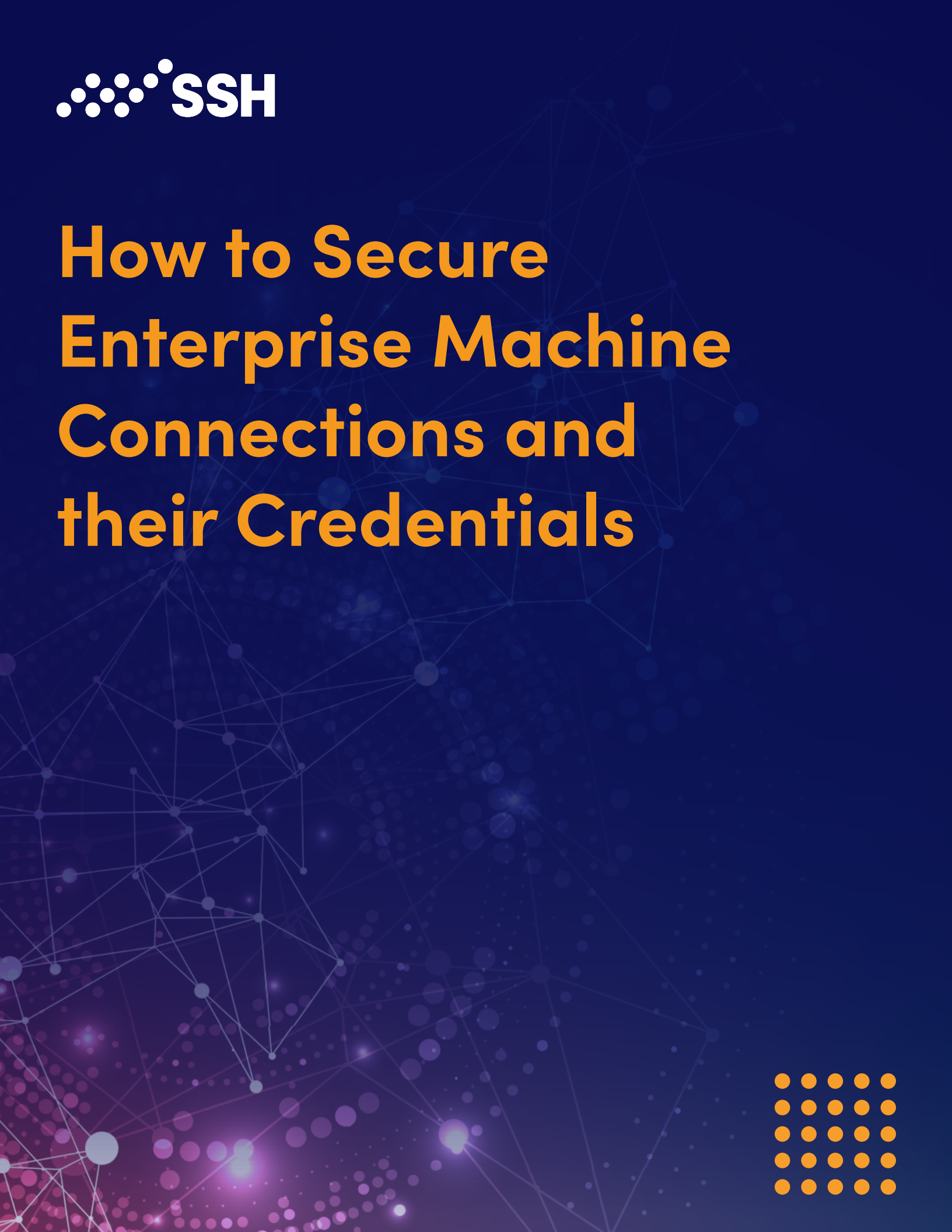
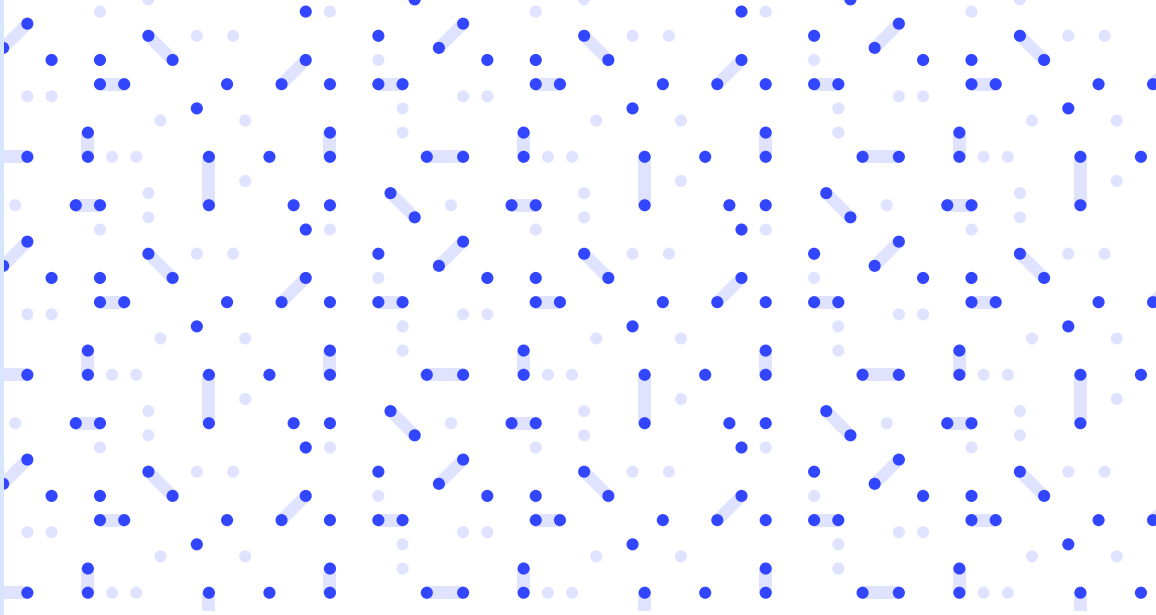
SSH

How to Secure Enterprise Machine Connections and their Credentials



Index



Introduction

We humans like to believe that we're in total control of the technology we create and use. But within complex IT infrastructures and cybersecurity systems, many events and activities are orchestrated, controlled, and managed by machines and machines only.

Many enterprises overlook the activity occurring between these machines, where there is often no human involvement, and largely ignore the credentials machines share with each other. But like passwords and other access credentials, machine credentials can be compromised and used to gain access to proprietary databases, applications, or server infrastructures. Compromised machine credentials can even bypass existing security governance solutions put in place by the enterprise.

The higher the number of machine-to-machine (M2M) connections existing in your network, the more machine credentials to be managed — and the greater the risks associated with their mismanagement.

So why do so many businesses overlook these critical sources of vulnerability?

In this white paper, we will explore how and why machine credentials are being neglected, the risks associated with unmanaged machine credentials, and the ways enterprises can solve the machine credential problem.

What are Machine Credentials and M2M connections?

Machine-to-machine access credentials allow machines to gain instantaneous access, when necessary. Examples of machine credentials include certificates, APIs, and SSH keys. M2M credentials are generated by machines, not humans — and they often never even pass through human hands.

At its core, a network is essentially a web of machine connections. Machine credentials are used for connecting machines to machines, as opposed to connecting humans and machines. Every one of these connections requires instant authorization in order to perform its task. In an ideal security environment, M2M credentials are managed and secured by automated tools, ensuring that they are never exposed to end-users.

M2M connections are all around us. Examples of machine-to-machine connections include:

- **Application to application connections (A2A):**
  Machines can send and receive APIs, and authenticate them using machine secrets. This forms connections that allow applications to communicate. For instance, enabling an individual to open a banking app on their phone, then open the app on their computer and be automatically logged in.
- **File transfers:**
  Machine-to-machine file transfers help disparate servers share critical information without humans reading this secret data. However, there is often a lack of consistent security mechanisms in place to appropriately secure file transfers, and in some cases there may be no authentication or encryption at all.
- **Application-to-application scheduled batch jobs:**
  A batch job refers to a scheduled program created to run multiple jobs simultaneously without requiring human interference. Batch applications can be used to read and write files, create reports, and clean up data by scanning and editing files.

To ensure comprehensive cybersecurity, businesses must adopt and enforce controls, regulations, and rules to preside over machine-to-machine credentials. If appropriate security measures are not adopted to protect machine-to-machine credentials, they are at risk of being intercepted by malicious actors or otherwise compromised.

The Machine Credential Management Problem

Many businesses have invested considerably in privileged access management (PAM) solutions that ensure passwords are strictly governed, organized, and controlled. However, many standard PAM solutions fail to properly manage machine credentials. In fact, 80% of SSH keys, a common type of machine credential, go undetected by traditional PAM tools.

The crux of the machine credential management problem is that PAM solutions are simply not equipped to provide comprehensive M2M credential management.

In the 2021 Magic Quadrant for Privileged Access Management Report, Gartner estimates that 70% of organizations this year will start implementing practices associated with PAM across all their use cases. That means companies will likely continue using PAM solutions to manage all their use cases — even the ones that don't comprehensively cover M2M credential management.

The sobering news is that managing your organization's privileged passwords doesn't ensure the comprehensive governance of your machine-to-machine credentials. In the worst case scenario, enterprises may only have 10% of their access credentials managed, even when using PAM. To make matters worse, many company leaders don't even realize that machine credentials like SSH keys are access credentials, leading to further complacency with M2M credential management.

Why is it Important to Protect Machine Credentials?

The importance of effectively managing, securing, and protecting machine-to-machine credentials cannot be overstated. Here are just some of the many reasons why it is essential that your enterprise appropriately manage and secure its M2M connections and machine credentials:

Increased vulnerability

When the location and use of machine credentials aren't tracked, they become vulnerabilities that hackers or other malicious actors can exploit. Malicious actors can then use these exploited machine credentials to access critical enterprise systems and their proprietary data.

Compliance issues

Machine credentials are an IT audit failure point and their ungoverned use breaches multiple regulations. As a result, mismanaged machine-to-machine credentials could result in fines and other regulatory consequences.

Accumulation of credentials and related issues

The scale of the machine credential mismanagement problems represents a key issue in and of itself. Because M2M credentials occur every time a new machine-to-machine connection is made, they accumulate exponentially over the years — often growing into the tens of thousands. Based on SSH experience, machine-to-machine credentials outnumber passwords 10 to 1.

Accessing a web of connections

Networks are made up of many M2M connections, all of which use machine-field authentication to give and receive access. In some cases, hackers can piggyback off compromised machine connections to access other existing M2M credentials. This makes it easy for them to hop from one non-important server to your critical infrastructure.

Undetected faults and damage

Perhaps the most important reason to protect and maintain visibility over M2M credentials is the fact that a stolen, shared, or otherwise compromised machine credential can easily go undetected. When machine credentials are stolen and reused, the existing security controls may perceive the access as legitimate — causing a hacker's malicious access to effectively bypass existing security systems.

Outdated credentials

Even if credentials like SSH keys don't expire by default, their security standards are being upgraded over the years. An automated machine connection that has been running for years without any updates might be running vulnerable protocol versions that increase the likelihood of a breach or other misuse.

Why Are So Many Companies Failing to Address Machine Credentials?

Despite the importance of securing and protecting machine-to-machine credentials, many enterprises fail to properly address the machine credential management problem.

Why is this the case?

Lack of knowledge of what machine credentials are

Many machine credentials aren't recognized as access credentials. There are many kinds of M2M connections and credentials, each serving a unique purpose and providing differing levels of access. But since these connections typically occur behind the scenes, without human intervention, it's easy for people to forget about them — or even fail to realize they exist in the first place.

Lack of understanding of how to interact with machine connections

Incorrectly tampering with a critical M2M credential could be detrimental to your network, potentially compromising hundreds of other system functions such as files, transmissions, and application APIs. Often, when people try to implement M2M credential management, fear of creating problems and disrupting critical connections hampers their efforts.

Lack of education regarding the security of machine credentials

M2M credentials can be highly complex in nature. SSH keys, for example, consist of lengthy strings of code and have a default key length of 1024 bits — making them virtually unbreakable in the event of a brute force attack. This complexity has led many people to believe that M2M credentials are significantly less vulnerable to threats. In fact, the opposite is true: because these credentials are mismanaged, their strength alone won't help: they are more susceptible to cyberattacks, especially if they are easy to harvest.

Lack of accountability for properly securing machine connections

The reasons outlined above provide some insight into why some organizations struggle to secure their machine-to-machine credentials. But when individuals and teams within a company don't take accountability for their partial or complete lack of management, nothing changes. This can result in thousands of M2M credentials accumulating with no oversight. In addition to the risk of breach and compromise, unmanaged machine credentials can cause a lack of reporting that prevents teams from identifying threats and their sources.

Machine Credential Management Best Practices

SSH wants to empower every organization to efficiently and sustainably manage their enterprise machine credentials. To that end, we've established four key best practices:

1 Identify where all critical assets are located

This will help you keep credentials organized, so they can be managed more effectively. Identifying critical assets also helps you understand the number of known and potential vulnerabilities associated with M2M credentials.

2 Identify who has access privileges, and how they access the assets

It's essential that enterprises have visibility over which machines can access, modify, or share important files and documents. Companies should also identify which instances human-run accounts can manage and the appropriate instances for machine accounts.

3 Enforce controls on how machine credentials are used, to ensure they are never exposed to human end-users

When people interfere with M2M credentials, even with appropriate training and good intentions, the risk of human error increases. Using a specialist automated tool to manage machine credentials will support enterprise processes, and help you ensure that your credentials adhere to the relevant compliance requirements. This will also reduce overhead and human involvement.

4 Audit, track and optionally record sessions

The use of machine credentials should be logged and audited just like, for the most part, interactive sessions are. A solid trail of activities will help demonstrate compliance and provide important insight if something goes wrong. Session recording is a great feature for monitoring the most critical connections.

For many enterprises, following even these three steps can feel like an insurmountable challenge. Your IT environment may have accumulated tens of thousands of M2M credentials over the years, scattered throughout your infrastructure.

Since our inception, SSH has been pioneering the evolution of cybersecurity. We are always looking for new and better ways of overcoming the most pressing cybersecurity challenges of today and tomorrow, including machine credential management. That's why we support two ways to manage your machine connection credentials.

Two Machine Credential Management Solutions

SSH offers two ways for organizations to approach the challenge of managing credential management — both of which can be leveraged through the SSH Universal Key Manager Zero Trust (UKM Zero Trust).

The first option is the traditional approach: leveraging a specialist solution that enables you to follow M2M credential management best practices. Specialist tools like UKM Zero Trust can locate all machine credentials automatically, remove the ones that shouldn't exist, and store the necessary credentials in an inventory and database that securely rotates them to keep them strong. Features of UKM Zero Trust that help you manage M2M credentials include:

- Assessment of M2M connection risks across your entire IT ecosystem
- Automatic handling of M2M credential lifecycles
- Identifying and removing problematic M2M credentials

The second option is to move to an ephemeral certificate approach. This innovative approach replaces machine credentials with ephemeral certificates that grant just-in-time access. After granting access, the certificates simply cease to exist — eliminating the problem of risky machine credentials altogether.

You Can Have Both: Machine Credential Management Now and Forever

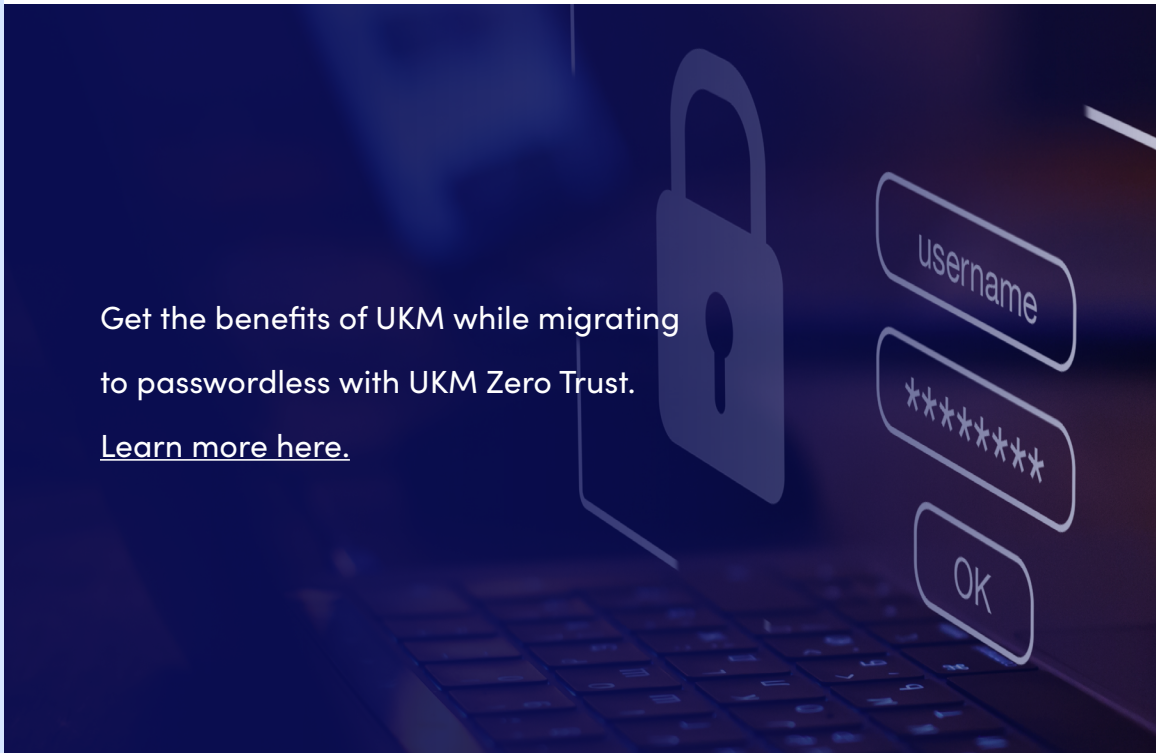
UKM Zero Trust enables you to move to a credential-less approach while maintaining your current M2M connections, helping you migrate to an environment that supports:

- Ephemeral, short-lived privileged access tickets
- Automatic expiration of M2M connections
- Complete removal of all credentials and their related vulnerabilities, including those associated with keys and passwords
- Radical reduction in managing and rotating machine credentials for operational efficiency and huge cost savings
- Auditing, tracking and recording M2M connections for forensics, compliance and policy enforcement

Which solution is right for you? The answer will vary depending on the scale of your problem. Ask yourself: would you rather use UKM Zero Trust to automatically rotate your machine credentials, or replace them with temporary access certificates?

Just-in-time, ephemeral certificates are the future of cybersecurity. In fact, Gartner has placed passwordless authentication at the center of its Impact Radar for 2022. What applies to passwords, applies to other credentials as well.

To ensure a future-proof cybersecurity approach, use UKM Zero Trust to begin migrating to a passwordless and keyless environment at a pace that best suits your enterprise. UKM Zero Trust allows you to manage, store, and automatically rotate your existing credentials while simultaneously introducing new credentials as ephemeral certificates. This capability enables you to gradually replace existing credentials with ephemeral certificates for a more efficient, secure, and enduring network of machine-to-machine credentials.



Get the benefits of UKM while migrating to passwordless with UKM Zero Trust.

Learn more here.

SSH

We'd love to hear from you

Get in touch
with our experts
around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH COMMUNICATIONS
SECURITY CORPORATION

Karvaamokuja 2b, Suite 600

FI-00380 Helsinki

Finland

+358 20 500 7000

info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.

434 W 33rd Street, Suite 842

New York, NY, 10001

USA

Tel: +1 212 319 3191

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

Let’s get to know each other

Want to find out more about how we safeguard mission-critical data in transit, in use, and at rest for leading organizations around the world? We’d love to hear from you.

Request a Demo