LEARNING MADE EASY

Venafi Special Edition

TLS Machine Identity Management

for dummies®
A Wiley Brand

Learn what machine identities are

Understand machine identity risks

Proactively manage machine identities

Brought to you by

VENAFI®

About Venafi

Venafi is the cybersecurity market leader in and the inventor of machine identity management, securing machine-to-machine connections and communications. Venafi protects machine identity types by orchestrating cryptographic keys and digital certificates for SSL/TLS, SSH, code signing, mobile, and IoT. Venafi provides global visibility of machine identities and the risks associated with them for the extended enterprise — on-premises, mobile, virtual, cloud, and IoT — at machine speed and scale. Venafi puts this intelligence into action with automated remediation that reduces the security and availability risks connected with weak or compromised machine identities while safeguarding the flow of information to trusted machines and preventing communication with machines that aren't trusted.

With more than 30 patents, Venafi delivers innovative solutions for the world's most demanding and security-conscious Global 5000 organizations and government agencies.

For more information, visit **http://venafi.com**.

TLS Machine Identity Management

Venafi Special Edition

for dummies®
A Wiley Brand

TLS Machine Identity Management For Dummies ®, Venafi Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-80961-6 (pbk); ISBN: 978-1-119-80962-3 (ebk). Some blank pages in the print version may not be included in the ePDF version.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager and Development Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Ashley Coffey

Business Development Representative: Molly Daugherty

Production Editor: Mohammed Zafar Ali

Table of Contents

Introduction

Businesses spend billions of dollars each year on identity and access management (IAM), but almost all this money is spent on managing the digital identities — usernames and passwords — of humans. On the other hand, businesses spend almost nothing on managing machine identities, even though the entire digital economy hinges on secure communications between machines. As businesses transform their operations to be primarily digital — called *digital transformation* — the need for secure machine identities has become even more critical.

About This Book

Welcome to *TLS Machine Identity Management For Dummies*, Venafi Special Edition. This book helps you understand where machine identities are used in your network and what you need to do to keep these identities up-to-date and protected. You discover how machine identities contribute to your security strategy and what you need to do to effectively manage the growing number of machine identities that your infrastructure requires. You discover why you should make managing machine identities a priority in your organization.

A successful machine identity management program requires visibility, intelligence, and automation across all machine identity management types, including Transport Layer Security (TLS) keys and certificates, Secure Shell (SSH) keys, and code signing keys and certificates. While this book helps you understand the challenges of managing TLS machine identities specifically, your organization may want to investigate a solution that helps you manage all types of critical machine identities.

Foolish Assumptions

In writing this book, we knew that the information would be useful to many people, but we have to admit that we made a few assumptions about who we think you are. We assume that

- You want to learn more about the weakest areas of your organization's security program.
- You're a public key infrastructure (PKI) administrator or a system administrator responsible for properly managing your organization's TLS encryption assets. Or, you manage this function within your organization's security or operations group.
- You're somewhat familiar with encryption and security.
- You want to discover an easy, effective, and direct way to manage and protect your machine identities.

Icons Used in This Book

We occasionally use special icons to focus attention on important items. Here's what you'll find in this book:


REMEMBER

The Remember icon highlights important facts about machine identities and their effective management. So sip your coffee and read on.


TIP

The Tip icon gives you the best ways to lower machine identity risks. This content helps you get the most out of your management efforts.


WARNING

The Warning icon flags risky situations that, if not dealt with, can leave your organization more vulnerable to cybercriminal attacks. So take note! The information contained in this icon can help you prioritize your TLS machine identity management tasks.


TECHNICAL STUFF

The Technical Stuff icon notes when the book goes a little deeper into the nitty gritty of TLS machine identity management. You don't need this information to understand the rest of the book, but this gives the techie types more details.

IN THIS CHAPTER

- Explaining Transport Layer Security (TLS) machine identities
- Looking into how machine identities are used

Chapter 1
Understanding TLS Machine Identities and How to Manage Them

As businesses become primarily digital, an ever-increasing number of machines are required to drive unprecedented improvements in business efficiency, productivity, agility, and speed. But machines don't work in isolation. They need to be in constant communication with other machines. Before machines can communicate securely, they need some way to determine if the other machine is trustworthy.

When online, humans rely on usernames and passwords to identify and authenticate themselves to machines. Machines also have digital identities, but they don't rely on usernames and passwords for authentication. Instead, they rely on cryptographic keys and digital certificates that serve as machine identities.

At the beginning of every secure communication, machines check these digital identities to establish trust, authenticate other machines, and encrypt communication. In this chapter, you discover how machines are used to enable all kinds of digital communications and how these machine identities work — and you also see why they need to be managed and protected.

Defining Transport Layer Security (TLS) Machine Identities

Transport Layer Security (TLS) is a cryptographic protocol that provides end-to-end communications security over digital connections. This widely adopted protocol is used to secure Internet communications and online transactions and is designed to prevent eavesdropping, tampering, and message forgery for machine-to-machine communications.

To understand TLS machine identity management, you need to know a little more about the security assets that make up machine identities: cryptographic keys and digital certificates.

Cryptographic keys

Public key cryptography (or *asymmetric cryptography*) is used to secure machine communications. Matched pairs of asymmetric numbers are used as "keys" (one public and one private) that authenticate, encrypt, and decrypt a digital exchange. These key pairs are used when a machine or person initiates secure, private communications.

A public key can be given to anyone, but the private key must be kept secret by its owner. Public keys can be used by any party that receives them to encrypt data and validate digital signatures. Private keys are only used by their owners to decrypt information (which was encrypted with the public key) or to digitally sign information to prove that it came from the owner of the private key.

Public key cryptography relies on key length and cryptographic algorithms for security. Key length is the length of a key in bits — it's similar to the number of characters in a password. The cryptographic algorithm is the group of mathematical equations used to securely generate and apply key pairs for authentication, encryption, and decryption. Because public key cryptography serves as the basis for secure communications on the Internet, and because most organizations don't manage these critical security assets well, cybercriminals devote a lot of effort to trying to compromise keys and certificates.

Digital certificates

Whenever you want to communicate securely with another party online, you must make sure you're using that party's public key. To do this, you use a *digital certificate* to associate the public key with its owner. The owner is usually a machine (the definition of machine here is pretty elastic and can include software or a domain such as a website) or, less commonly, a person. A *digital certificate* is also called a *public key certificate.* The majority of TLS certificates used today are based on the international standard X.509.

People rely on X.509 digital certificates because they're issued by a trusted source called a Certificate Authority (CA) and include several types of identifying information:

- A public key
- A unique name for the machine (for example, `www.company.com`) or the person who owns the certificate
- The name of the organization that issued the certificate (the issuing CA)
- An issue date and expiration date, after which the certificate can no longer be used
- The CA's digital signature

In addition to this information, every certificate includes information about how it should be used. Together, the information in a certificate serves as a machine identity. This identity is checked before a machine can access servers or other machines.

Understanding How TLS Machine Identities Are Used

Machines use encrypted connections to establish trust in all kinds of digital transactions. To do this, machines use digital certificates and cryptographic keys (discussed in the earlier section "Defining Transport Layer Security (TLS) Machine Identities") to create machine identities that validate the legitimacy of both communicating machines. To better understand how this works, the following list gives you some of the ways TLS machine identities are used to support vital business functions:

- **Securing web transactions with HTTPS:** Machine identities, such as TLS or Secure Sockets Layer (SSL) certificates, are critical to the security of web transactions, such as online banking and e-commerce. These certificates enable an encrypted connection between a web browser and web server, load balancer, application server, or next-generation firewall.


WARNING

If the certificates used to secure HTTPS aren't properly managed, cybercriminals can gain access to these critical machine identities. After this happens, cybercriminals can eavesdrop on encrypted traffic or impersonate a trusted system.

- **Securing cloud-native environments:** Development Operations (DevOps) teams are focused on speeding up the delivery of products and services. These results are made possible by cloud-first strategies where developers use cloud-based, self-contained runtime environments, known as *containers,* to run individual modules called *microservices.*


REMEMBER

Each microservice and container should have a certificate to identify and authenticate it and to support encryption. These certificates serve as valid machine identities that allow containers to communicate securely with other containers, microservices, and cloud-native applications. Because these machines are spun up and down several times a day, they may require temporary certificates. These certificates exist only for the period during which access is required, and they automatically expire when they're no longer needed.


WARNING

Issuing keys and certificates manually for containers and cloud-native applications can slow the delivery of IT services. The resulting frustration can cause developers to avoid encryption altogether or to skimp on key and certificate security. When this happens, it exposes your organization to unnecessary security vulnerabilities, and it can also insert error-prone, manual steps into an increasingly automated DevOps environment.

- **Securing communication on connected IoT and mobile devices:** With increasing numbers of IoT devices and remote and mobile workers, digital certificates have become a vital element of mobile security; they provide the foundation for authenticating mobile devices that access enterprise networks. Also, mobile device certificates are increasingly

being used for remote enterprise access that uses TLS and Internet Protocol Security Virtual Private Networks (IPsec VPNs). In addition, mobile access to Internet of Things (IoT) devices on enterprise networks relies on certificates for authentication.

WARNING

Security for IoT and mobile devices is frequently owned by different teams from those that manage TLS keys and certificates — and both teams may have different objectives. Without central oversight, consistent management for mobile and IoT machine identity securities is nearly impossible. Two common examples of inconsistent TLS machine identity management for mobile and IoT are the use of a duplicated certificate on multiple devices and the on-going use of unrevoked certificates issued to past employees. Both are poor practices that allow certificates to be misused.

SEEING TLS MACHINE IDENTITIES IN USE

Here's a basic example of how TLS machine identities are used every day: When you attempt to connect to a website from your phone or laptop, the web server provides its machine identity (digital certificate) so you can be sure you're connecting to the correct site. This verification is particularly important if you're going to complete an online transaction, such as making a purchase or completing a banking transaction. Of course, this step is just one in a complex string of machine-to-machine communications needed to complete the transaction. Each subsequent step also requires each of the machines involved to be identified and authenticated, but this example helps illustrate why managing machine identities is vital to the security of almost every form of digital communication.

IN THIS CHAPTER

- Recognizing the cloud computing machine identity crisis
- Generating machine identities in DevOps
- Seeing the impact of IoT and mobile devices
- Outsourcing to smart machines and robotic processes

Chapter 2
Managing the Rapid Growth of Machines

As the world moves toward doing more business online, most large organizations respond with supporting technologies that help digitally transform their operations. This digital transformation also drives an increase in the number of new machines that are critical to business success. To operate securely, all these systems, applications, and websites need to have valid Transport Layer Security (TLS) machine identities.

As a result of digital transformation, organizations that once managed thousands of machines just a few years ago are now trying to manage hundreds of thousands or even millions. These numbers are expected to grow by at least 50 percent per year within the next several years. As the number of machines in businesses increases, so does the number of corresponding machine identities. In turn, this exponential growth increases the complexity of managing TLS machine identities. Two main factors contribute to the growth of machines:

- **Shorter machine identity life cycles:** Machine identities used to have a life span of over five years. But in 2020, that life span was lowered to one year, and we expect that to shrink to six or three months. When your certificate life cycle

is cut by half, you need to manage twice as many certificates over the same time period. Without additional staffing or increased capabilities, such as automation, managing machine identities can quickly overwhelm your team.

- **Accelerated development:** To keep up with rapidly changing market conditions, organizations rely on fast and adaptable development environments. As developers update and enhance applications in smaller chunks, they require immediate access to an ever-growing number of machine identities — both in development and for live updates. To keep pace with their timelines, developers need highly automated access to machine identities that's built into their development frameworks.

Exponential growth in machine identities — coupled with the need to replace certificates more often — complicates the already complex challenge of maintaining effective, enterprise-wide machine identity management programs. Take a look at Figure 2-1. You can see that certificate life spans have shortened significantly over a 10-year period, increasing the time, effort, and cost of management.

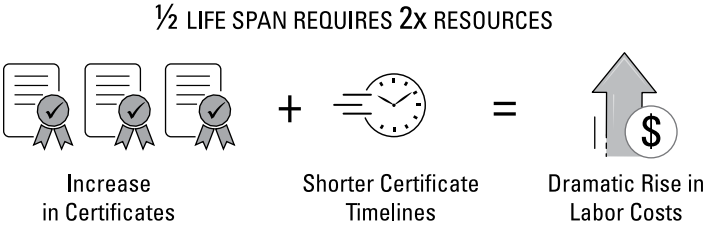

FIGURE 2-1: Shorter certificate life spans require more resources to manage.

This chapter outlines the key trends driving the rising number of TLS machine identities on enterprise networks.

Machine Identities in the Cloud

Cloud computing and virtualization have profoundly changed the definition of machines to include software that emulates physical servers. This shift in how IT networks are structured allows enterprises to run faster, improve network manageability, reduce maintenance, and quickly adjust resources to address fluctuations

in business demand. As businesses increase their reliance on machines, the number of machines is growing exponentially. Cloud services, containers, microservices, service meshes, and container orchestration platforms rely on machine identities for secure machine-to-machine communication, so machine identities need to be managed effectively to secure cloud workloads.

TECHNICAL STUFF

The average life span of a container is one day. A virtual machine is about 15 days. But a typical AWS Lambda container only lasts about an hour, which means that the number of cloud machine identities that needs to be issued, installed, and later decommissioned, is growing at an extraordinary rate.

Flexibility makes cloud computing valuable to businesses but also makes securing communication to, from, and within the cloud more complex. Without secure machine identities, you can't keep cloud communication private and secure.

Machine Identities in DevOps

DevOps teams support innovation by compartmentalizing applications to accelerate deployment of incremental changes to small segments of software. This has ushered in an entirely new definition of machines — each individual container and module within an application requires a unique identity so it can communicate securely. The scale of the new containers and microservices required for DevOps increases the number of variables in the already complex task of deploying and managing machine-to-machine communications in the cloud.

REMEMBER

An effective machine identity management program must provide developers the fastest, easiest way to get secure machine identities. Otherwise, they may be tempted to take shortcuts that undermine the effectiveness of machine identities. Building a machine identity management program from the ground up to support infrastructure-as-code and policy-as-code design patterns gives developers the speed they need to innovate — while staying safely within the policies established and supported by security and compliance teams.

Mobile and IoT Machine Identities

The use of Internet of Things (IoT) and mobile devices in enterprises is growing. Even though mobile devices have been around for a couple of decades, they interact with, store, and process substantial amounts of enterprise data. From industrial machinery and intelligent transportation systems to health monitoring and emergency notification systems, a broad range of IoT devices is already deployed by enterprises. Each device requires network connectivity so it can collect and transfer data. As a result, the volume of IoT communications is expected to more than double over the next five years.

WARNING

Organizations need to uniquely identify and authenticate each mobile device connecting to their networks, as well as the various applications on these devices. If left unmanaged, attackers can leverage a weak or vulnerable mobile machine identity to gain access to critical enterprise network services and assets and use them as part of a broader attack strategy.

IoT devices typically have limited CPU and storage capabilities so captured data must be transmitted to a central location to be collected, stored, and analyzed. Unless communications between IoT devices and extended enterprise networks are authenticated with valid, unique machine identities, the data can be stolen or compromised.

Smart Machines and Robotic Processes

The exponential increase in available processing power, storage capacity, and communication bandwidth makes it possible for critical tasks to be outsourced to smart machines — including Robotic Process Automation (RPA). These smart machines can solve increasingly complex problems and make decisions automatically without human intervention, so this technology is changing the way work is done.

Smart machines leverage artificial intelligence (AI) and machine learning. Securing smart machine identities is increasingly important because smart machines are often connected to critical infrastructure. Cybercriminals who gain access to identities for robots or smart machines can greatly change the outcome of automated tasks outsourced to smart machines.

IN THIS CHAPTER

- Dealing with outages from expired certificates
- Experiencing security breaches caused by rogue certificates
- Responding slowly to cryptographic incidents
- Compounding issues with rapid certificate growth
- Learning the risks of insufficient intelligence
- Summarizing the major consequences of the risks

Chapter 3
Recognizing TLS Machine Identity Management Risks

From service outages to security breaches, weak Transport Layer Security (TLS) machine identity management can wreak havoc with your business. In this chapter, you look at five of the most common TLS machine identity management risks and explore how these can impact your business.

Application Outages Caused by Expired Certificates

When certificates are issued, they're assigned an expiration date. If a certificate isn't replaced before it expires, it can trigger a certificate-related outage of the system it supports. That

unplanned outage and the associated downtime will continue until a new certificate is issued and installed. Without the correct intelligence, such as knowing where each certificate is installed and who controls access to that system, certificate-related outages are notoriously difficult to diagnose.

MANAGING CERTIFICATES WITH AUTOMATION

With the advance in digital robotics and expansion of operations technology, machine identities are multiplying at a faster rate than human identities. These identities are used for all manners of process and must be controlled. This proliferation drives the need for companies to implement automation to manage and secure machine identities. And Tim Callahan, Senior Vice President, Global Security, and Global Chief Information Security Officer, AFLAC, decided to do just that.

Callahan has led information security efforts for financial institutions for over two decades and regularly meets with other chief information security officers (CISOs) to share best practices. In his discussions, managing machine identities is consistently a topic of concern and a challenge in large and complex technological environments.

One of the first issues that comes up in these discussions is the impact an expiring certificate has on production and customer service for outward facing websites. And in a close second place is the issue of not knowing how many certificates are in the company and where they are.

To solve these problems, Callahan turned to Venafi. Venafi helps discover the presence of all certificates and decipher their validity and security; it also manages them to ensure they don't bring down production due to expiration. AFLAC can keep track of the versions that are in its environment to ensure it doesn't have insecure certificates. Also, the insurance company can ensure that the proper certificates are used when programmers need to install a certificate.

With the Venafi platform, AFLAC has accomplished this feat of managing certificates in an automated fashion that enables self-service for its system administrators and developers. Authorized users can log in to get what they need, but security staff has visibility and control.

For more information on automation, head to Chapter 6.

WARNING

If a certificate is used on more than one system, such as on load balancers, its expiration can cause simultaneous outages on multiple systems. The consequences of certificate-related outages on critical infrastructure are so severe that they're the catalyst that forces organizations to re-evaluate the way they manage and secure machine identities.

Security Breaches Facilitated by Rogue Certificates

Most security controls trust digital communications that are authenticated by using machine identities. But when the private keys and certificates (we talk about these in Chapter 1) that serve as machine identities are compromised or forged, cybercriminals can use them to appear legitimate, which allows them to circumvent security controls. Cybercriminals also use stolen machine identities to gain privileged access to critical systems so they can move deeper into your network and stay hidden for extended periods of time.

In addition, cybercriminals know that most enterprise security controls blindly trust encrypted traffic, so they use encryption — such as HTTPS connections — to hide attacks, evade detection, and bypass critical security controls. This is one key reason why most network attacks use HTTPS.

WARNING

Although the details of most breaches aren't made public, many of the largest data breaches exhibit key symptoms of attacks that leverage machine identities, such as abuse of privileged access, pivoting between systems via trusted access, and persistence for long periods of time on the network.

Slow Incident Response Caused by Lack of Crypto-Agility

To remain agile enough to avoid the certificate outages and the increasing number of threats to your machine identities, you must be prepared to respond quickly to cryptographic events. Many industry experts call this ability to respond quickly to

cryptographic vulnerabilities Crypto-Agility. For example, what would you do if one of your Certificate Authorities (CAs) was compromised and you needed to replace all the certificates from that CA quickly? Other large-scale security events that require timely response include

- The discovery of a machine identity using a vulnerable algorithm (for example, SHA-1)
- The exploitation of a cryptographic library bug (one of the most notable was Heartbleed)
- When a leading browser decides it will no longer trust certificates issued by one of your CAs

When you need to respond to any type of crypto event that affects machine identities, time is critical. The longer a security threat, outage, or breach continues, the greater the potential for serious damage.

Operational Inefficiencies Compounded by Rapid Certificate Growth

Organizations typically spend an average of four hours per year managing each digital certificate that serves as a machine identity. With thousands, or even hundreds of thousands, of machine identities, the resulting overhead can add up quickly — the resource drain is getting worse as certificate life spans get shorter and shorter. If your machine identity operations aren't running smoothly — which is the case in most organizations — the time required can escalate fast, especially when there's an outage or breach.

As more IT workloads move to the cloud, and as more IT services are containerized, manual machine identity creation and management simply can't keep up. In most cases, different groups of system administrators configure and manage machine identities for the systems they control. This makes it hard to consistently enforce security policies companywide and gather information rapidly when you're trying to respond to a security event.

When you add in other organizational factors, such as administrators who are unfamiliar with certificates or trust stores (where certificates from trusted CAs should be kept), it's easy to see why

organizations aren't able to respond quickly to security events that impact or misuse machine identities.

Negative Audit Findings Triggered by Insufficient Intelligence

Machine identities are increasingly subject to corporate, government, and industry policies and regulations, including several standards that focus specifically on cryptographic key and certificate management and security. Because most organizations don't have a strong machine identity management program, it's not unusual for auditors to discover that an organization is unable to monitor machine identities, identify vulnerabilities, or enforce policies — all of which create significant risks.

The most common audit findings include

- An incomplete inventory of machine identities
- The use of unauthorized CAs
- Expired certificates
- Unrestricted use of self-signed certificates

Auditors may also flag specific machine identity weaknesses, such as long lifetimes or weak key algorithms (we cover this in Chapter 4). If you're tasked with addressing these negative compliance findings and you don't have an automated machine identity management program in place, you face a lengthy, manual project.

Looking at the Consequences of Machine Identity Risks

When a machine identity is compromised and used in a cyberattack or expires unexpectedly and causes an outage, the negative consequences can be significant. And because the consequences of a breach or outage are interrelated, if you have a serious incident, you're likely to suffer from more than one repercussion:

- **Damaged reputation:** Outages and breaches can wreak havoc on the reliability and availability of your services.

The resulting erosion of customer and partner trust can damage your business's reputation and take months, or even years, to overcome.

- **Loss of revenue:** Downtime from an outage or a breach can negatively impact your bottom line through the loss of critical services or the loss of customer and partner confidence.
- **Costly remediation:** Slow incident response and inefficient machine identity operations make recovering from an unplanned outage, security event, or negative audit finding a lengthy and costly process. The longer it takes to fix the problem, the higher the risk of serious damage.
- **Higher resource costs:** All machine identity risks require time and resources to mitigate them. And if you're relying on manual tasks to manage machine identities, these resource costs will increase dramatically.
- **Loss of employment:** The cumulative impact of outages and attacks that use machine identities can be serious. Over the past years, several C-suite executives lost their jobs in the fallout from major breaches.

Are you concerned about the security risks connected with TLS certificate proliferation? many chief information Officers (CIOs) are. In fact, Venafi sponsored a study by market research firm Coleman Parkes that surveyed 550 CIOs from five countries: United States, United Kingdom, France, Germany, and Australia. The study results, shown in Figure 3-1, explore how CIOs are thinking about the risks connected with machine identities.

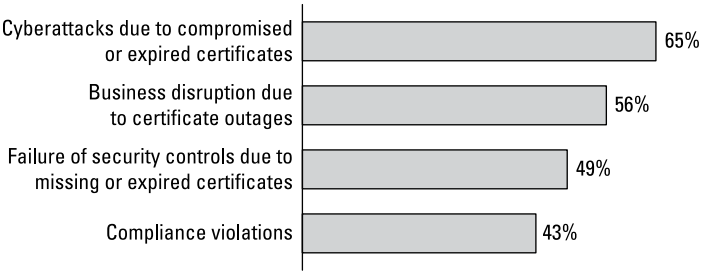

FIGURE 3-1: The machine identity risks on the minds of CIOs.

IN THIS CHAPTER

- Looking at organizational machine identity challenges
- Working around ineffective management tools

Chapter 4
Understanding TLS Machine Identity Management Challenges

Given the rapid rise in the number of new machines on enterprise networks and their critical nature, it's surprising that they're not better managed. Even in organizations that take cybersecurity seriously (and all companies should), the challenges inherent in traditional approaches to machine identity management make it difficult to implement and maintain.

In this chapter, you discover the challenges that organizations face in providing effective Transport Layer Security (TLS) machine identity management, and you look at the key reasons most security programs fall short in this crucial area.

Facing Organizational Challenges

Even though machine identities play a critical role in securing automated machine-to-machine communication, they're one of the least understood and weakly defended parts of companies' networks.

Distributed responsibility

One of the biggest challenges in TLS machine identity management programs is overcoming the way enterprises assign responsibility for the management and security of machine identities. In an ideal situation, your security team would automate the entire certificate life cycle with a self-service option that delivers policy-enforced, secure, and reliable key and certificate management. You would then require the different lines of business to rely on these services to minimize risk and comply with policies on the machines they control. However, what often happens is that each group that uses and maintains machine identities is left to determine how best to manage and protect them.

Because machines support so many different critical functions, nearly every business unit needs machine identities. This results in teams with different goals and skills deciding how they'll secure the machine identities they control. And because many administrators don't fully understand the impact of TLS machine identity management, they often treat it as an afterthought. This comparative lack of attention routinely leaves machine identities untracked, unmonitored, and unsecured.

To put TLS machine identity management into perspective, can you imagine what would happen to your organization's security if you allowed each business unit to decide how to manage usernames and passwords? Securing machine-to-machine communications is equally as important, requiring consistently enforced key and certificate security.

No global visibility and intelligence

Because most organizations don't have a complete and accurate inventory of their machine identities, they don't have ways to understand exactly how their machine identities are being used. This lack of enterprise-wide visibility prevents you from detecting irregular use of machine identities, which is an early indicator of a breach.

Also, with limited visibility and tracking, certificates can unexpectedly expire, triggering critical service outages (we discuss this topic in Chapter 2). If you don't have the information you need to manage the entire certificate life cycle and proactively

identify impending expiration dates, you can't create dependable, proactive certificate renewal processes.

To make matters worse, a lack of intelligence can make it nearly impossible for you to track certificate ownership. If an administrator who controls a machine identity resigns, is terminated, or is reassigned, certificate ownership is in limbo. When one of these orphaned certificates expires, you're left scrambling because you don't have enough information about the certificate to respond quickly.

Similarly, a lack of visibility into machine identities can restrict incident response following a security event. Often, your security teams won't have enough information to assess the role of machine identities in a breach. The time it takes to collect this intelligence causes delays in the incident response process. And in the aftermath of a security event, most security teams don't think about the need to rotate keys and certificates to prevent further exposure.

WARNING

If you don't rotate keys after a breach, attackers with compromised keys and certificates will continue to have access to your network devices and services. Of course, your organization would never accept limited visibility and weak management of usernames and passwords, yet most organizations accept a lack of visibility into machine identities, which often control high levels of privileged access.

Continuous development cycles

DevOps teams are often among the largest consumers of machine identities in many of today's businesses. To meet aggressive development demands, these teams may need to spin up and tear down machine identities several times a day for containers or microservices. The sheer speed of these DevOps processes creates an alarming number of machine identities.

DevOps teams often operate independently of other enterprise teams, including Security. So it's difficult to enforce consistent security and management best practices for machine identities. Security teams are left out in the dark with no way to see how many machine identities are being created, where they're being used, and who's using them.

Lack of expertise

When your administrators need advice about machine identities they control, they don't have many experts that they can consult. Surprisingly, even in organizations with hundreds of thousands of machine identities, there are just a few encryption experts on staff who understand the intricacies of the machine identity life cycle. Without automation, these experts can't manage all the machine identities used across your enterprise.

To add insult to injury, the tools your organization uses to manage machine identities usually require in-depth know-how. This leaves your average system administrator using online search engines to figure out what to do.

Relying on Ineffective Management Tools

Just a few years ago, the number of machine identities in your organization was just a fraction of what you need today. Plus, earlier machine identities didn't need to be updated or changed as often as they do now, and machine identities weren't targeted as frequently by cybercriminals. But that's all changed. New risks have made the need to manage and protect machine identities far more urgent, but most organizations are still relying on the management tools they used years ago. We cover the problems with these tools in this section.

Manual tracking

Despite the automation of many IT functions, many organizations still use manual tracking methods to manage their machine identities. Like these organizations, you may have tried to build an inventory of keys and certificates on spreadsheets or by using shared Intranet databases. This approach may have been sufficient for a limited number of physical machines, but with the surging number of physical and virtual machines on enterprise networks, this manual approach isn't just error-prone; it's completely impractical.

If you're using a manual approach, you're probably tracking only a tiny fraction of the machine identities used for a subset of critical services. This leaves the majority of your machine identities,

including those that support important business functions, unmanaged and unprotected.

Home-grown scripts

When organizations try to automate manual machine identity processes, they often start by using custom software scripts. These programs rarely collect all the information necessary to effectively manage machine identities and rapidly become cumbersome and difficult to maintain. And when the script developer changes positions or leaves the company, you're left with a custom-built tool that's difficult or impossible to adjust or use.

Siloed management tools

Because manual tracking simply isn't feasible, a growing number of organizations are turning to siloed management tools, such as those provided by Certificate Authorities (CAs), to manage their certificates. Unfortunately, this approach also has severe limitations.

The information that siloed management tools delivers simply isn't enough to keep your machine identities protected. For example, CA dashboards may only let you manage certificates issued by that particular CA. Because virtually all enterprises use more than one CA, each CA dashboard only provides management for a limited set of certificates. As a result, it's difficult to prioritize security risks across all certificates or efficiently deploy limited IT and security resources to address those risks.

In addition, these siloed tools don't contain information about where certificates are installed, and without this most basic information, it's nearly impossible to quickly track down a certificate's location. Relying exclusively on these tools also makes it difficult to identify weaknesses or detect vulnerabilities either in the certificates or on the servers where they're installed. And what if someone in your organization decides to get a free or low-cost certificate from a CA that isn't authorized by your organization's certificate issuance policies? (This happens more often than you might think.)

IN THIS CHAPTER

- Getting visibility across all machine identities
- Knowing which types of machine identity intelligence you need

Chapter 5
Gathering Machine Identity Intelligence

Whether your organization is trying to prevent machine identity attacks or stop outages, there's a lot riding on the effectiveness of your machine identity management program. But to create an effective program, you need technology specifically designed to address the unique management and security challenges of machine identities.

This chapter helps you identify the types of intelligence you need to collect so you can reduce security risks, eliminate outages, and consistently enforce a wide range of machine identity policies.

Getting Visibility Across All Your Machine Identities

REMEMBER

Before you even begin a machine identity management program, you need an inventory of all the machine identities used across your enterprise. To successfully gather this information, keep in mind the dynamic nature of machine identities and the different types of data necessary to effectively manage them.

To build a successful machine identity management program, you need the following types of visibility:

- **Extensive, enterprise-wide discovery:** First and foremost, you need a comprehensive, up-to-date view of all your machine identities, including those on virtual, cloud, mobile, and IoT infrastructures. While you can discover server certificates via port scanning, you must also be able to locate client and trusted Certificate Authority (CA) certificates, which require discovery of files and/or configuration data. Ideally, your inventory should include partner, supplier, and customer machine identities to ensure that setting up encrypted communication with them is safe.
- **Central repository:** Any solution you implement should include a secure, central repository of machine identities to enable centralized access and comprehensive analysis.
- **Reporting and analytics:** Equip your security analysts and stakeholders with the information they need to rapidly identify machine identity anomalies and vulnerabilities through dashboards, reports, analytics, and alerts tailored to their roles and areas of expertise.

Collecting Critical Types of Machine Identity Intelligence

To gain the intelligence you need to enforce policies and detect machine identity anomalies and vulnerabilities, you need to be able to discover and collect information on the critical attributes of each of your machine identities:

- **Machine identity type:** To understand exactly how your machine identities are being used, make sure that you know the type of machine identity employed. For example, you need to identify whether Transport Layer Security (TLS) certificates contain usage flags for server, client, email encryption, and so on — each of these use cases has different risk profiles. Without this information, you won't be able to understand if a machine identity is being used inappropriately and, potentially, maliciously.

REMEMBER

- **Key strength:** Key length impacts key strength; the longer the key length, the more secure the key. Cybercriminals use *brute force* attacks that essentially try each possible key combination until they find one that can decrypt the data. So the shorter the key length, the easier it is for attackers to figure out the value of a private key.

  As more computational power becomes available to conduct brute force attacks, key strength requirements must evolve. Key lengths that are sufficient today may not be sufficient next month or year. You need information about key strength in order to find and replace weak keys and to provide evidence of compliance.

- **Cryptographic algorithms:** Asymmetric algorithms, such as Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), and Elliptical Curve Digital Signature Algorithm (ECDSA), serve as the foundation for machine identities. Advances in quantum computing make it imperative that you monitor the use of asymmetric algorithms. This information helps you rapidly assess the level of risk from new cryptographic threats and vulnerabilities.

- **Hash algorithms:** Weak hash algorithms on certificates make it more likely for attackers to forge CA signatures and create rogue certificates that can be used to impersonate legitimate systems. For example, successful collision attacks have been demonstrated on the SHA-1 hash algorithm since 2017. But many organizations still use this deprecated algorithm in their internal networks.

- **Length of validity:** The life span of external certificates (those used to secure HTTPS) is limited to one year — and that life span is likely to continue to shorten over time. But internal certificates (those that aren't public facing) may have indefinite life spans.

  Because most private keys for internal machine identities are stored in files on the systems that they identify, the longer their validity period, the more likely they can be used to compromise those systems.

  For example, if you don't revoke access to an administrator's private keys when the administrator is reassigned or terminated, the keys will remain active until the certificates expire, making shorter certificate life spans an important security control.

- **Issuing CA:** Ensuring that your certificates are issued by approved CAs is fundamental to TLS machine identity management. You need to be able to find certificates issued by unauthorized CAs as well as self-signed certificates. Because these certificates don't follow policy or certificate management best practices and often go unmonitored, they increase your risk of security breaches and outages. Plus, they limit your ability to quickly replace large numbers of certificates in response to a security event.

This information provides a basic machine identity inventory that can be retrieved from the keys and certificates that serve as machine identities. However, to effectively manage your machine identities, you also need additional intelligence beyond what you can retrieve from the keys and certificates themselves. That intelligence includes the following:

- **Location:** Up-to-date information about where a key or certificate is installed on every machine is essential to effective TLS machine identity management and is critical for incident response. Without location information, machine identity problems can be extremely difficult to diagnose and even harder to fix. Location information should include
  - The machine address
  - File location
  - Hardware Security Module (HSM), if applicable
- **Owner:** Machine identities exist across countless systems and different groups. Central public key infrastructure (PKI) and security teams rarely have the permissions necessary to manage these systems directly, and updates to machine identities often have to be performed locally. So, when a security vulnerability is detected, such as a weak algorithm, operational risk, or impending expiration, the PKI or security team needs to be able to rapidly contact the appropriate owner to solve the problem. On a broader scale, if a CA compromise occurs, the PKI or security team must immediately notify the owners of every system that uses certificates issued by that CA before replacement can begin.

- **Cipher strength:** Each machine that uses a machine identity is configured to use certain ciphers, such as Advanced Encryption Standard (AES). Weak ciphers undermine the strength of encryption and can facilitate compromises by cybercriminals.
- **Protocol versions:** New vulnerabilities are regularly found in TLS protocols. To reduce the chance of compromise, ensure that you're using only approved protocol versions.
- **Certificate life cycle:** When you have complete visibility across the entire certificate life cycle, including length of validity and expiration dates, you can set policies to issue renewal notifications to certificate owners before certificates expire. You can also automate the entire certificate life cycle and set policies that ensure orphaned or unsecure machine identities are rotated out of use at specified intervals.
- **Configuration:** Misconfigured servers, applications, or keystores may leave otherwise secure keys and certificates open to compromise.

After you've gathered intelligence for all machine identities, you can use it to identify machine identity vulnerabilities, anomalies, risks, and trends. When dealing with tens of thousands — or even millions — of machine identities, automated analytics, dashboards, reporting, and alerts are the only way to rapidly identify risks across both broad and specific machine populations. As part of these automated processes, analytics should be sent to security information and event management (SIEM), service mesh, and ticketing systems; and email alerts should be issued.

To highlight risks, reports must be able to collate critical data and translate it into actionable intelligence, and you need the flexibility to design specific reports for different audiences and deliver them on a regular schedule or on demand.


TIP

Machines and their machine identities support nearly every important business function. Business groups need machine identity intelligence for the systems they control so they can support security best practices and take rapid remedial action when needed.

IN THIS CHAPTER

- Improving TLS machine identity management with automation
- Integrating with a broader technology ecosystem
- Mitigating TLS machine identity management risks with automation

Chapter 6
Using Automation to Improve TLS Machine Identity Management

After you have access to comprehensive machine identity intelligence (which we cover in Chapter 5), you can identify machine identity vulnerabilities and risks. But if you attempt to address these risks and vulnerabilities by using manual methods, you'll quickly become frustrated and overwhelmed. Automating your management and security processes is the most effective way to build and maintain a successful Transport Layer Security (TLS) machine identity management program.

In this chapter, we identify the different types of automation that are necessary to build TLS machine identity management, and we help you explore how automation integrates machine identity intelligence with your technology ecosystem. We also show you how automating management mitigates the risks we talk about in Chapter 3.

Bolstering TLS Machine Identity Management with Automation

Automation allows you to orchestrate a set of rapid actions that can be focused on a single machine identity or an entire group of identities at machine speed. These actions can be scheduled in advance, or they can be triggered by a specific set of conditions. To maximize the benefits of automation, you need five key capabilities.

Life cycle automation

Using manual processes to deploy, install, rotate, and replace machine identities is inherently error-prone and resource intensive. You may find it difficult to manually track the progress of complex, multi-step processes across multiple systems. Another shortcoming of manual management is that it gives your administrators direct access to private keys, which increases the possibility of private key compromise.

TECHNICAL STUFF

To manually deploy a new certificate, an administrator must follow these steps:

1. **Generate a new key pair.**
2. **Generate a certificate signing request (CSR).**
3. **Submit the CSR to a Certificate Authority (CA).**
4. **Retrieve the issued certificate and CA certificate chain from the CA.**
5. **Install the certificate and CA chain.**
6. **Configure the application, and often restart the application.**

   The certificate and private key may also need to be installed on multiple systems if you're using clustering or load balancing.

TIP

But by automating the entire machine identity life cycle, you can reap the following benefits:

- Ensure that all tasks are performed consistently across the enterprise, no matter how many machine identities or how

many different uses of these machine identities are employed in your organization — this includes managing certificate requests, issuance, installation, validation, renewals, and replacements.

- Decommission machine identities quickly to prevent unused machine identities from being exploited by cybercriminals.
- Improve security by removing administrator access to keystores.
- Simplify the adoption of Hardware Security Modules (HSMs) to improve the protection of private keys on mission-critical systems.

Policy enforcement

Automation is a critical capability that makes it possible to consistently enforce your organization's corporate machine identity policies and applicable regulatory requirements. When you leave compliance in the hands of the various administrators who are responsible for the keys and certificates on the systems they control, the policy enforcement results will be inconsistent.

For the best results, automated policy enforcement should drive every aspect of your machine identities, including configuration, issuance, use, ownership, management, security, and decommissioning. With these capabilities, you can quickly and automatically revoke and replace any machine identities that don't conform to appropriate policies. Plus, you'll have the flexibility to enforce machine identity policies in a variety of ways: globally, by logical group, or by individual identity.


TIP

One way security teams can leverage automation to deliver secure machine identities is to deliver them through certificate-as-a-service. This approach allows your system administrators to easily manage the machine identities they control. And because security policies are automatically applied to machine identities issued through the service, your security team will know that corporate policies and industry regulations are being enforced.

Remediation

Automation gives you the agility you need to rapidly respond to critical security events such as a CA compromise or zero-day vulnerability in a cryptographic algorithm or library. For example, if

a large-scale security event occurs, automation is the only way you can quickly make bulk changes to all affected certificates, private keys, and CA certificate chains. Automation is also the fastest way to remediate more focused security events, such as replacing a compromised certificate that's used across multiple machines.

Validation

Because machine identities include a complex set of variables, determining whether they're properly installed and configured is difficult if you're using manual installation. Validating the installation and proper use of machine identities is complicated because they're stored and used across a diverse range of devices, applications, and containers. But without access to this information, you won't be able to tell whether any configuration changes you make will impact the security and operation of your machine identities.

REMEMBER

Automation can solve these problems by validating that every machine identity is installed properly and working correctly. Ongoing validation ensures that your machine identities continue to be effectively managed and secured. Validation is also useful when you're grappling with large-scale security events. For example, when responding to a CA compromise or vulnerable algorithm, you need to have an accurate assessment of the progress of machine identity replacement across the enterprise.

Continuous monitoring

Machine identity intelligence loses its value if it only represents a single point in time. Automating your intelligence gathering is the only way to continually monitor the security and health of your machine identities. Plus, when your intelligence is automatically updated, you can generate alerts when anomalies or vulnerabilities are detected.

Without continuous monitoring, it's easy to miss the changes that are common to machine identities:

- Rapid changes on cloud and virtual servers and the applications that run on them
- Software update failures that cause configurations to be rolled back, overwriting a new certificate with an old, potentially vulnerable, or expired certificate

- The deployment and use of certificates from an unauthorized CA
- Insecure development test certificates that are inadvertently rolled out to production

These examples are just a few of the millions of changes to machine identities that happen constantly, but they illustrate why you need comprehensive, continuous monitoring for every machine identity used in your organization.


TIP

When you've set up your TLS machine identity management program to continually capture the information you need, you can rely on that intelligence to drive automated actions. The more management and security processes that can be reliably automated, the more benefits you see — from fewer errors to a reduction in management resources and better security.

Integrating with Your Technology Ecosystem

Machine identities are used by nearly all the technology solutions that are deployed across your expanded network and security infrastructure. You need to be prepared to integrate and orchestrate machine identities across a multitude of enterprise IT systems.

Operating systems and applications

Enterprises rely on a broad range of operating systems (AIX, Red Hat, Solaris, Windows, and so on) and applications (Apache, WebSphere, IIS, and more) for their mission-critical operations. Each of these systems and applications has a machine identity that plays a fundamental role in the security of communications to and from these systems.

Access to machine identity intelligence allows you to automate key and CSR generation for certificates and CA certificate chain installation, validation, and renewal. Automating access to machine identities helps preserve the uptime and security of these important systems, and it's the most efficient way to encrypt both internal and external traffic.

DevOps frameworks and containers

DevOps platforms require the rapid creation and provisioning of machine identities to ensure secure computing and application deployment. If you automate the delivery and monitoring of machine identities in development environments, you can increase security while supporting the deployment of new servers, applications, and containers at machine speed.

MAJOR RETAIL DevOps PUSH AIDED BY AUTOMATED TLS MACHINE IDENTITY MANAGEMENT

A worldwide leading retailer adopted DevOps to benefit from the faster and continuous approach to software development. To prepare for this move, the IT organization took steps to facilitate DevOps practices, migrating to a continuous delivery platform to automate cloud deployments. In the process, it deployed a range of DevOps tools for developers but chose not to prioritize TLS machine identity management.

As a result, the retailer's InfoSec department, especially its public key infrastructure (PKI) team, struggled with certificate issuance and management in the faster DevOps infrastructure. The main problem was that its manual method of provisioning and managing certificates directly conflicted with DevOps processes. The developer and engineering teams needed a machine identity solution that would enable — not hinder — the rapid pace of agile development, and the security team needed to ensure that high security standards weren't being compromised.

Venafi automated the retailer's TLS certificate management processes, enabling policy-enforced provisioning and renewal, which integrated seamlessly with the retailer's DevOps tools, including Kubernetes, Terraform, and Chef. With the Venafi solution, developers no longer have to involve the PKI team to obtain or renew certificates and the PKI team doesn't have to be concerned about missing, expired, or vulnerable certificates that threaten the availability and security of the retailer's network.

Integrating TLS machine identity management with popular DevOps tools, like Kubernetes and Ansible, as well as core technologies like service meshes and containerization, gives you centralized management, policy enforcement, and visibility of DevOps machine identities. This allows developers to go fast without jeopardizing enterprise security programs and policies.

Load balancing

Load balancers have become a primary conduit through which organizations manage and process communications with customers, partners, and employees. Because load balancers frontend so many applications, they also host a large number of machine identities that represent each backend application. Due to the critical nature of the services load balancers handle and the scale of machine identities they host — sometimes more than 1,000 machine identities per load balancer — you can't easily collect intelligence or manage the life cycle of these machine identities without automation.

TLS inspection

TLS inspection devices provide critical visibility into TLS data streams. To do this, they must have access to the private keys for the thousands of systems on which they're monitoring traffic. To support TLS inspection at this scale, you need the ability to automatically and securely transfer and install private keys on TLS inspection devices.

HSMs

Most private keys are stored in files on the systems they secure. This makes them susceptible to compromise. To prevent these risks, you can use HSM solutions to generate, store, and access keys within the safe confines of a security-hardened appliance. Using HSMs also helps you simplify compliance because auditors understand their security benefits.


WARNING

However, adding HSMs can also increase management complexity because they add a layer between your systems and your private keys. You can avoid this complexity by integrating machine identity automation into your HSM processes.

Security information and event management

Integrating automated machine identity intelligence directly into security information and event management (SIEM) platforms allows your security teams to correlate machine identity intelligence with other security information. Integrating with Security Orchestration, Automation, and Response (SOAR) also helps improve your ability to swiftly detect and respond to attacks.

Future technologies for quantum computing, IoT, and RPA

It's important to protect your business today while preparing for the future. Integrating with hybrid quantum cryptography is a great first step. Plus, as your business digitally transforms to support newer Internet of Things (IoT) implementation and Robotic Process Automation (RPA), you'll need to bring high-speed, high-scale identity security to managing your machines and devices to complete the full circle of your Zero Trust efforts.

Other enterprise systems and services

In addition to the other systems we outline in this chapter, you also need the ability to integrate TLS machine identity management with other enterprise systems, such as identity management solutions, configuration management databases, reporting and analytics, ticketing systems, and change control. With these integrations, you can streamline operations and improve security.

Overcoming Machine Identity Risks with Automation

In Chapter 3, we outline the risks of weak TLS machine identity management. Intelligence-driven automation is the only approach that can address these, and many other, machine identity risks. To help avoid the impacts of these risks, follow these guidelines:

- **Avoid certificate-related outages** by eliminating manual errors and automating the entire certificate life cycle to ensure machine identities are renewed before they expire. Information on certificate location and ownership quickly targets renewal requests with automated escalations as needed.
- **Prevent breaches** by automating the collection of risk intelligence required to quickly identify and respond to machine identity vulnerabilities, weaknesses, or security events. Automated policy-enforcement and life cycle management ensure unused or old keys and certificates are decommissioned.
- **Accelerate incident response** by automating the identification of impacted keys and certificates as well as the actions needed to remediate large groups of machine identities, so you can dramatically increase the speed of your response to large-scale security events.
- **Streamline operations** by automating routine administrative tasks to eliminate manual, error-prone processes and reduce the expertise and resources needed to manage the growing number of machine identities.
- **Ensure compliance** by automating policy enforcement to improve audit readiness, offering automated validation of TLS machine identity management, and generating scheduled or on-demand compliance reports.

REMEMBER

Automation also makes it easy to implement role-based access controls that allow or block access to machine identities. Implementing change management and role-based access controls ensures you can effectively manage machine identities and demonstrate this control for audits.

IN THIS CHAPTER

- Learning the steps to an effective TLS machine identity management program
- Making your TLS machine identity management program scalable and adaptable
- Including the steps that eliminate outages and prevent breaches
- Delivering policy-enforced self-service as part of your program for improved security and operations

Chapter 7
Ten Steps to TLS Machine Identity Management

Secure communication between machines is essential to the success of every enterprise. But how do you keep the identities of your machines safe when their identities are added and changed every day? To build your own Transport Layer Security (TLS) machine identity management program, you need to take specific steps. We cover that process in this chapter, and together, these steps enable your organization to protect all the machine identities you're using today and position you to keep up with the growing number of machines your enterprise will need moving forward.

Follow the ten steps outlined in this chapter.

1. Locate All Your Machine Identities

Getting a list of all your machine identities and knowing where they're all installed, who owns them, and how they're used is the first step in effectively managing them. After your discovery is complete, you'll have visibility into your keys, certificates, and the machines on which they're installed as well as the rest of the metadata that makes up machine identities. This information is used to communicate trustworthiness, provide encryption, and protect machine-to-machine communication.

2. Set Up and Enforce Security Policies

To keep your machine identities safe, you need to set up corporate policies and best practices to govern these critical security assets. This helps you control every aspect of machine identities — issuance, use, ownership, management, security, and decommissioning. Enforcing policies also ensures that your machine identities comply with industry and government regulations.

REMEMBER

Defining certificate policies is important, but those policies won't improve security or compliance if you can't enforce them. Automating the enforcement of machine identity policies ensures that you're maximizing the security and availability of every machine identity your organization uses.

3. Continuously Gather Machine Identity Intelligence

Because the number and type of machines on your network are constantly changing, you need an ongoing program to update intelligence on your machine identities. Some of this intelligence is available within the machine identity itself, and some you need to gather from the conditions of its use and its environment. This information is critical to your ability to drive intelligent, automated actions in your TLS machine identity management program.

4. Automate the Machine Identity Life Cycle

Automating the entire machine identity life cycle — including the management of certificate requests, issuance, installation, renewals, and replacements — is important because it allows you to avoid error-prone, resource-intensive manual actions, while improving operations and security.

WARNING

If you can't automate your machine identity life cycle, you may increase the risk of experiencing certificate-related outages and serious security breaches.

5. Validate Correct Installation and Configuration

Validation ensures that machine identities are installed properly and working correctly. Validation not only helps you with ongoing management and security, but also it demonstrates compliance and shows progress when you need to replace a large number of machine identities.

6. Monitor for Anomalous Use

After you've established a baseline of normal machine identity usage, you can start monitoring and flagging anomalous behavior, which can indicate a machine identity compromise.

7. Set Up Notifications and Alerts

The ability to find and evaluate potential machine identity issues before they become business interruptions or exposures is critical. If you set up automated alerts and notifications based on policy, they can inform you of unauthorized changes or impending actions that need to be taken. Automated alerts allow you to take immediate action before outages happen or attackers take advantage of weak or unprotected machine identities.

8. Remediate Machine Identities that Don't Conform to Policy

After a policy change, continuous monitoring can flag if the change results in another policy being violated or otherwise causes a machine identity to become noncompliant. When this happens, you must act quickly.

REMEMBER

Automated, intelligence-driven action allows you to quickly address all compliance issues as well as quickly respond to any security incident that requires bulk remediation.

9. Use a Certificate Service to Deliver Machine Identities

Providing end-users with an easy way to access machine identities allows you to quickly deliver secure, policy-enforced machine identities to all business units. Plus, integrating self-service solutions with DevOps toolsets and cloud platforms allows your developers to seamlessly request and install secure certificates without incurring any delays.

10. Integrate with Your Technology Ecosystem

You can improve the effectiveness of your network and security systems by integrating TLS machine identity management and security, giving these crucial technologies easy access to up-to-date keys and certificates and machine identity intelligence.

Manage and protect your machine identities

There are two actors on every network: humans and machines. Humans rely on usernames and passwords to identify and authenticate themselves, but machines don't. Instead, they use cryptographic keys and digital certificates that serve as machine identities. Every year, businesses spend billions managing usernames and passwords but almost nothing managing SSL/TLS machine identities that secure nearly every critical business function. Learn why cybercriminals target machine identities and how effective management can keep yours safe.

Inside...

- How machine identities are used
- Where machine identities are exposed
- Tips on managing machine identities
- The impact of machine growth
- Why automation is essential

VENAFI®

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-80961-6
Not For Resale

for dummies® A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.