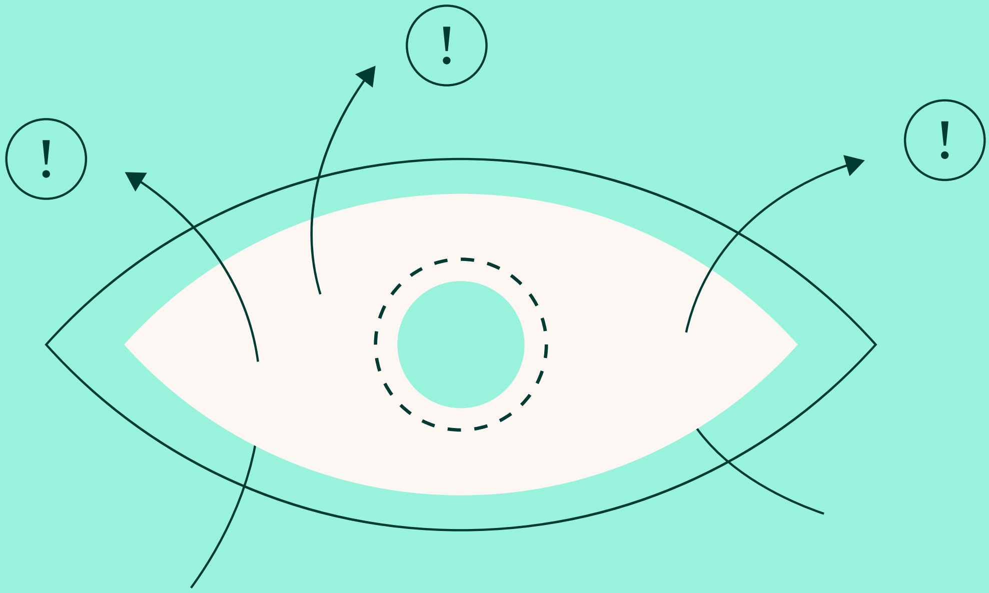
EBOOK

MACHINE IDENTITIES:
Your Biggest Blind Spot for Compliance Risk



A practical guide to identifying and fixing hidden compliance risks in your machine identity infrastructure.

segura®

Introduction

Facing the Invisible Threat

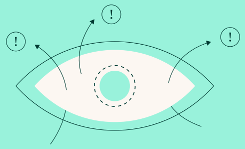
Machine identities, including APIs, bots, and service accounts, are silently multiplying across your IT environments. Yet these non-human identities often remain unseen, unmanaged, and vulnerable to compliance risks.

This eBook shines a light on this hidden area of risk, clearly explains why it matters, and offers actionable steps your team can take right away.

Created with insights from:
Segura® and IDMWORKS

Facilitated by:
Identity Defined Security Alliance

Inside This Guide



Chapter 1

What Are Machine Identities?

What Are Machine Identities?

Machine identities perform critical tasks behind the scenes, from cloud services to automated scripts. They’re the digital identities used by non-human entities to connect, communicate, and complete tasks.

Joseph Carson from Segura® describes them clearly:

> “Think about everything running quietly in your infrastructure—databases, backups, API calls. They’re powered by machine identities. And there are a lot more of them than you realize.”

Chapter 2

Why Machine Identities are Your Compliance Weak Spot

Why Machine Identities are Your Compliance Weak Spot

Unmanaged machine identities create significant compliance risks:

- They often remain active far longer than needed.
- They usually lack clear accountability.
- Few organizations track their activities consistently.

Jessica Sebastian from IDMWORKS sums it up:

> “Machine identities quietly multiply, and most organizations don’t notice them until there’s a compliance issue. By then, it’s often too late.”

Chapter 3

Visibility, Ownership, and Traceability: Where Are You Struggling?

Visibility, Ownership, and Traceability:

Where Are You Struggling?

Machine identity governance isn't just a technical challenge; it's an organizational one. **We asked participants to share their biggest struggle with machine identities, and the results were telling:**

43% said "Ownership" is the #1 issue.

When responsibility is spread across DevOps, IT, security, and compliance teams, it's easy for machine identities to fall through the cracks.

29% cited "Traceability" — a lack of visibility into what identities are doing, who created them, and what they've accessed.

This becomes a major issue during audits, especially when logs are fragmented or nonexistent.

Another 29% pointed to "Lifecycle Management" as their main hurdle.

Controlling the creation, rotation, and decommissioning of machine identities continues to be largely manual and inconsistent.

Surprisingly, **no one chose "Visibility"** as their top concern. This may signal that some teams believe they have enough visibility, but the lack of traceability and ownership suggests otherwise.

> **"When no one owns it, it rarely gets fixed. That's why the governance piece is so essential—it's not just technical; it's organizational."**
>
> — **Jessica Sebastian**, IDMWORKS

Chapter 4

Auditors Are Watching. Are You Ready?

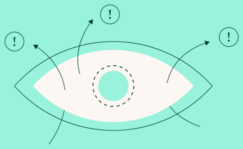
Auditors Are Watching. Are You Ready?

Auditors now explicitly focus on machine identities, **expecting**:

1. Clear, documented inventory.
2. Evidence of ongoing lifecycle management.
3. Defined accountability for every identity.
4. Clear audit trails.

Henrique Stabelin from Segura®, emphasizes:

“Failing to show auditors you’re managing your machine identities is no longer acceptable. You’ll need clear proof that you have it under control.”



Chapter 5

The Certificate Time Bomb: Why You Need Automation Now

The Certificate Time Bomb:

Why You Need Automation Now

Digital certificates are a critical but often neglected part of the machine identity landscape. As certificate lifespans shrink, manual renewal becomes unsustainable.

The TLS/SSL certificate industry is moving toward a **47-day validity period by 2029**, starting with a **reduction to 200 days in March 2026 and further to 100 days in March 2027**. That's a drastic shift from today's 398-day standard.

Why does this matter?

Shorter lifespans = tighter renewal windows.

Organizations without automation face higher risks of expired certs and service outages.

Manual processes won't scale.

Renewing certificates every 47 days across hybrid environments is nearly impossible without automation.

Auditors are paying attention.

Missed renewals and inconsistent certificate governance are now red flags in compliance audits.

Chapter 6

How Are Your Peers Managing Certificates?

How Are Your Peers Managing Certificates?

Poll results from Segura® confirmed the urgency:

75% admitted they're not sure or not involved in certificate management.

This lack of ownership or visibility is a growing liability, especially as certificate lifespans shrink.

25% said they use native tools like AWS Certificate Manager.

These tools help, but they only cover part of the picture and don't replace centralized governance.

That's a significant maturity gap… and a major opportunity.

We're seeing increased demand for **automated certificate management** across regulated sectors as leaders prepare for the coming changes.

> **"If managing certificates manually was painful before, imagine doing it every 47 days. Automation isn't optional anymore—it's essential."**
>
> — **Joseph Carson**, Segura®

Chapter 7

Five Practical Steps for Managing Machine Identities Effectively

Five Practical Steps for Managing Machine Identities Effectively

Here are five **best practices to quickly reduce risk**:

1. **Inventory First:**
   Identify and catalog all machine identities.

2. **Prioritize by Risk:**
   Secure identities with privileged access first.

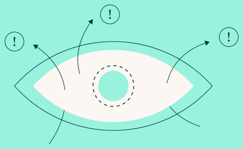
3. **Assign Ownership:**
   Clearly define responsibility across teams.

4. **Automate Lifecycle:**
   Rotate credentials and certificates regularly.

5. **Integrate IAM/PAM:**
   Treat machine identities as part of your broader identity management strategy.

Jessica advises:

“Perfection isn’t your goal—small improvements done consistently will deliver big results.”



Chapter 8

Simplifying Compliance with PAM and IAM

Simplifying Compliance with PAM and IAM

Privileged Access Management (PAM) solutions **help you manage machine identities securely by offering**:

- Automated discovery and lifecycle management.
- Secure vaulting of credentials and secrets.
- Anomaly detection and alerts.
- Simple and reliable audit trails.

Henrique highlights:

> “PAM isn’t just for human administrators anymore—it’s your best tool for handling the complexity and risk of privileged machine identities.”

Chapter 9

Bringing It All Together: People, Processes, and Product

Bringing It All Together:

People, Processes, and Product

As David Muniz emphasizes:

> **“It’s not just about having the right product. You need alignment across the 3 Ps: People, Processes, and Product. Without that, machine identity management won’t scale — and it won’t pass audit.”**

This balance is crucial. Organizations that effectively manage machine identities invest in skilled teams, well-defined governance workflows, and solutions that automate discovery, policy enforcement, and auditing. It’s the synergy of these three pillars that drives sustainable, compliant machine identity programs.

Chapter 10

Selling Machine Identity Management Internally

Selling Machine Identity Management Internally

How do you convince stakeholders to invest in machine identity management?

Focus on Risk Reduction:

Lower compliance and cybersecurity risks.

Highlight Efficiency Gains:

Automating identity management saves resources and time.

Showcase Business Value:

Secure identities drive business agility and innovation.

Joseph Carson shares practical insight:

“Business leaders respond to clear value. Position identity management as a way to enable business growth and reduce costly incidents.”

Chapter 11

Your Next Steps to Reduce Risk Immediately

Your Next Steps to Reduce Risk Immediately

Start today:

- Get visibility quickly. **Inventory your machine identities.**
- **Prioritize your highest-risk identities** for immediate action.
- **Automate lifecycle management**, including rotation, renewal, and revocation.
- **Clearly assign ownership** and responsibility.
- **Integrate machine identity management** into your **existing IAM strategy.**

Jessica encourages a practical approach:

> "Don't wait until it's perfect. Just start securing your most critical identities right now."

Conclusion

Machine identities are now front and center on auditors' radar, presenting a serious compliance risk. The good news is you can reduce that risk quickly by gaining visibility, automating lifecycle management, and clearly assigning responsibility.

Take these steps now to strengthen your security, simplify compliance, and protect your business from costly blind spots.

Get Started

Schedule a 1:1 session with an identity expert

REQUEST A DEMO NOW!

About Segura®

Segura® provides an all-in-one platform for managing machine and human identities, including certificates, secrets, and privileged access. Fast to deploy and simple to use, with full control of machine identities and automated compliance.

About IDMWORKS

IDMWORKS is a trusted identity security partner that delivers clear, practical solutions for managing identities, helping companies simplify compliance, reduce risks, and operate efficiently.

segura® | Futureproof Identity Security | segura.security

EBOOK

MACHINE IDENTITIES: Your Biggest Blind Spot for Compliance Risk

Document Classification: Public | July 2025