ANM
TECH DAY

Know Who's Knocking: Build Your Identity Strategy

Robert Ochoa

CISSP, CRISC, SSCP, CHSP

Director, Cybersecurity

Robert Ochoa

Director, Cybersecurity

CISSP, CRISC, SSCP, CHSP | U.S. Army Veteran

- U.S. Army Veteran
- 30+ Years networking and cybersecurity experience
- Industry experience: Motorola, 3Com, Lucent, Insight, Cisco, Okta
- Hold several industry certifications
- Leadership and systems engineering background

Key Skills:

- Driving Business Outcomes
- Leadership | Creating High Performance Teams
- Cybersecurity Solutions
- Identity and Access Management (IAM)
- Governance and Compliance

www.linkedin.com/in/robochoa

anm

What We Will Cover

Agenda

- Know Who's Knocking: Build Your Identity Strategy
  - How modern identity has changed
  - Building a resilient identity foundation
  - Investments vs outcomes
  - A practical framework approach
  - Key Takeaways
- Q & A

ANM
TECH DAY

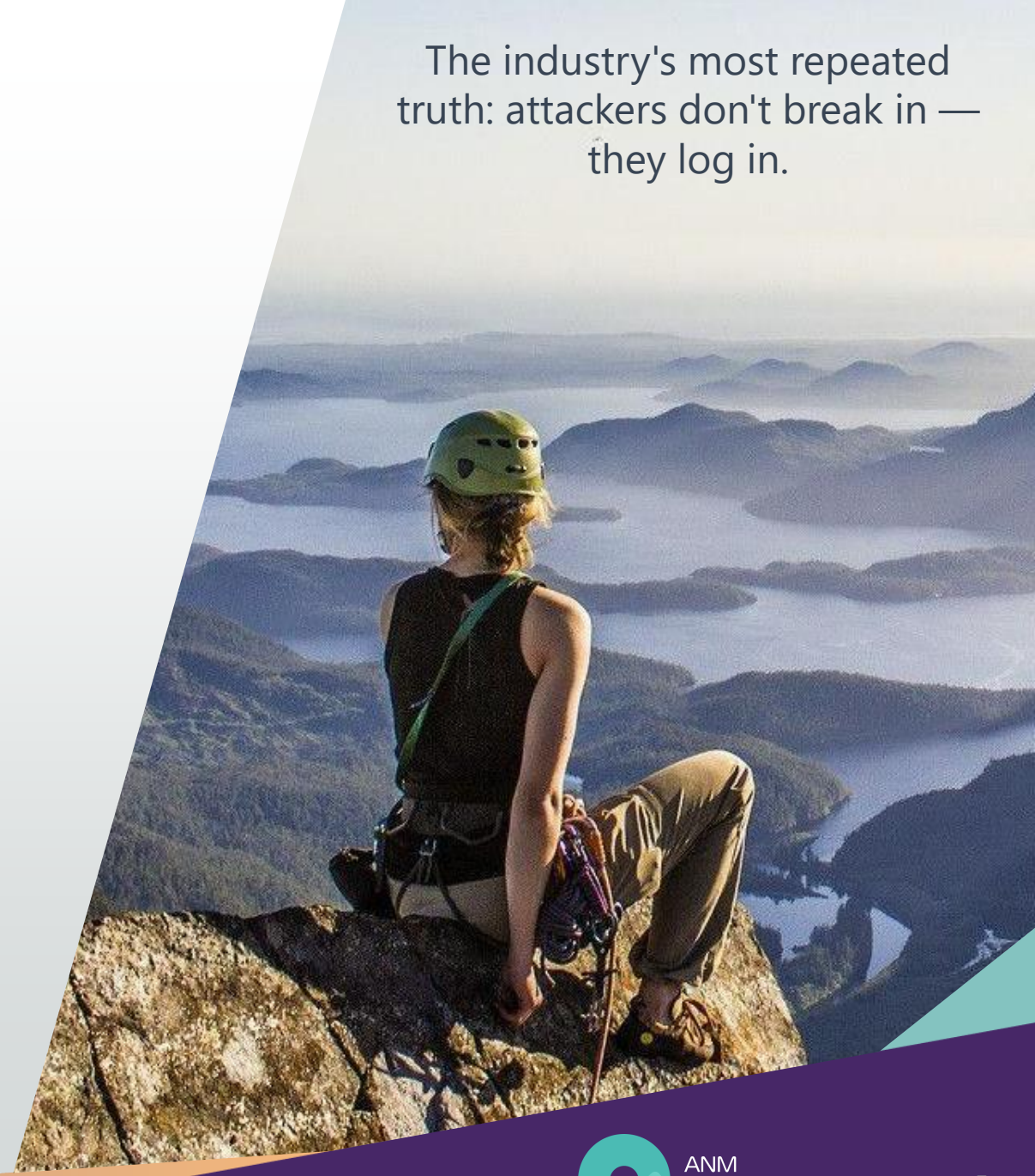
How modern identity has changed

Three Truths

Current-day Realities

- **Identity is the New Perimeter**
  - Shift from network to identity
  - Identity governs access
  - Weak identity governance increases risk of credential exploitation
- **Attackers Don’t Break In — They Log In**
  - Modern attacks target valid user credentials through phishing, credential stuffing, and social engineering techniques.
  - Need for continuous risk evaluation
- **Leadership Reality: Tools Before Strategy**
  - Often implement identity tools reactively, resulting in fragmented controls and unclear ownership.
  - Without a governance framework, organizations face orphaned accounts, excessive privileges, and manual processes.

The industry's most repeated truth: attackers don't break in — they log in.



Identity Has Expanded Beyond Humans

Age of AI Agents

- **Expanded Identity Scope**
  - Identities creep well beyond employees, contractors, partners, and customers with unique risks.
- **Non-Human Identities**
  - Non-human identities like service accounts, APIs, and AI agents now outnumber human users, requiring special governance.
- **Governance Challenges**
  - Static roles and audits struggle with identity proliferation; modern governance requires automation and strong authentication.
- **Strategic Identity Management**
  - Effective identity strategies apply least privilege, continuous monitoring, and accountability to all identity types.

Infosecurity Magazine citing SANS Institute (April 9, 2026)

Gartner, Machines Can't Keep a Secret (March 6, 2026)

CyberArk: Machine Identities Outnumber Humans by More Than 80 to 1

Reality for Most Enterprises

NHI Ratios by Organization Type

Sector	Typical Ratio	Why It Matters
SLED	**5:1 – 15:1**	On-prem heavy, legacy systems, limited SaaS integration
Traditional Enterprise	**15:1 – 40:1**	Legacy + modern SaaS mix, moderate cloud adoption
Commercial / Mid-Market	**30:1 – 80:1**	Active SaaS stack, DevOps practices, growing cloud
Cloud-Native	**100:1 – 500:1+**	Microservices, CI/CD pipelines, containers, AI workloads

What Counts as a Non-Human Identity

Established

- Service Accounts — Windows AD, database, application
- API Keys & Tokens — Salesforce, AWS, GitHub, Stripe
- SaaS OAuth Grants — Slack, Google Workspace, HubSpot, M365
- Workflow Automation — Zapier, Power Automate, Make/Integromat
- CI/CD Pipelines — GitHub Actions, Jenkins, Azure DevOps
- Cloud Workload IDs — AWS IAM roles, Azure Managed Identities, GCP

Emerging

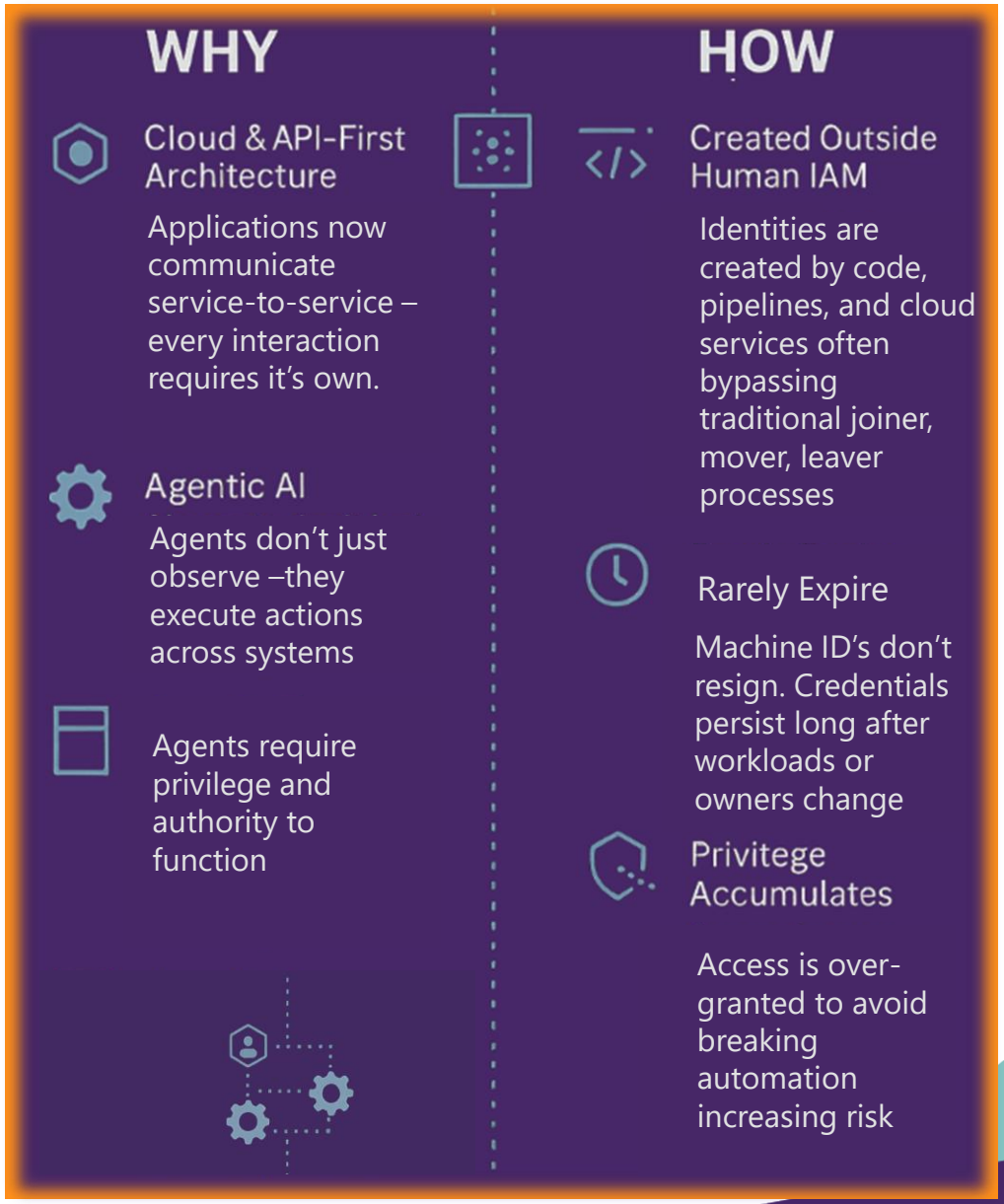
- AI Agents & Copilots — LLM API keys, Copilot connectors
- Short-lived Certs — TLS/SSL now on 47-day lifecycle mandate

Non-Human Identities

An exponential explosion

- **WHY**
  - Digital systems now do the work people used to do
  - Speed and scale has overtaken human control
  - AI is shifting identity from access to action

- **HOW**
  - Identities are instantiated programmatically, not provisioned deliberately – by people
  - Lifecycle ownership is unclear or nonexistent
  - Operational convenience overrides least-privilege discipline



AI: Defining the Shifting Identity Landscape

Key Implications

- **AI Rewrites Vulnerability Discovery**

  Glasswing's AI found 1,000+ zero-day flaws in weeks — including a 27-year-old bug — outpacing any human-led security audit.

- **Identity Is the Last Defensible Perimeter**

  As AI accelerates attacks, identity becomes the primary control plane. Network perimeters no longer define trust boundaries.

- **Non-Human Identities Are the Blind Spot**

  AI agents need governed, scoped, auditable access — not user-level permissions. Your IAM strategy must account for machine principals.

- **The Industry Is Already Mobilizing**

  AWS, Microsoft, Google, CrowdStrike & 8 others are activating around AI-powered defense — signaling a fundamental paradigm shift.

- **Zero-Trust + AI-Aware IAM = Your Foundation**

  Identity-first architecture, least-privilege access, and continuous authentication are now security requirements, not best practices.

ANM
TECH DAY

Building a resilient identity foundation

Zero Trust Architecture Technologies by Pillar

Goals

- **Verify Explicitly**
- **Enforce Least Privilege**
- **Assume Breach**
- **Identity-Centric Enforcement**

Identity

- **Identity and Access Management (IAM)**
- **Privileged Access Management (PAM)**
- **Multifactor Authentication (MFA)**
- **Identity Governance and Administration (IGA)**
- **Behavioral Analytics**

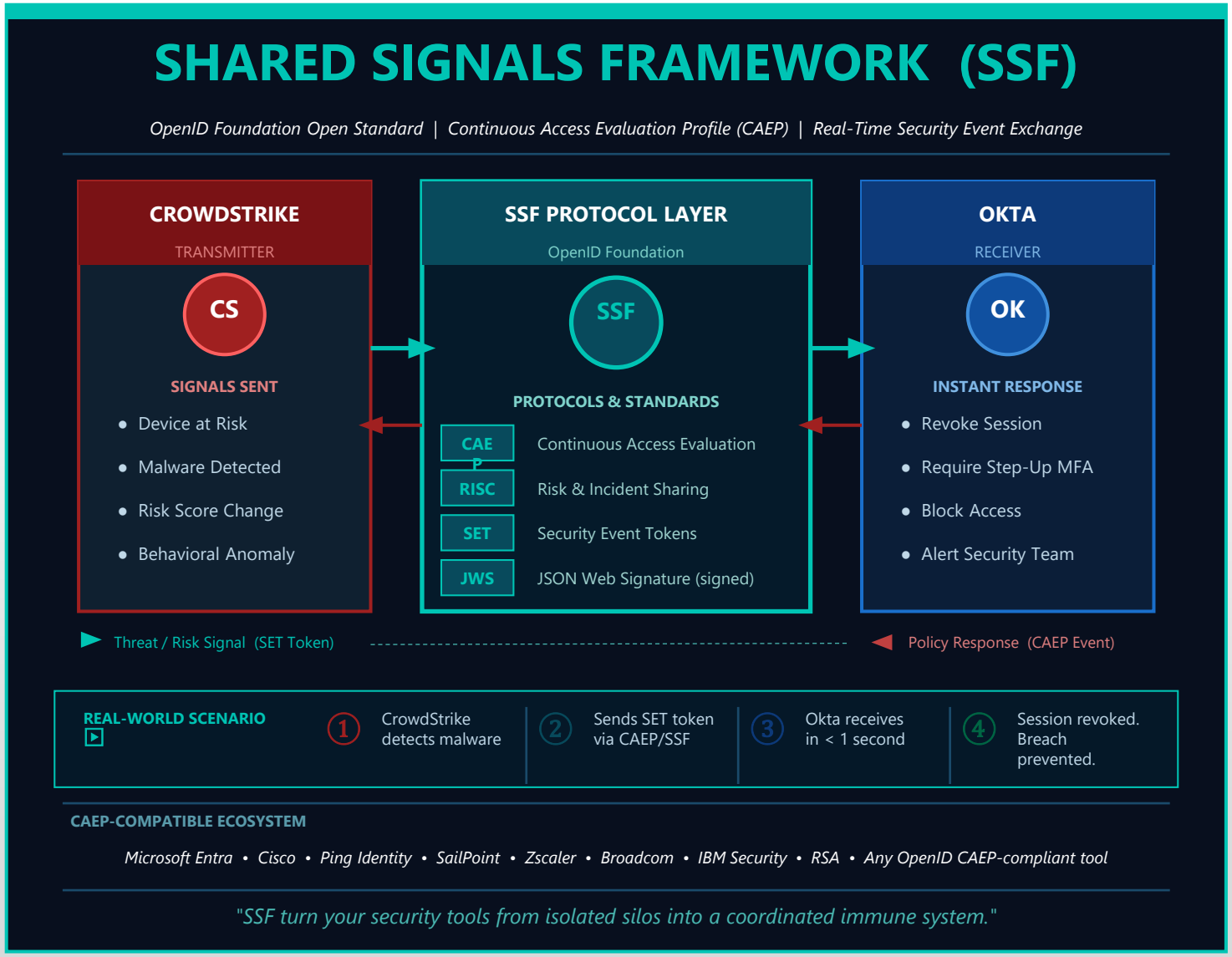
Identity | Device | Network | Apps & Workloads | Data

What are we looking for?

Core Identity Capabilities | Tools & Technology

- **Identity Governance Administration**
  - Governs the full identity lifecycle — human and non-human. Automates provisioning and deprovisioning to eliminate orphaned accounts and enforce least privilege.
- **Privileged Access Management**
  - Eliminates standing privilege for humans and machines. JIT access, credential vaulting, and rotation. Apply the same rigor to service accounts, API keys, and AI agent credentials as to admin accounts.
- **Machine Identity Management**
  - Manages lifecycle, secrets, and access controls for service accounts, certificates, and AI agent identities — the fastest-growing and least-governed identity class.
- **Adaptive Risk-Based Authentication**
  - Adjusts authentication strength based on context and risk signals. For NHIs that can't do MFA, short-lived tokens, continuous monitoring, and behavioral baselines serve the same function.
- **Cloud-Driven Control Plane**
  - Centralizes visibility and policy enforcement across hybrid and multi-cloud — critical as NHIs proliferate across AWS, Azure, GCP, and SaaS simultaneously.

Shared Signals Framework: Identity's Real-Time Security Nervous System



Why SSF Should Be in Every Cybersecurity Strategy

- **Real-Time vs. Polling: From Minutes to Milliseconds**

  Legacy security tools poll for changes every 15–60 minutes. SSF pushes verified events instantly — stopping lateral movement before it starts.

- **Open Standard: No Vendor Lock-In**

  Any CAEP-compliant tool — CrowdStrike, Microsoft Entra, Okta, Zscaler — can signal any other. One open protocol, unlimited integrations.

- **Continuous Verification at Machine Speed**

  SSF is the technical backbone of Zero Trust. Every session is re-evaluated on every signal — not just at login — in real time.

- **Bidirectional Intelligence**

  Signals flow both ways: your IdP knows about endpoint threats; your EDR knows about session anomalies. Your tools become one unified defense.

- **Game Changer: A Breach Stopped in < 1 Second**

  CrowdStrike detects malware → sends SET token → Okta revokes the session before the attacker pivots. No manual intervention required.

Shorter Certificates, Faster Rotation

CA/B Forum Mandated Changes

What is changing

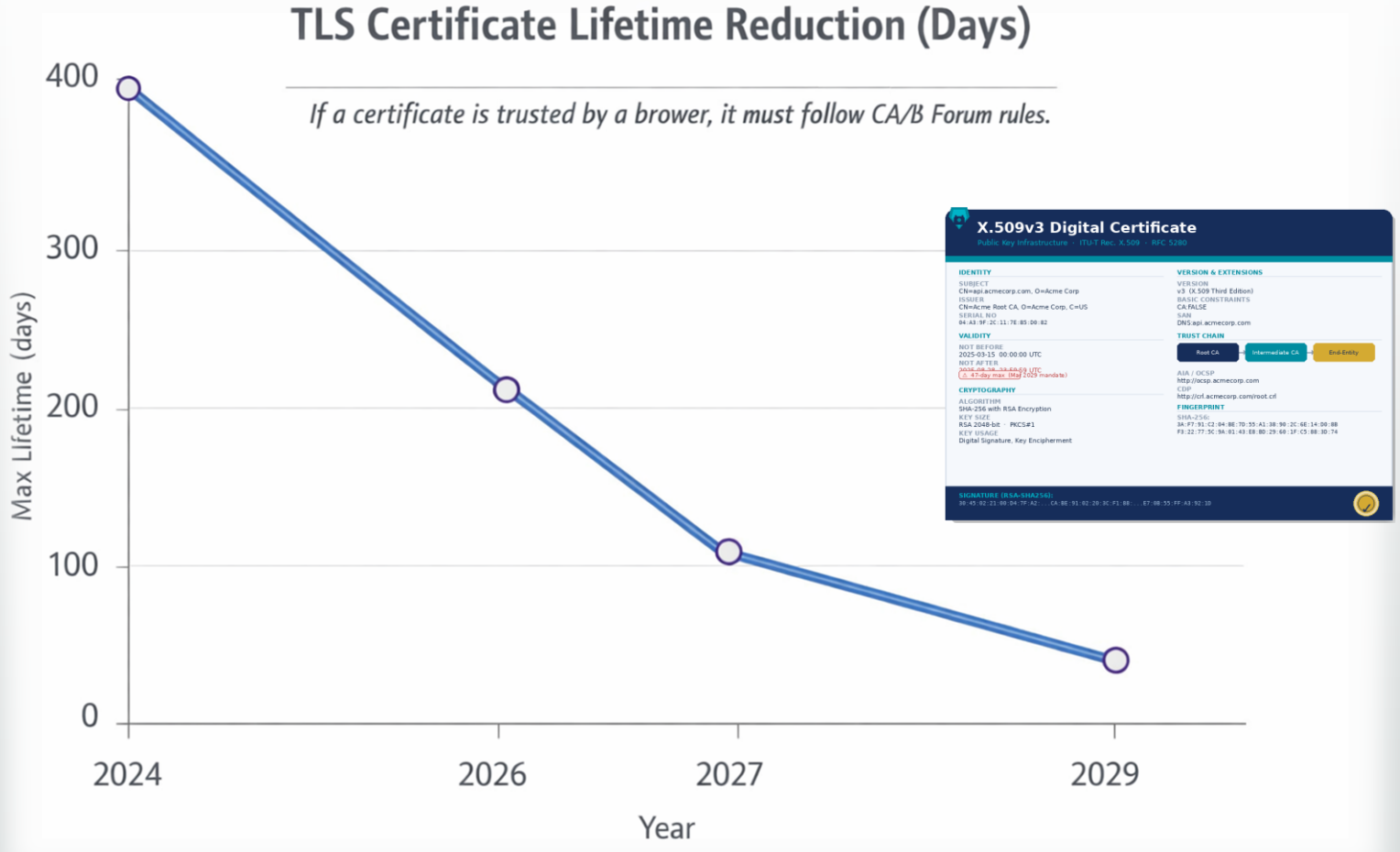
Max public TLS lifetimes step down from 398 days today to 200 (Mar 2026), 100 (Mar 2027), and 47 (Mar 2029). Domain Control Validation (DCV) reuse windows also shrinks, down to ~10 days.

Why it matters

Renewals jump from yearly to 8+ per service per year. Browser enforcement is automatic, making automation (ACME/API issuance + integrated deployment) a requirement—not a choice.

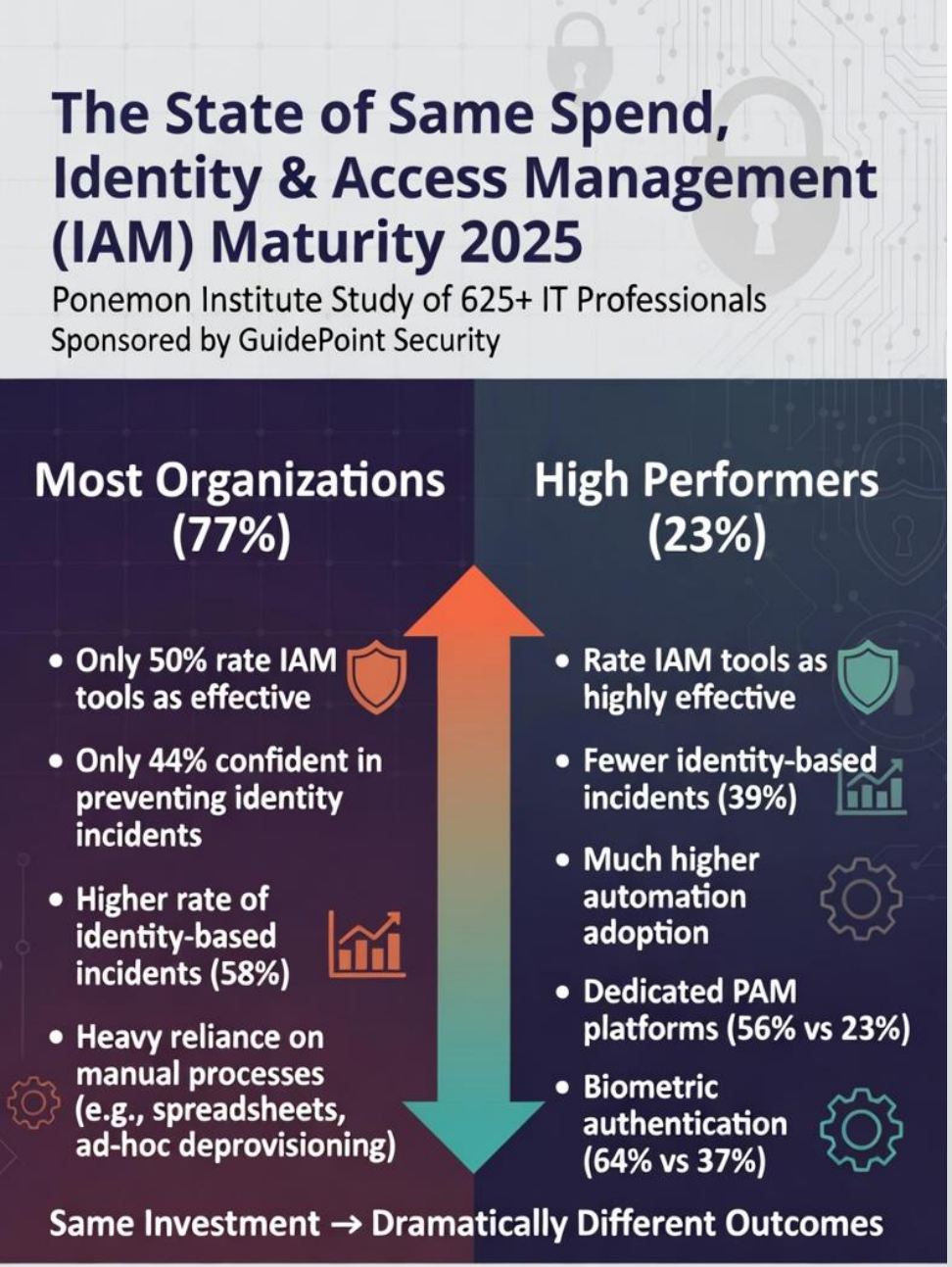
What this means for every credential

Whether your agents authenticate with certificates, OAuth tokens, or API keys – the direction is the same: short-lived, automated, no standing access. The CA/B Forum mandate is the regulatory proof point. Your NHI strategy needs to apply the same logic everywhere.



ANM
TECH DAY

Investments vs outcomes



ANM

CASE STUDY

A Tale of Two Org's

Same Spend, Different Result | Local Government

Organization A

Reactive | Siloed Tools

- Identity tools deployed in isolation
- **58% identity-based incident rate**
- Manual processes, spreadsheets
- Poor cross-system visibility

Organization B

Strategic | Integrated

- Identity aligned to business roles
- **39% identity-based incident rate**
- High automation adoption
- PAM + IGA working together

Same investment → Dramatically different outcomes

The State of Identity and Access Management (IAM) Maturity – Ponemon Institute

Connecting Identity Spend to Business Value

Cloud-Driven Control Plane

- **Value Your Machine ID Capabilities**
  - Manage mutually exclusive NHI's and create associated access controls
- **Impact of IGA**
  - Identity Governance and Administration streamlines onboarding and reduces access errors, boosting productivity, lowering risk.
- **Benefits of PAM**
  - Privileged Access Management minimizes insider risks and supports compliance requirements.
- **Role of Identity Analytics**
  - Identity analytics enhance audit readiness and provide insights into emerging risk trends.

Value is workflow and security

Different Approaches

Managing Non-human Identities | Closing the Blind Spot

Cyberark

PAM-First Approach

AI agents as privileged identities

- Access Model: Ephemeral credentials, Just-In-Time (JIT) Access, Zero Standing Privilege (ZSP), delegation tokens + session controls

Okta

IGA & IAM-First Approach

AI agents as first-class non-human identities (NHIs)

- Access Model: OAuth 2.0 tokens with scoped, policy-driven access, register agents in the Universal Directory

Microsoft

Ecosystem-Native Approach

AI agents as native agent identities

- Access Model: Dedicated Microsoft ***Entra Agent ID*** (specialized workload identity), specialized Entra tokens for agents

Commonality: Token based, dynamic, JIT, ZSP, IGA, shift from statics

ANM
TECH DAY

A practical framework approach

Six Pillars of Identity Strategy & Execution

1. **Identity Inventory:** Inventory all human and NHI accounts for a complete landscape to reduce unknown risks (start with your native IdP, NHI-specific tool like Astrix or Entro against your AD, cloud, and code; assign an owner to everything)

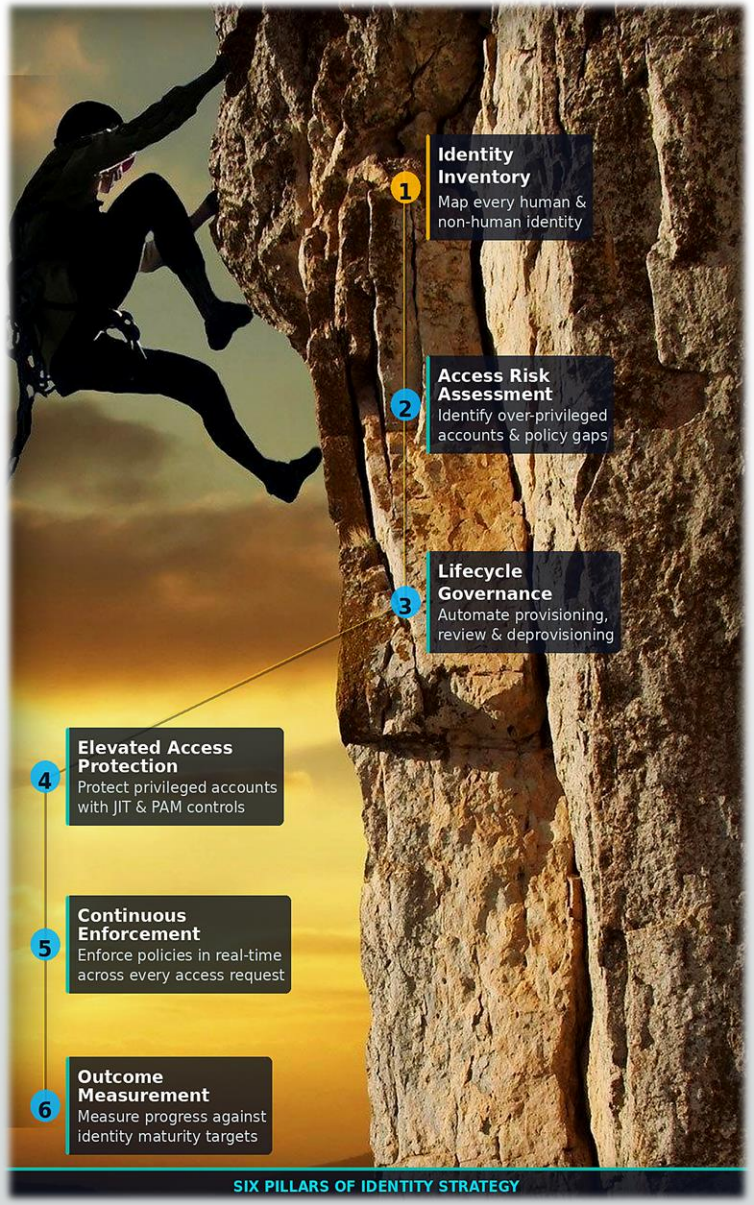
2. **Access Risk Assessment:** Evaluate existing access to detect over-privileged accounts and potential security risks (AD sweeps--"Password Never Expires & non-interactive logon history," cloud IAM enumeration, secrets and code repository scanning, ITDR monitoring, CAP's, PAM workflows, etc.).

3. **Lifecycle Governance**: Automate identity LCM and enforce policies for secure and compliant user access (IGA workflows, automate JLM's, HRIS workflows, apply the same lifecycle logic to NHIs, build in scheduled access reviews with teeth).

4. **Elevated Access Protection:** Use just-in-time access and continuous monitoring to safeguard privileged accounts (PAM, Eliminate standing privileges with JIT access, Vault and rotate every privileged credential, Require approval workflows for PAM requests).

5. **Continuous Enforcement:** Implement adaptive controls that continuously enforce access policies to respond to changing risks (PAM, ITDR, connect tools w/ Shared Signals Framework, make policy adaptive, not static).

6. **Outcome Measurement:** Measure identity strategy effectiveness using business-relevant metrics for continuous improvement (look at risk reduction not compliance, reduction in standing privileged accounts, increase in JIT, less orphaned, fewer incidents, etc.).



Phased Adoption

Bite Sizes with Urgency

- **Start with visibility and quick wins**
  - Establish a baseline by inventorying identities and access, closing obvious gaps, and delivering early improvements that reduce risk without disrupting users or operations.
- **Introduce automation and structured access management**
  - Automate joiner-mover-leaver processes, standardize access provisioning, and reduce manual effort while improving consistency and speed.
- **Advance to governance, controls, and analytics**
  - Apply policy-driven governance, privileged access controls, and analytics to continuously enforce least privilege and detect risk at scale.
- **Measure outcomes and iterate deliberately**
  - Track progress using business-relevant metrics (risk reduction, access turnaround time, audit effort) to guide ongoing improvements and investment decisions.

Comes down to Cloud IdP handling NHI's , PAM, IGA

Phased full-stack identity deployments

Key Takeaways

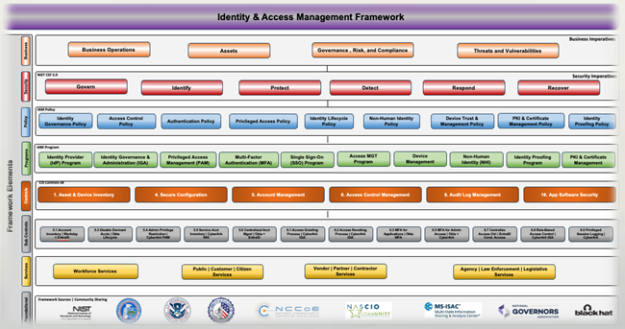
“Know who's knocking?” The answer to that question is the whole game.

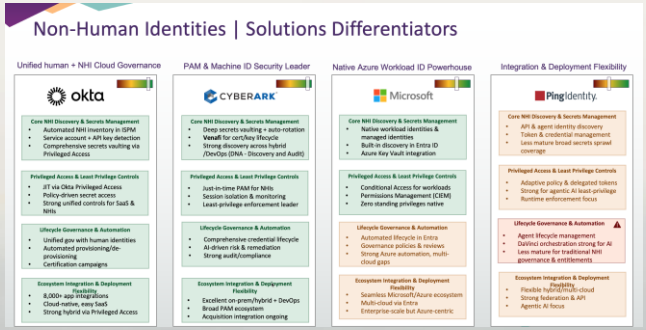
- **Identity is the perimeter now. Not the network — the identity.**
- **Your non-human identities outnumber your people. If you're not governing them, no one is.**
- **Tools alone don’t reduce risk. Strategy does.**
- **Strong identity controls don’t slow the business — weak ones do.**
- **Phase it, measure it, and keep moving. Don’t try to boil the ocean.**

Now you know who's knocking. The question is: are you ready to answer?

How ANM Can Help?

- **Workshops**: Understand your environment with key stakeholders. Where are the gaps?
- **Tools Rationalization**: Inventory, heat map, analysis, roadmap
- **Cost Analysis**: Help analyze Opex vs Capex, ROI and TCO of current and potential changes





robert.ochoa@anm.com

Call your Account Manager and ask about an Identity Workshop for your organization. Let ANM help you on your Identity Journey.

Q & A

Robert Ochoa
Director, Cybersecurity
robert.ochoa@anm.com
602.380.5101

www.linkedin.com/in/robochoa