IAM Excellence Day 2026 – Digital Identities in the age of AI

Andre Priebe, CTO iC Consult

March 24th, 2026

iC CONSULT

The Leader in Identity & Access Management

We are the Trusted Partner of Choice for Identity Security.

iC Consult is the leading independent consultancy, system integrator, and managed services provider for Identity Security. Our service portfolio covers Managed Services for IAM including advisory, architecture, implementation, integration, support, and operations, ensuring that we can support our customers throughout their entire IAM journey.

MENTIONED
Leading Expert in IAM
IAM Professional Services Listing
Gartner

MENTIONED
Overall Leader
Leadership Compass System Integrators
KuppingerCole ANALYSTS

- 25+ Years Experience
- 850+ Employees
- 20+ Global Offices
- 300+ Active Customers
- 30+ Partners

CYBERARK Delinea Microsoft okta Ping Identity
Omada ONE IDENTITY by Quest SailPoint Saviynt

Business Consulting & Technology Advisory

Paving Your Way to IAM Excellence

Implementation & Integration

Transforming your IAM Strategy into Action

Support & Operations

Ensuring Your IAM Infrastructure is Always Secure

IAM Managed Services

Streamlining and Securing Your IAM Experience

iC Consult | Contact us: sales@ic-consult.com | www.ic-consult.com

We Champion #IAM Excellence.

AI and Identity Security: Three Forces Reshaping IAM

AI is Attacking, Defending, and Enabling Identity — Simultaneously

☠

AI by Attackers

AI-Powered Phishing & Account Takeover

LLMs generate hyper-personalized spear-phishing emails at scale, bypassing traditional filters and increasing credential theft success rates dramatically.

Deepfake Identity Fraud

AI-generated voice and video clones defeat biometric authentication and trick helpdesk staff into resetting credentials.

AI and Identity Security: Three Forces Reshaping IAM

AI is Attacking, Defending, and Enabling Identity — Simultaneously

AI by Attackers

AI-Powered Phishing & Account Takeover

LLMs generate hyper-personalized spear-phishing emails at scale, bypassing traditional filters and increasing credential theft success rates dramatically.

Deepfake Identity Fraud

AI-generated voice and video clones defeat biometric authentication and trick helpdesk staff into resetting credentials.

AI for Identity Security

AI-Driven Anomaly Detection

ML models detect unusual access patterns and lateral movement in real time, enabling ITDR to identify compromised identities before damage occurs.

AI-driven IAM

AI auto-reviews entitlements and surfaces high-risk access for revocation, reducing rubber-stamping and certifier fatigue in IGA processes. Application on-boarding is accelerated by agentic AI.

AI and Identity Security: Three Forces Reshaping IAM

AI is Attacking, Defending, and Enabling Identity — Simultaneously

AI by Attackers

AI-Powered Phishing & Account Takeover

LLMs generate hyper-personalized spear-phishing emails at scale, bypassing traditional filters and increasing credential theft success rates dramatically.

Deepfake Identity Fraud

AI-generated voice and video clones defeat biometric authentication and trick helpdesk staff into resetting credentials.

AI for Identity Security

AI-Driven Anomaly Detection

ML models detect unusual access patterns and lateral movement in real time, enabling ITDR to identify compromised identities before damage occurs.

AI-driven IAM

AI auto-reviews entitlements and surfaces high-risk access for revocation, reducing rubber-stamping and certifier fatigue in IGA processes. Application on-boarding is accelerated by agentic AI.

Identity Security for AI

Governing Non-Human Identities

AI agents and copilots require dedicated machine identities, scoped permissions, and PAM controls to prevent privilege abuse and data exfiltration.

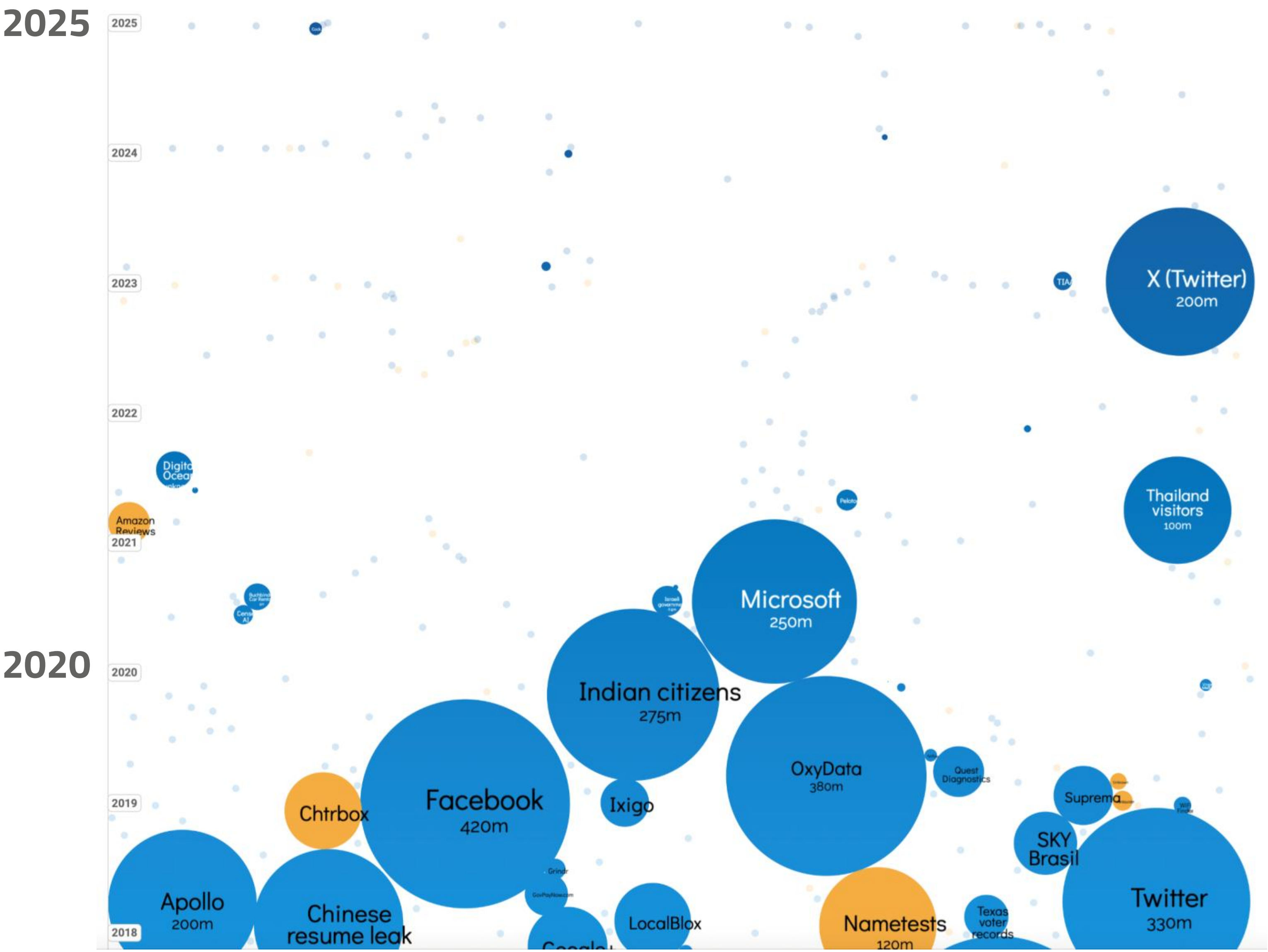
Zero Trust for Agentic Workflows

Continuous authentication and least-privilege policies ensure AI systems access only what they need, with full audit trail for compliance.

Identity Data Breaches

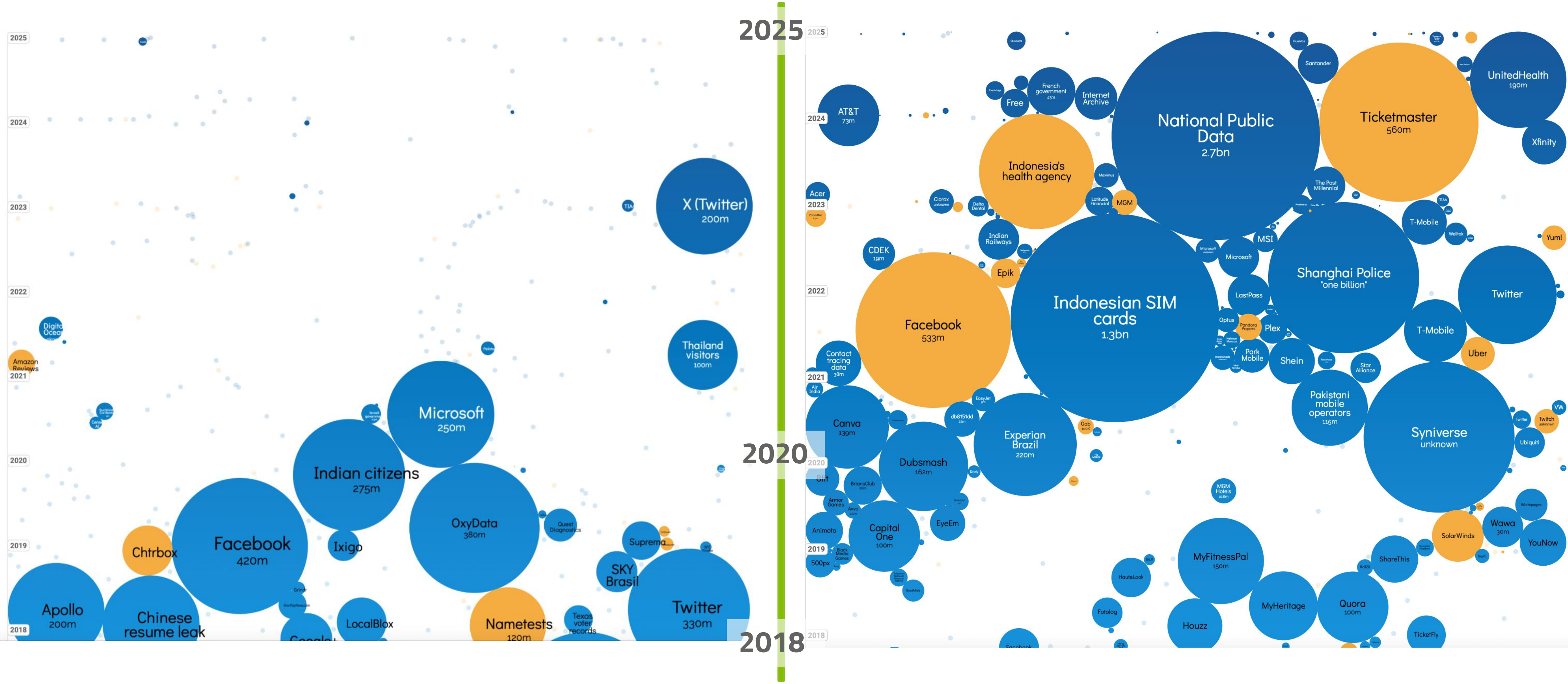
Caused by Poor Security

- Mis-configurations
- Broken access management
- Data Accessible without large efforts
- Level of Security is increasing significantly over the last years



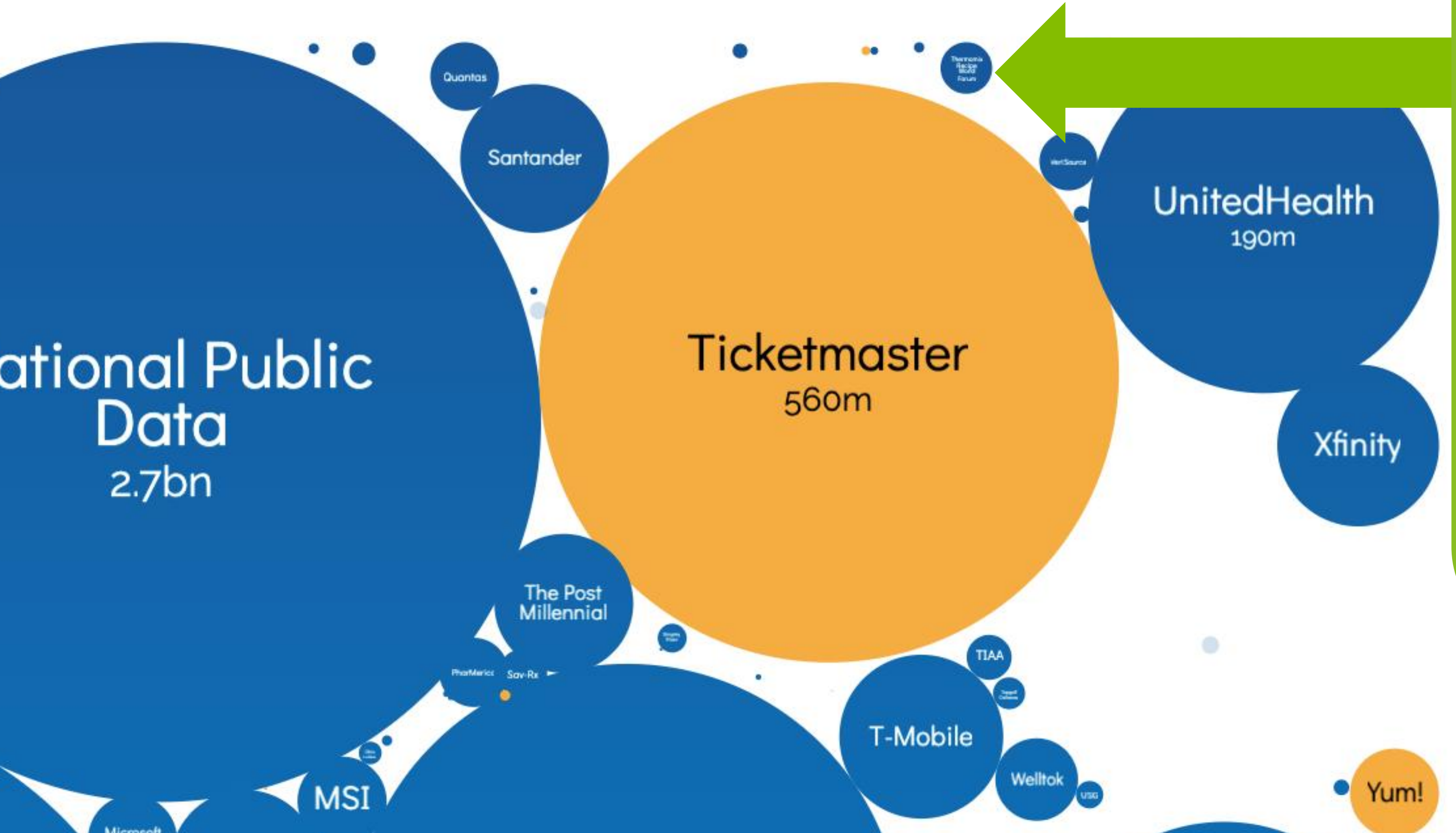
Identity Data Breaches

Caused by **Poor Security** vs **Sophisticated Attacks**



Identity Data Breaches

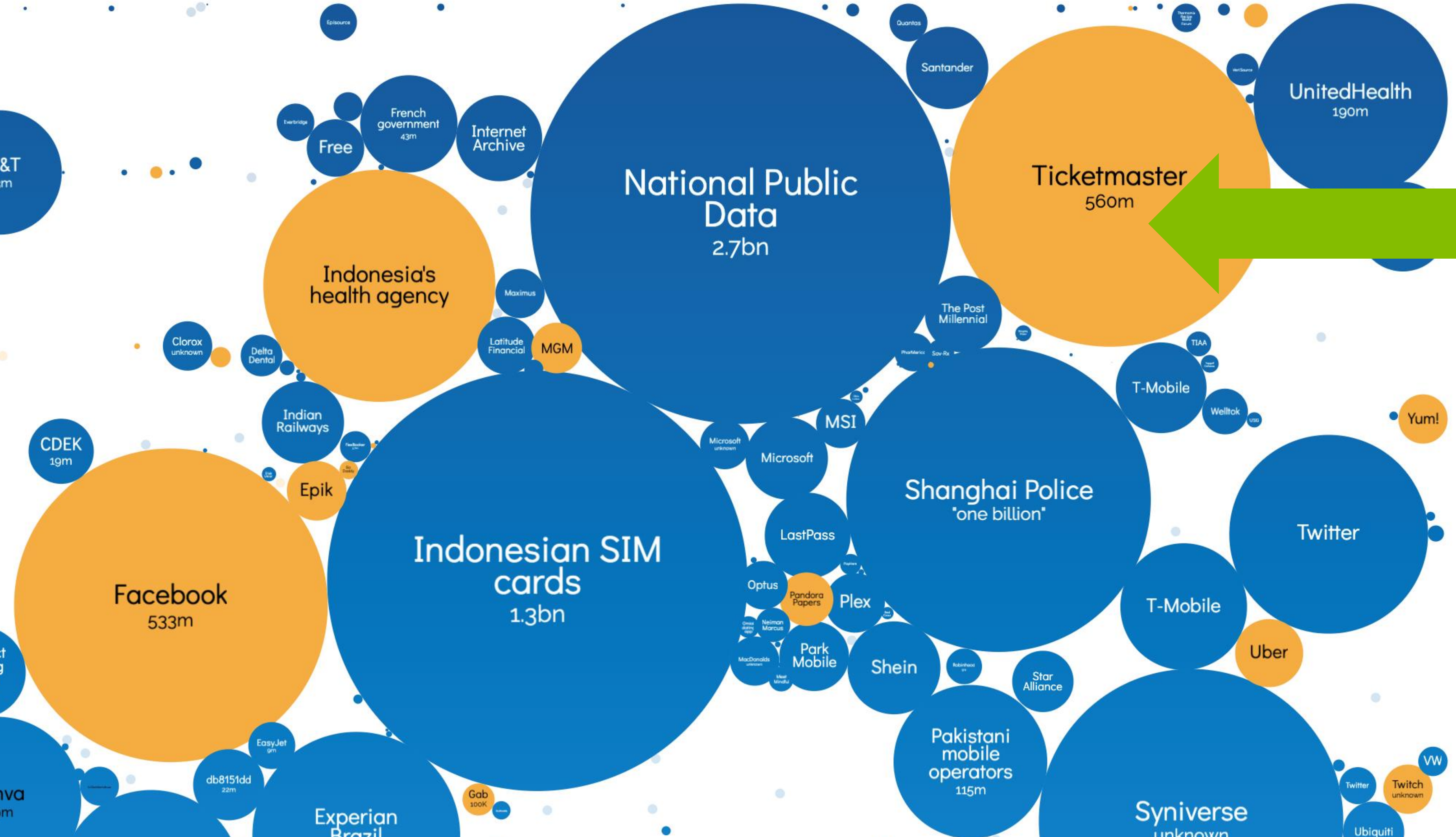
Caused by **Poor Security** vs **Sophisticated Attacks**



- **Rezeptwelt.de affected January 2025**
- **3.1 Million affected accounts**
- **Compromised data**
  - **Email addresses**
  - **Phone numbers**
  - **Birthdates**
  - **Physical addresses**
- **Luckily no recipes affected!**

Identity Data Breaches

Caused by **Poor Security** vs **Sophisticated Attacks**



Identity Data Breach – Ticketmaster

Causes and Consequences

What happened?

Identity Theft
at a contractor

snowflake
Weak Security Configuration at Ticketmaster Tenant.

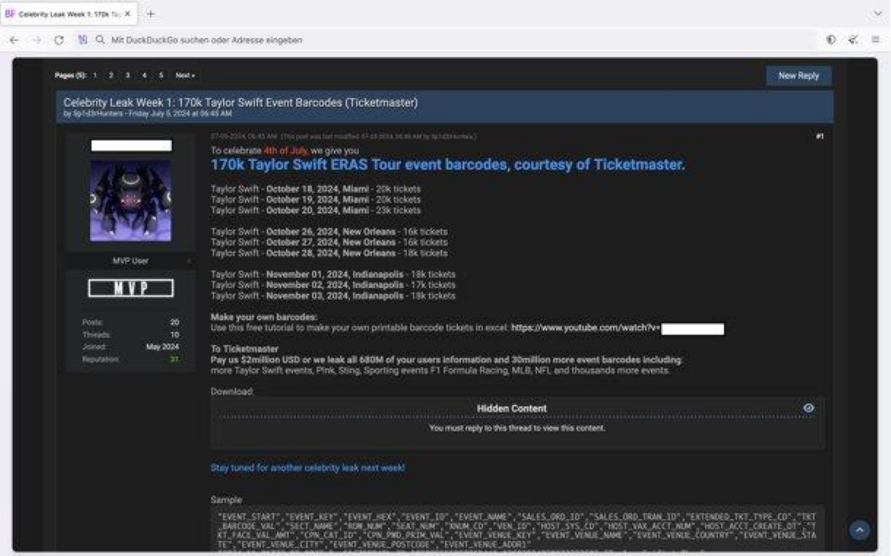
ticketmaster
Attacker had **access to several systems**, 560m records affected.

1 **External User affected**

2 **External SaaS affected**

Consequences of the attack

170k Taylor Swift ERAS Tour Digital Tickets exposed


Celebrity Leak Week 1: 170k Ta... ×
Mit DuckDuckGo suchen oder Adresse eingeben
Pages (5): 1 2 3 4 5 Next »
New Reply

Celebrity Leak Week 1: 170k Taylor Swift Event Barcodes (Ticketmaster)
by Sp1d3rHunters - Friday July 5, 2024 at 06:45 AM

[redacted]
MVP User
MVP
Posts: 20
Threads: 10
Joined: May 2024
Reputation: 31

07-05-2024, 06:45 AM (This post was last modified: 07-05-2024, 06:46 AM by Sp1d3rHunters.) #1

To celebrate 4th of July, we give you
170k Taylor Swift ERAS Tour event barcodes, courtesy of Ticketmaster.

Taylor Swift - **October 18, 2024, Miami** - 20k tickets
Taylor Swift - **October 19, 2024, Miami** - 20k tickets
Taylor Swift - **October 20, 2024, Miami** - 23k tickets

Taylor Swift - **October 26, 2024, New Orleans** - 16k tickets
Taylor Swift - **October 27, 2024, New Orleans** - 16k tickets
Taylor Swift - **October 28, 2024, New Orleans** - 18k tickets

Taylor Swift - **November 01, 2024, Indianapolis** - 18k tickets
Taylor Swift - **November 02, 2024, Indianapolis** - 17k tickets
Taylor Swift - **November 03, 2024, Indianapolis** - 18k tickets

Make your own barcodes:
Use this free tutorial to make your own printable barcode tickets in excel: **https://www.youtube.com/watch?v=**[redacted]

To Ticketmaster
Pay us $2million USD or we leak all 680M of your users information and 30million more event barcodes including:
more Taylor Swift events, Pink, Sting, Sporting events F1 Formula Racing, MLB, NFL and thousands more events.

Download:
Hidden Content
You must reply to this thread to view this content.

Stay tuned for another celebrity leak next week!

Sample

```
"EVENT_START","EVENT_KEY","EVENT_HEX","EVENT_ID","EVENT_NAME","SALES_ORD_ID","SALES_ORD_TRAN_ID","EXTENDED_TKT_TYPE_CD","TKT
_BARCODE_VAL","SECT_NAME","ROW_NUM","SEAT_NUM","XNUM_CD","VEN_ID","HOST_SYS_CD","HOST_VAX_ACCT_NUM","HOST_ACCT_CREATE_DT","T
KT_FACE_VAL_AMT","CPN_CAT_ID","CPN_PMD_PRIM_VAL","EVENT_VENUE_KEY","EVENT_VENUE_NAME","EVENT_VENUE_COUNTRY","EVENT_VENUE_STA
TE","EVENT_VENUE_CITY","EVENT_VENUE_POSTCODE","EVENT_VENUE_ADDR1"
```

Ticketmaster pays Identity Monitoring Services for customers **for 12months.**

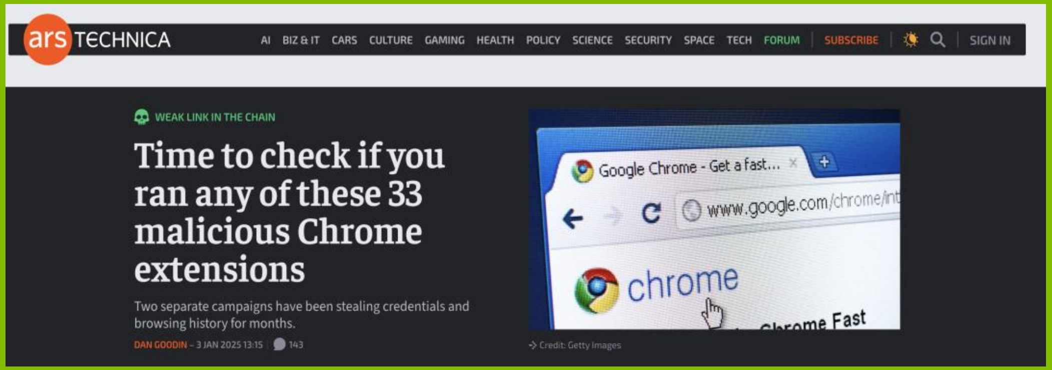
Browser Extension Attack (24th Dec. 2024)

Focused Assault on Chrome Extension Developers

Attackers exploited the Chrome Web Store to distribute harmful versions of popular Chrome Extensions

The attacker managed to gain access to browser sessions for various victim services

- Bypassing MFA
- Not detected as harmful code by Endpoint protection solutions



WEAK LINK IN THE CHAIN

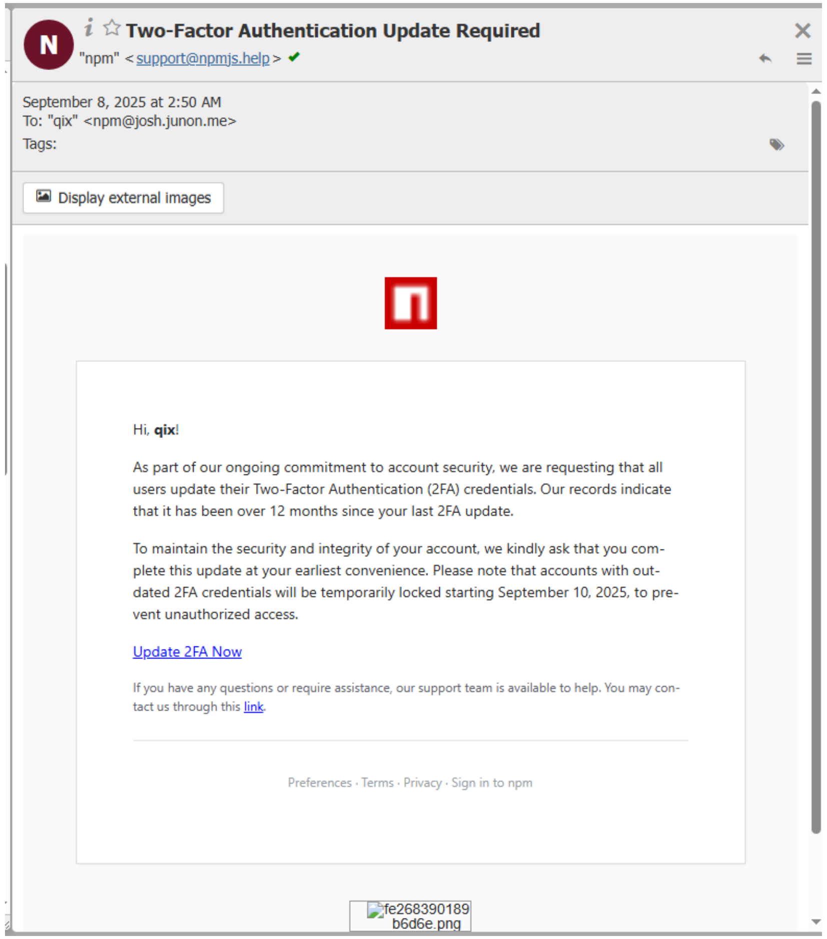
Time to check if you ran any of these 33 malicious Chrome extensions

Two separate campaigns have been stealing credentials and browsing history for months.

DAN GOODIN – 3 JAN 2025 13:15 | 143

Credit: Getty Images

Digital Supply Chain Under Attack



Two-Factor Authentication Update Required

"npm" <support@npmjs.help> ✔

September 8, 2025 at 2:50 AM
To: "qix" <npm@josh.junon.me>
Tags:

Hi, **qix**!

As part of our ongoing commitment to account security, we are requesting that all users update their Two-Factor Authentication (2FA) credentials. Our records indicate that it has been over 12 months since your last 2FA update.

To maintain the security and integrity of your account, we kindly ask that you complete this update at your earliest convenience. Please note that accounts with outdated 2FA credentials will be temporarily locked starting September 10, 2025, to prevent unauthorized access.

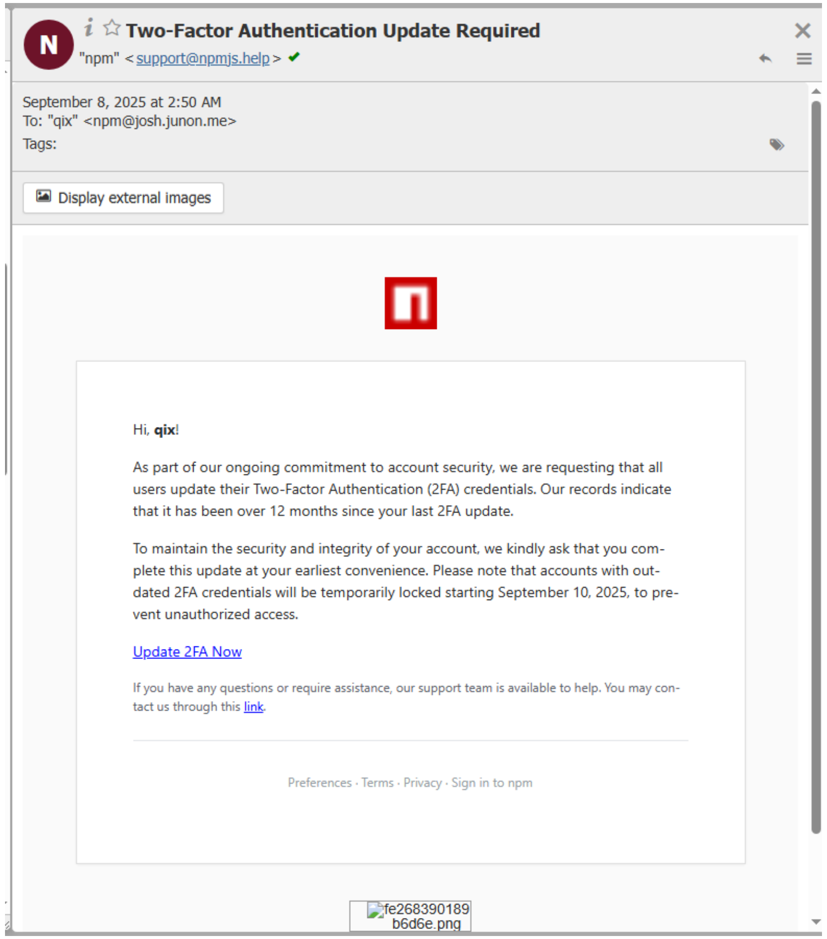
Update 2FA Now

If you have any questions or require assistance, our support team is available to help. You may contact us through this link.

Preferences · Terms · Privacy · Sign in to npm

18 very popular npm packages affected by phishing attack Sept. 8th, 2025

Digital Supply Chain Under Attack



Two-Factor Authentication Update Required

"npm" <support@npmjs.help> ✔

September 8, 2025 at 2:50 AM
To: "qix" <npm@josh.junon.me>
Tags:

Hi, **qix**!

As part of our ongoing commitment to account security, we are requesting that all users update their Two-Factor Authentication (2FA) credentials. Our records indicate that it has been over 12 months since your last 2FA update.

To maintain the security and integrity of your account, we kindly ask that you complete this update at your earliest convenience. Please note that accounts with outdated 2FA credentials will be temporarily locked starting September 10, 2025, to prevent unauthorized access.

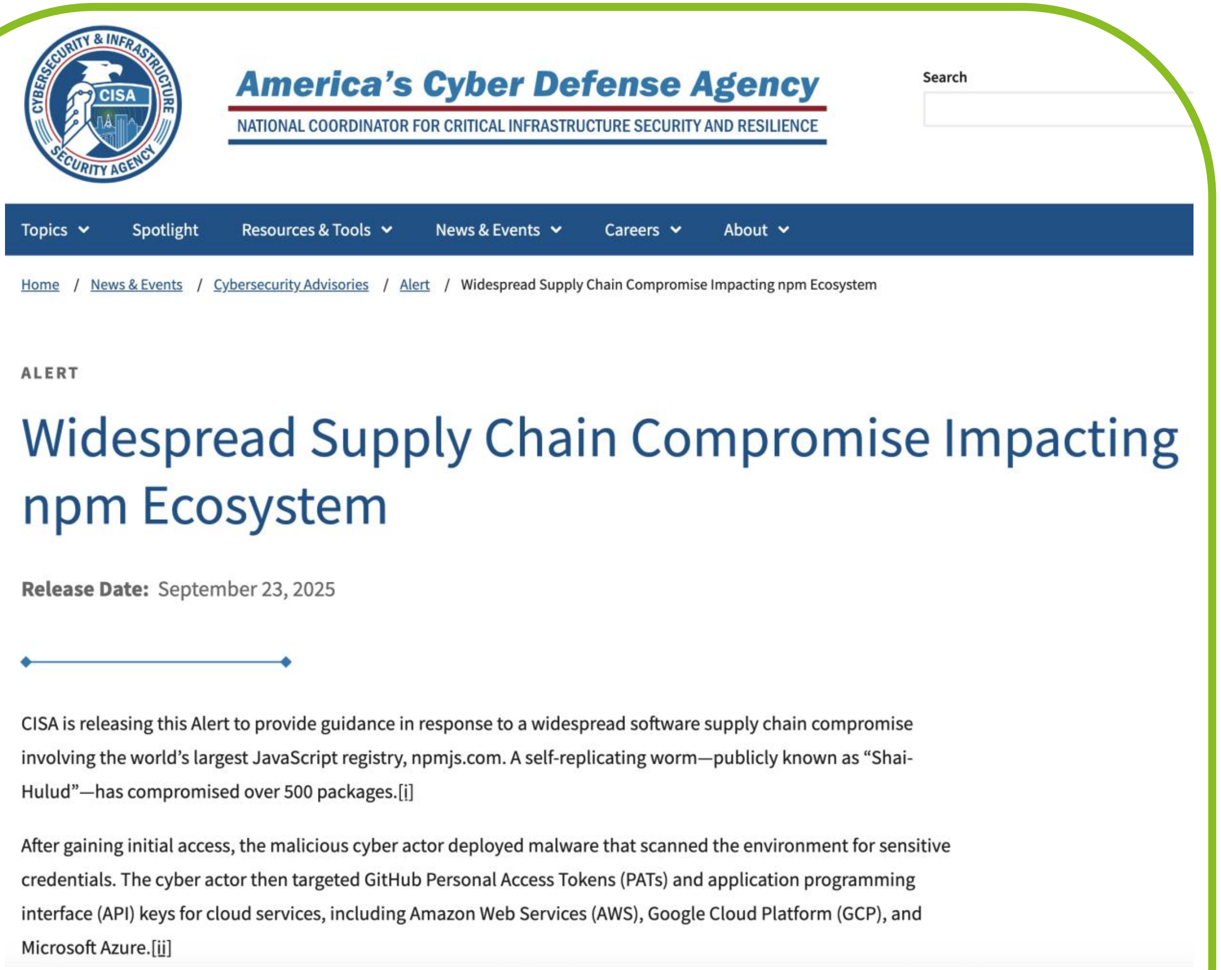
Update 2FA Now

If you have any questions or require assistance, our support team is available to help. You may contact us through this link.

Preferences · Terms · Privacy · Sign in to npm

fe268390189b6d6e.png

18 very popular npm packages affected by phishing attack Sept. 8th, 2025



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Home / News & Events / Cybersecurity Advisories / Alert / Widespread Supply Chain Compromise Impacting npm Ecosystem

ALERT

Widespread Supply Chain Compromise Impacting npm Ecosystem

Release Date: September 23, 2025

CISA is releasing this Alert to provide guidance in response to a widespread software supply chain compromise involving the world's largest JavaScript registry, npmjs.com. A self-replicating worm—publicly known as "Shai-Hulud"—has compromised over 500 packages.[i]

After gaining initial access, the malicious cyber actor deployed malware that scanned the environment for sensitive credentials. The cyber actor then targeted GitHub Personal Access Tokens (PATs) and application programming interface (API) keys for cloud services, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure.[ii]

>500 npm packages manipulated to steal credentials on Sept. 16th, 2025

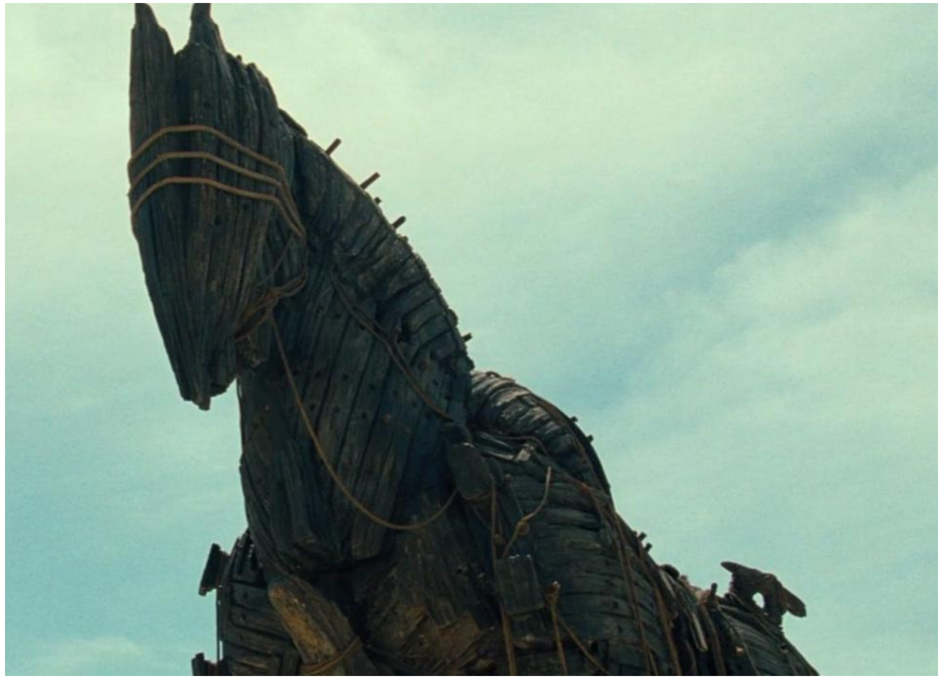
A short history of Cybersecurity

Is IAM proactive enough to defend against modern threats?

1

Network Era

- Attackers actively scan open ports and analyze running software to exploit known vulnerabilities.
- Security efforts focus primarily on protecting the network perimeter.
- Intrusion Detection/Prevention Systems (IDS/IPS) detect and block threats at early stages.



A short history of Cybersecurity

Is IAM proactive enough to defend against modern threats?

1

Network Era

- Attackers actively scan open ports and analyze running software to exploit known vulnerabilities.
- Security efforts focus primarily on protecting the network perimeter.
- Intrusion Detection/Prevention Systems (IDS/IPS) detect and block threats at early stages.

2

Device Era

- Attackers shift to targeting devices to bypass robust network defenses.
- Malware is delivered via email attachments, downloads, and USB drives.
- Endpoint protection technologies improve significantly, making malware detection effective.

3

Identity Era

- The focus moves to the identity layer, enabling access to resources without using malware.
- Identity and Access Management (IAM) systems themselves become targets.

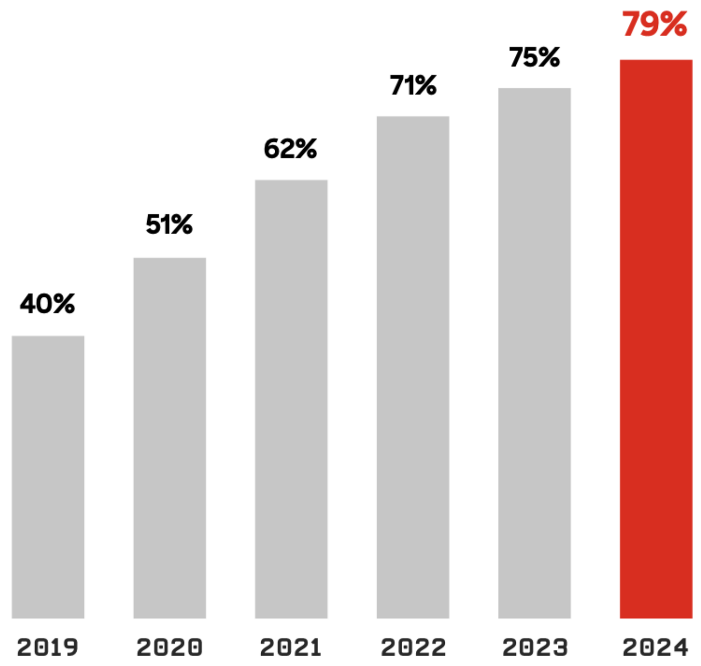


Figure 4. Percentage of detections that were malware-free, 2019-2024

Source: Crowdstrike, Global Threat Report 2025

Identity Access Management – Proactive enough?

Conceptual Challenges

IAM is doing an excellent job in protecting applications

- Enforcing Authentication and MFA
- Providing and managing access rights in a compliant and convenient way
- Joiner, Mover, Leaver and Re-certification ensure that privileges are removed, if not required anymore
- Taking care of machine credentials

Not good in detecting deviations

- e.g. user accounts not part of IAM, detecting additional entry points with locally stored credentials stored

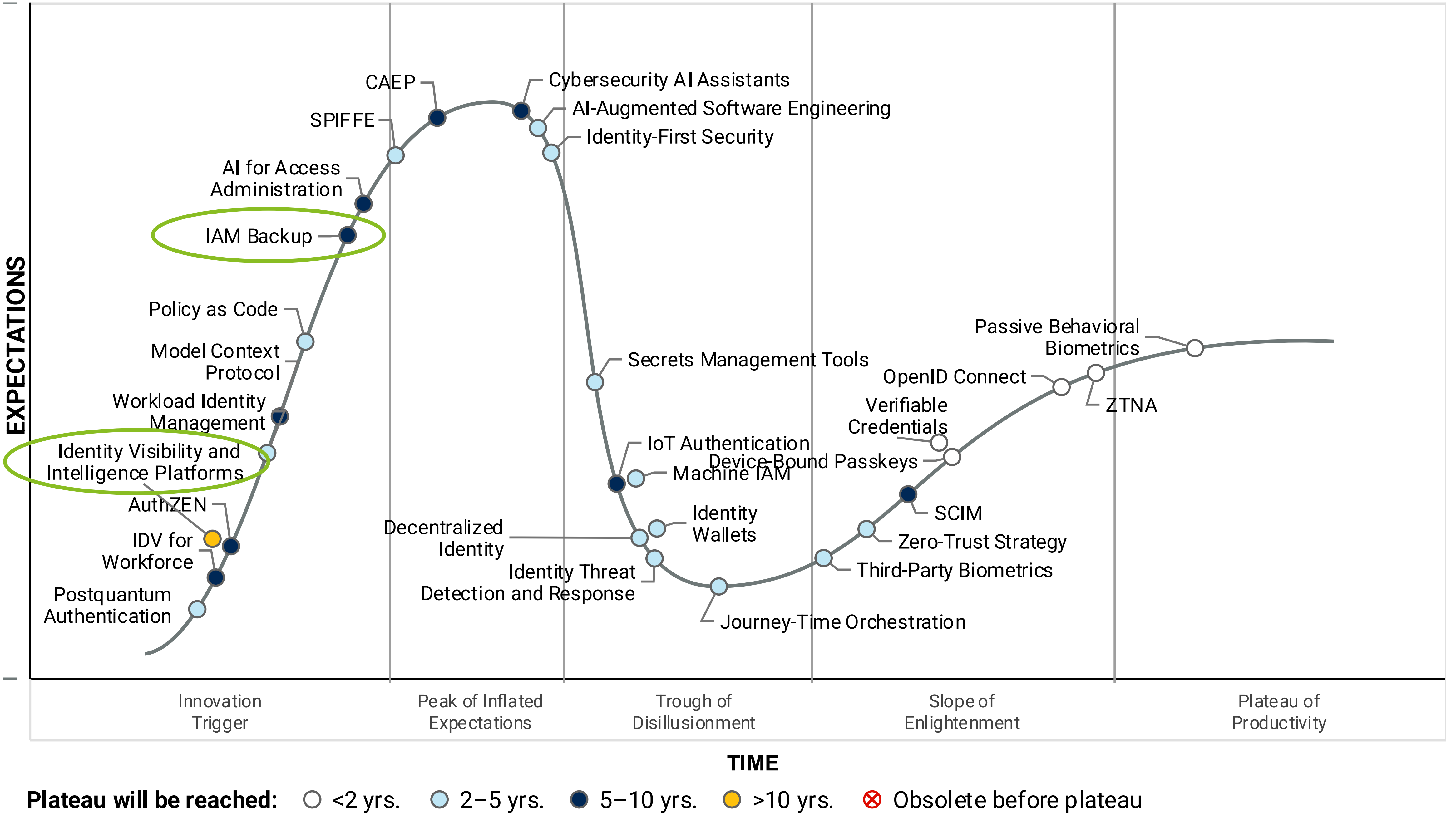
Not good in detecting misuse of sessions (cookies, access/refresh tokens) after the issuance

- Cookies, Access, and Refresh Tokens are vulnerable after issuance
- Many targeted attacks are focusing on the browser context

Agility! Today more important than ever before!

- Software Engineering is rapidly changing – Vibe coding might result in unknown identity risk

Digital Identity and Security 2025 (selected by iCC)



Identity Visibility & Intelligence Platforms

High Demand – Where Organizations Are Investing Now

By 2028, 70% of CISOs will utilize identity visibility and intelligence capabilities to shrink the IAM attack surface.

What IVIP Platforms Do

- Unified visibility across AM, IGA, and PAM silos
- Understanding of the Identity Security Posture
- Aggregate identity data from hybrid environments
- Continuous monitoring (beyond static access reviews)
- AI-enhanced anomaly detection and risk scoring
- Reduce blast radius of credential compromise

Why This Matters

Regulations
GDPR, NIS2, DORA demand continuous identity monitoring

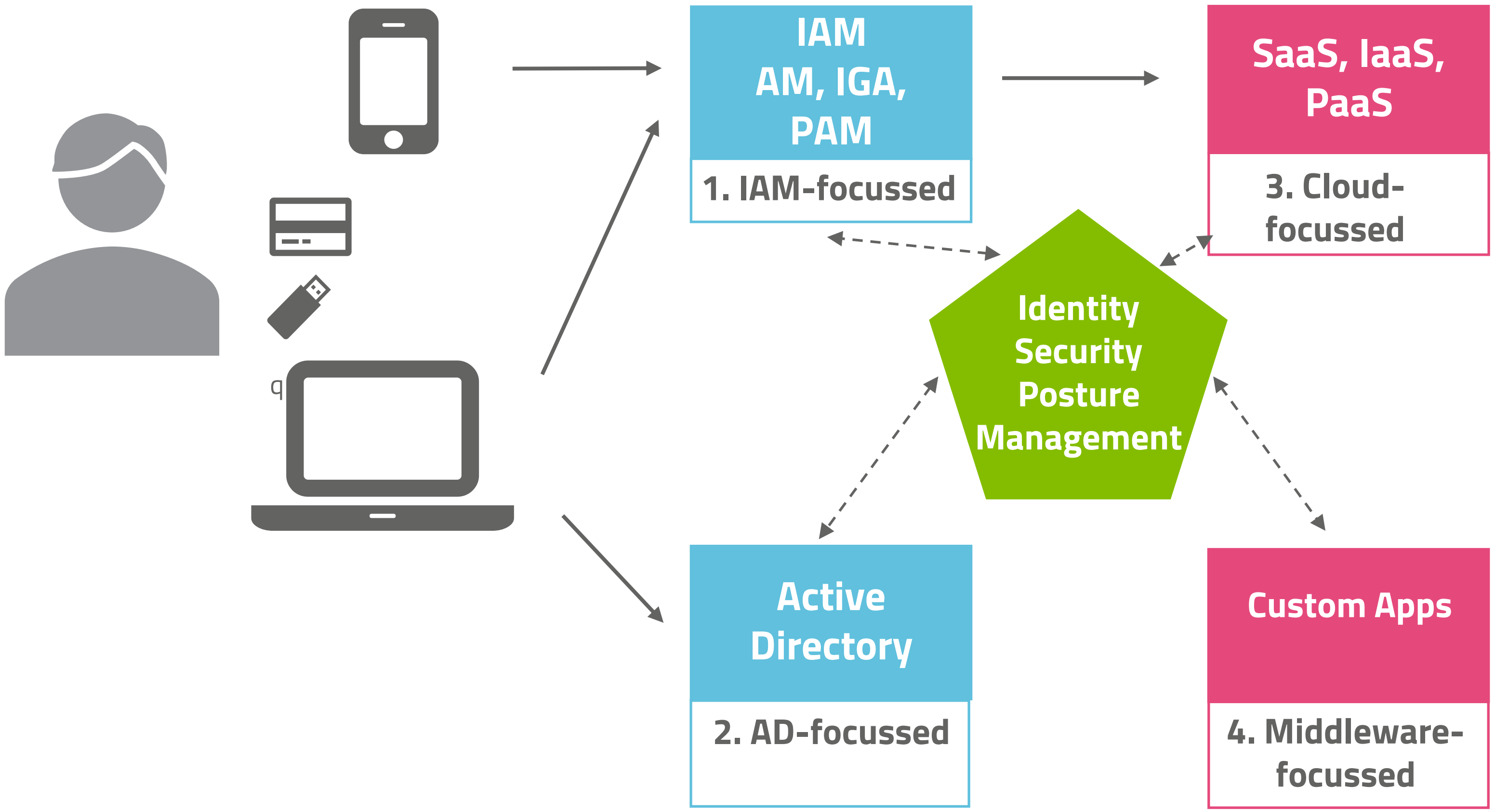
Complexity
Hybrid setups create fragmentation and blind spots

Cost
Prevention via IVIP is far cheaper than breach remediation

Source: Gartner, 2026 Predicts: Identity and Access Management

IVIP / ISPM Architecture Overview

Identity Visibility & Intelligence Platforms – Identity Security Posture Mgt



- Analysis of potential attack paths
- Detection of weak configurations
- Analysis of outliers, privileged users, etc.
- Discovery of accounts
- SoD Violations

Identity Disaster Recovery

Crisis Management for the Identity Layer – an Emerging Priority

What happens when your identity infrastructure is compromised? Most organizations have no answer.

The Problem

- Identity-based attacks are surging
- AD/Entra ID compromise = total lockout
- Traditional DR plans cover infra, not identity
- Recovery without clean identity baseline is guesswork

What Is Needed

- IAM Backup strategies (AD, IGA, AM config)
- Identity-aware incident response playbooks
- Clean room recovery for identity systems
- Automated credential rotation at scale

Apporach

- Assessment: identity DR readiness
- Playbook development for identity crises
- Integration with existing BC/DR programs
- IAM Backup on the Hype Cycle (Peak)

Managed Identity Security Service

IAM Operation Excellence meets Cyber Resilience

Identity Recovery

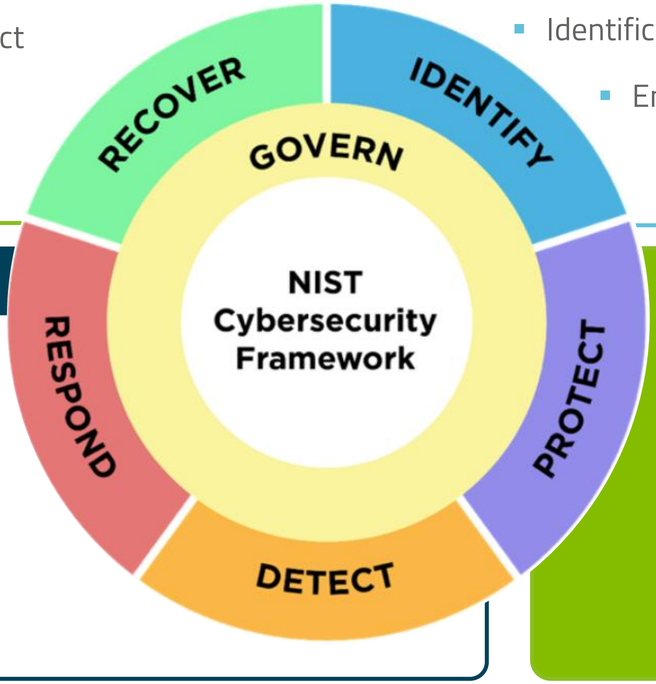
IST CS: Recover

- Focuses on restoring compromised identity repositories, such as Active Directory (AD).
- Identifies and analyzes changes made by attackers to detect unauthorized modifications.
- Ensures secure rollback and removal of malicious changes during the restoration process.

Identity Security Posture Management (ISPM) & IVIP

NIST CS: Identify

- Continuous assessment of identity configurations and policies.
- Identification of vulnerabilities and misconfigurations.
- Ensures compliance and reduces attack surface.



Identity (Threat) Protection

NIST CS: Detect & Respond

- Real-time detection of identity-related threats and anomalies.
- Leverages AI/ML to identify compromised accounts and credential misuse.
- Enables proactive threat mitigation and response.

IAM Core

Service Level Agreement

✓ Flexible service time models
✓ Optional 24/7 on-call availability
✓ Fast response times based on priority
✓ Customizable SLAs to match your business

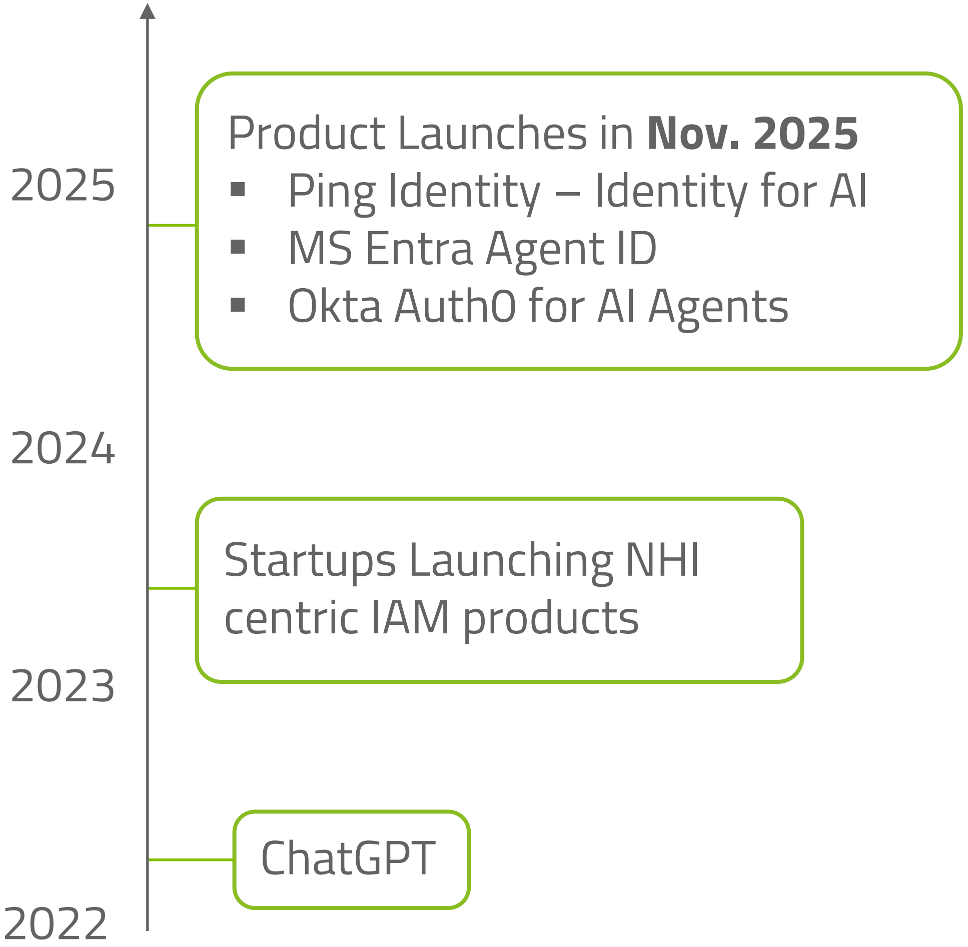
What sets us apart

✓ The same experts who implemented and operated your solution continue to support you.
✓ They know your environment inside out – for faster, smarter, and more effective service.

The CambrAIn Explosion

The CambrAIn Explosion

Identity for AI



2025

Product Launches in **Nov. 2025**

- Ping Identity – Identity for AI
- MS Entra Agent ID
- Okta Auth0 for AI Agents

2024

Startups Launching NHI centric IAM products

2023

ChatGPT

2022

Gartner - Top Security Trends 2026

January 2026

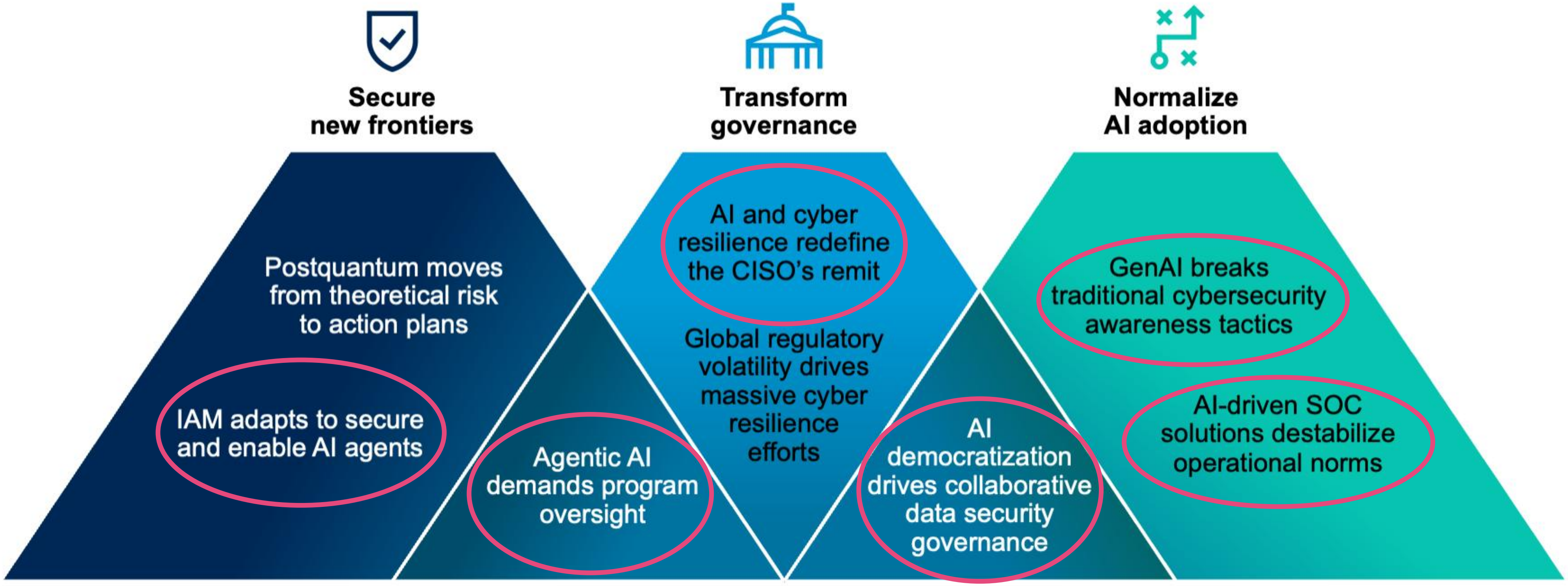
Secure new frontiers

Transform governance

Normalize AI adoption

Gartner - Top Security Trends 2026

January 2026



Secure new frontiers

Postquantum moves from theoretical risk to action plans

IAM adapts to secure and enable AI agents

Agentic AI demands program oversight

Transform governance

AI and cyber resilience redefine the CISO's remit

Global regulatory volatility drives massive cyber resilience efforts

AI democratization drives collaborative data security governance

Normalize AI adoption

GenAI breaks traditional cybersecurity awareness tactics

AI-driven SOC solutions destabilize operational norms

— AI-related Trend

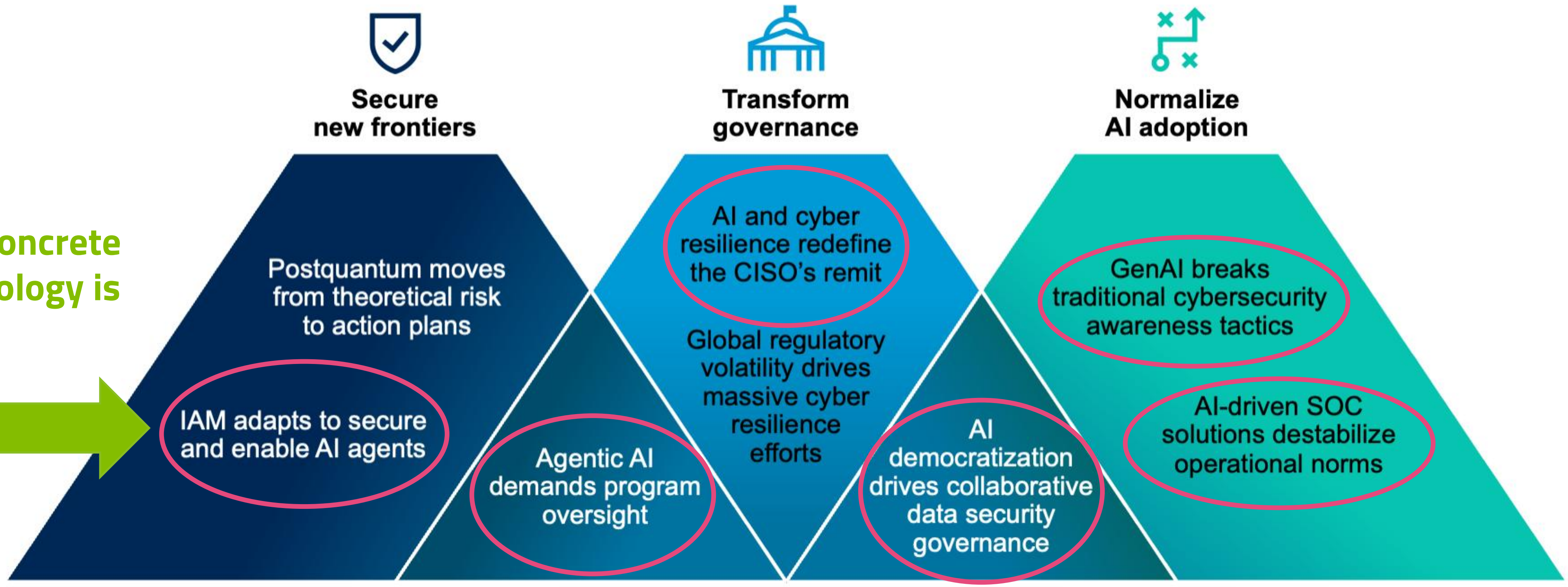
Gartner

Source: Gartner
840672

Gartner - Top Security Trends 2026

January 2026

Only concrete Technology is IAM



Secure new frontiers

Postquantum moves from theoretical risk to action plans

IAM adapts to secure and enable AI agents

Agentic AI demands program oversight

Transform governance

AI and cyber resilience redefine the CISO's remit

Global regulatory volatility drives massive cyber resilience efforts

AI democratization drives collaborative data security governance

Normalize AI adoption

GenAI breaks traditional cybersecurity awareness tactics

AI-driven SOC solutions destabilize operational norms

▬ **AI-related Trend**

Gartner

Source: Gartner
840672

The Spectrum of Autonomy

Type of AI Agents

ASSISTIVE AGENTS

(Copilots)

Operate within a human user's session. They "borrow" user context. Security focuses on delegation and preserving intent.

AUTONOMOUS AGENTS

(Agentic AI)

Perform asynchronous tasks without human presence. Require independent Agent Identities. Actions are nondeterministic.

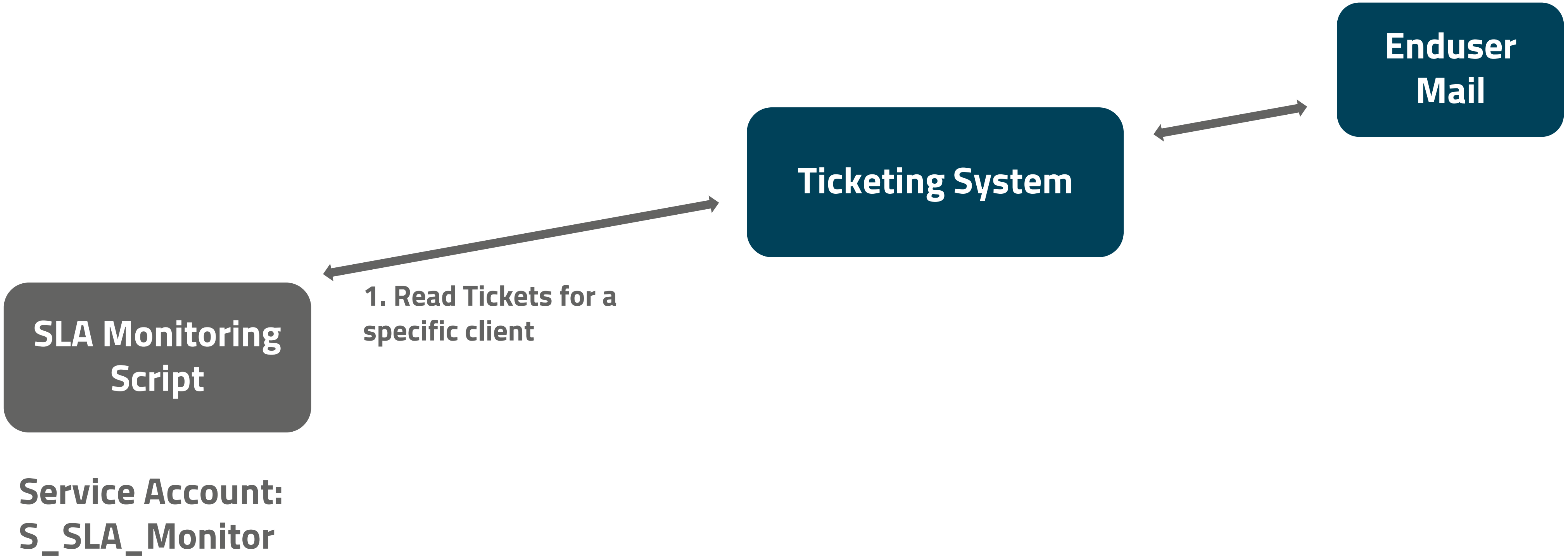
AGENTIC USERS

(Digital Employees)

Treats an agent as a "User" in the directory: capable of having a mailbox, attending meetings and appearing in org charts.

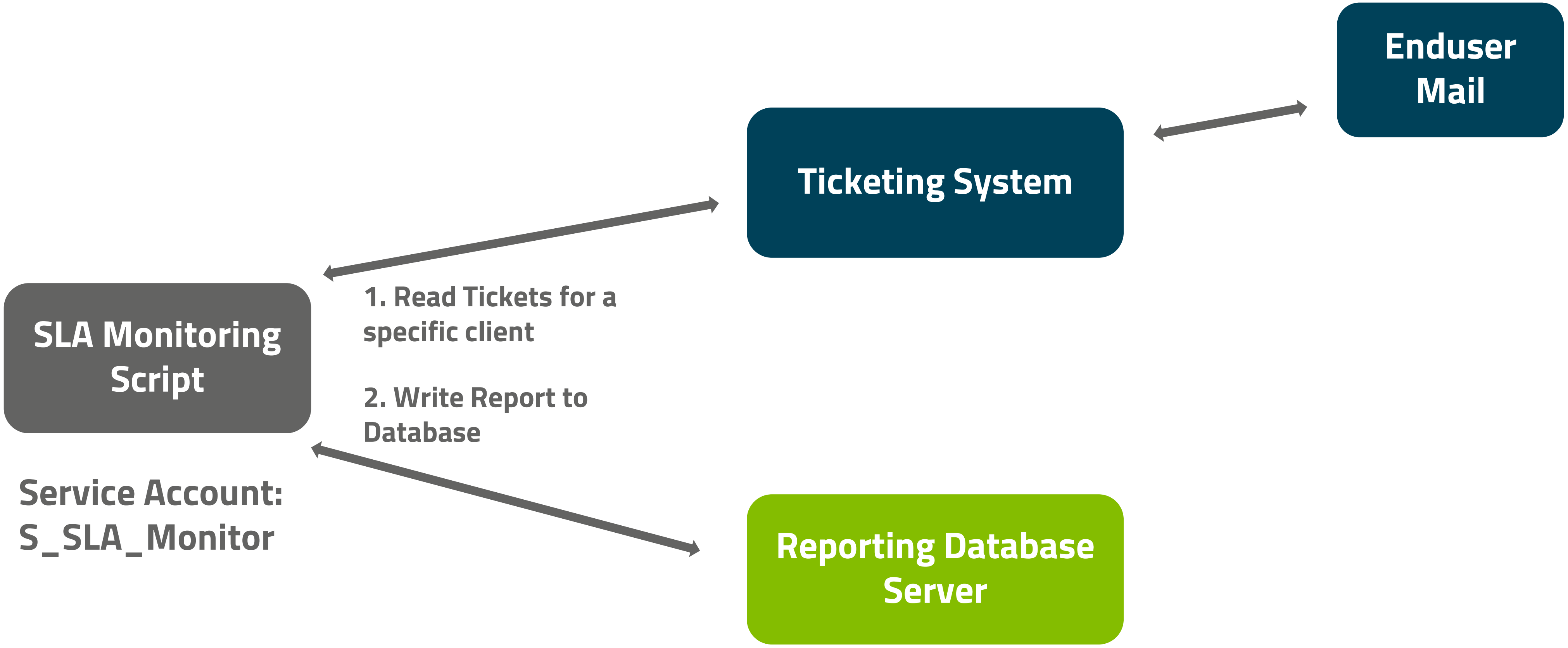
The „Traditional“ World

Scripts and Service Accounts


Enduser Mail
Ticketing System
SLA Monitoring Script
1. Read Tickets for a specific client
Service Account: S_SLA_Monitor

The „Traditional" World

Scripts and Service Accounts


Enduser Mail
Ticketing System
SLA Monitoring Script
1. Read Tickets for a specific client
2. Write Report to Database
Service Account: S_SLA_Monitor
Reporting Database Server

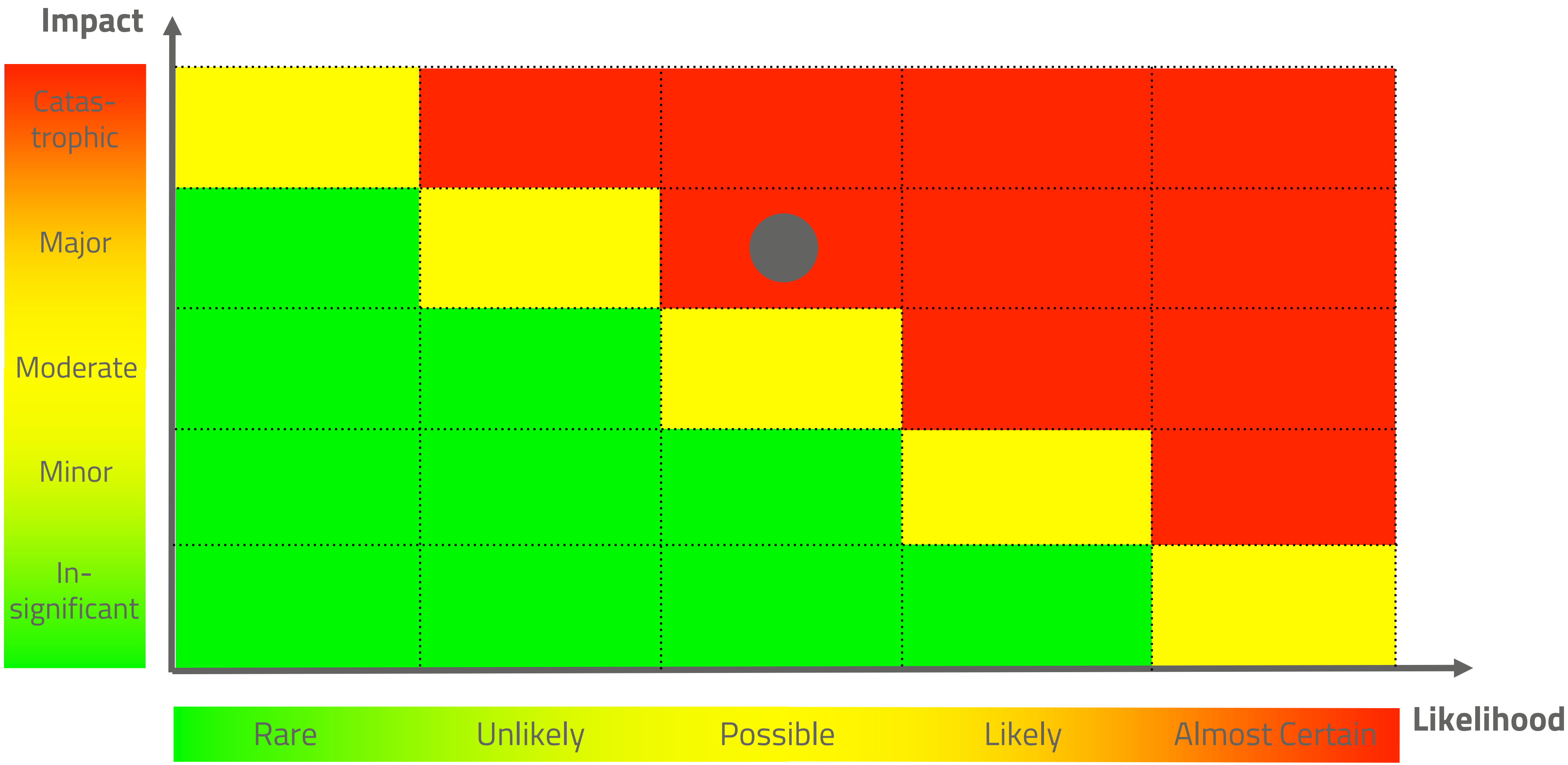
S_SLA_Monitor has privileges to **read/insert/update/delete/drop!**

Risks - Service Accounts and Scripts

Identity Risk Management

← Mitigations

● Business Risk

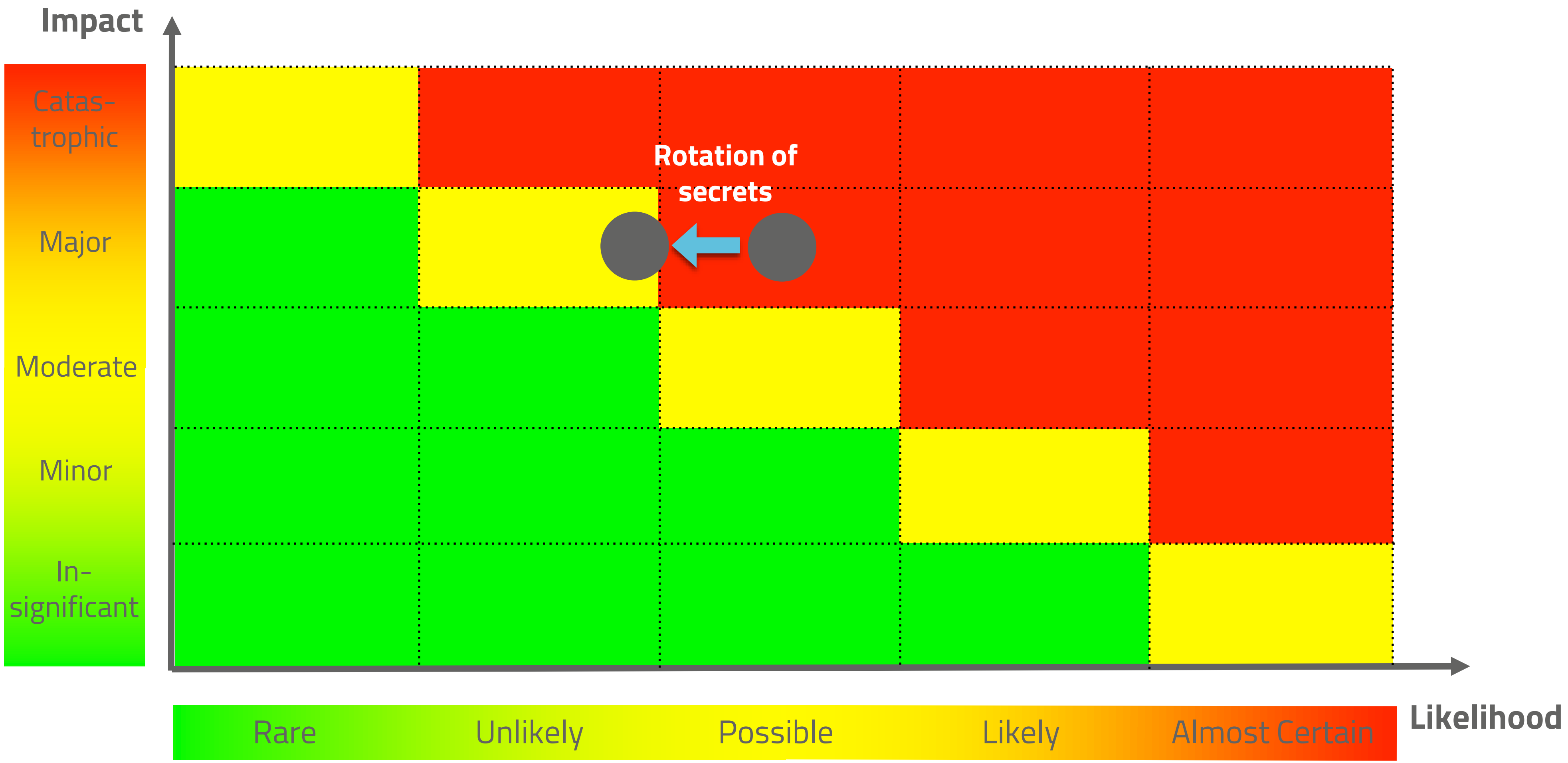


Risks - Service Accounts and Scripts

Identity Risk Management

← Mitigations

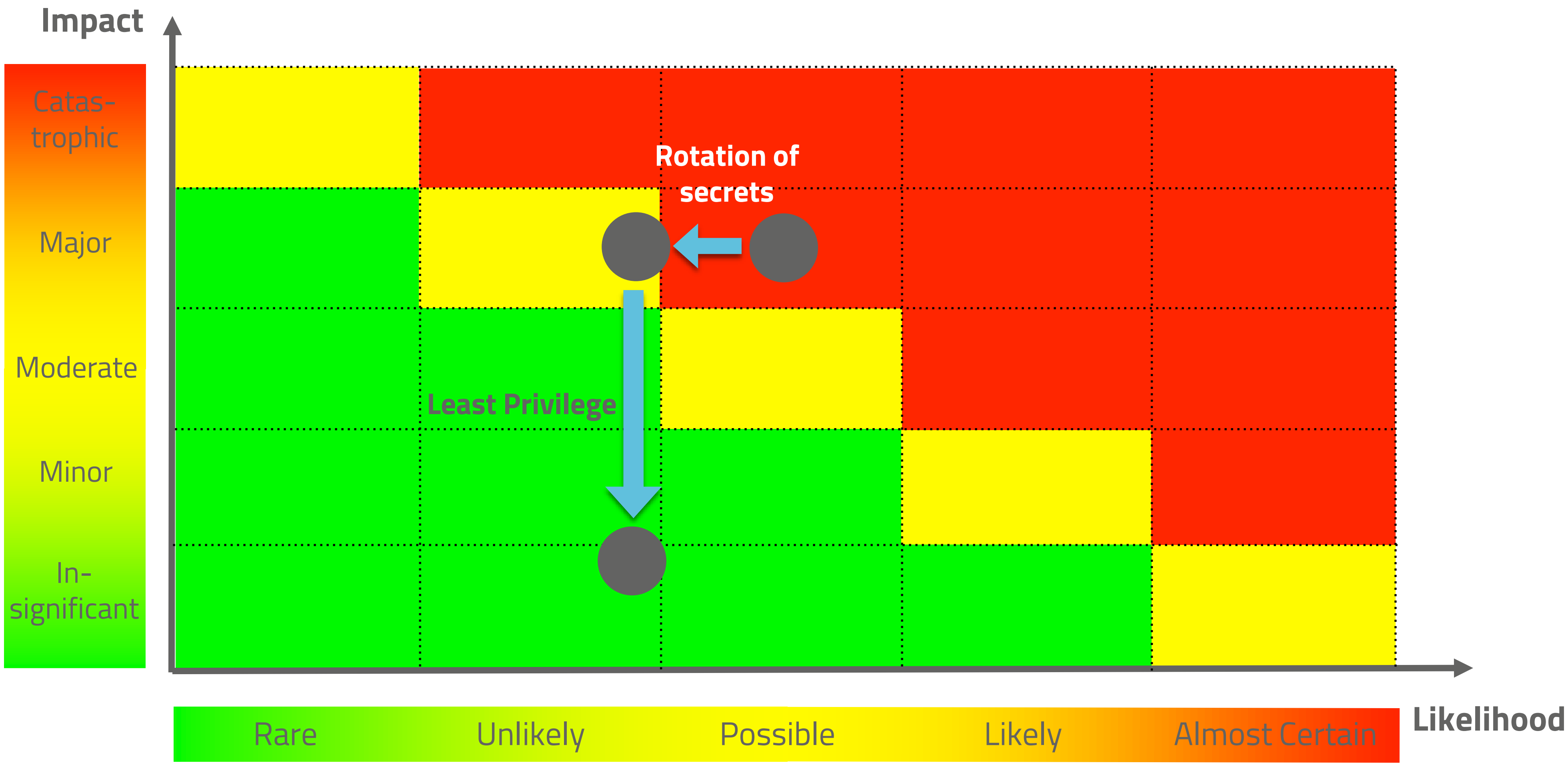
● Business Risk



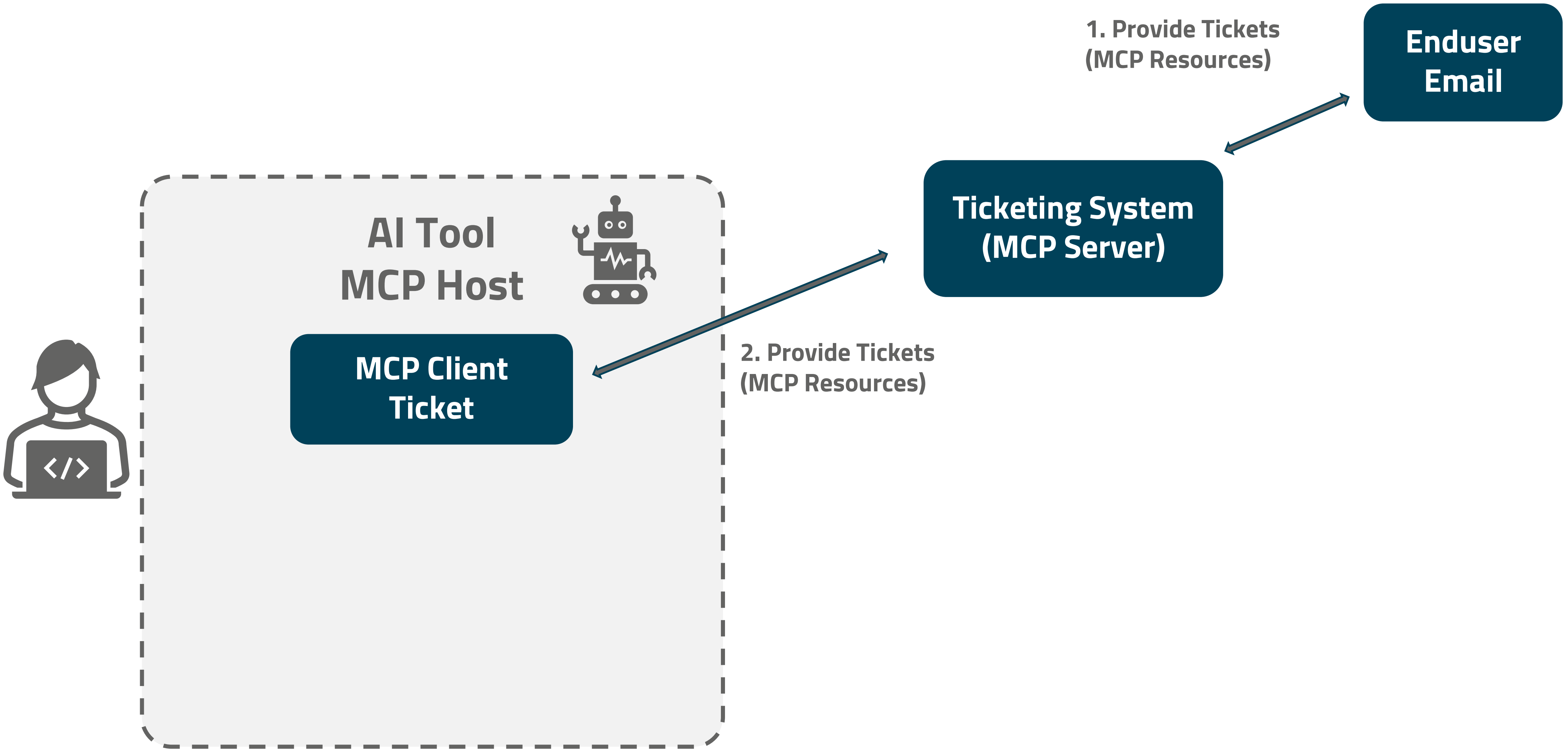
Risks - Service Accounts and Scripts

Identity Risk Management

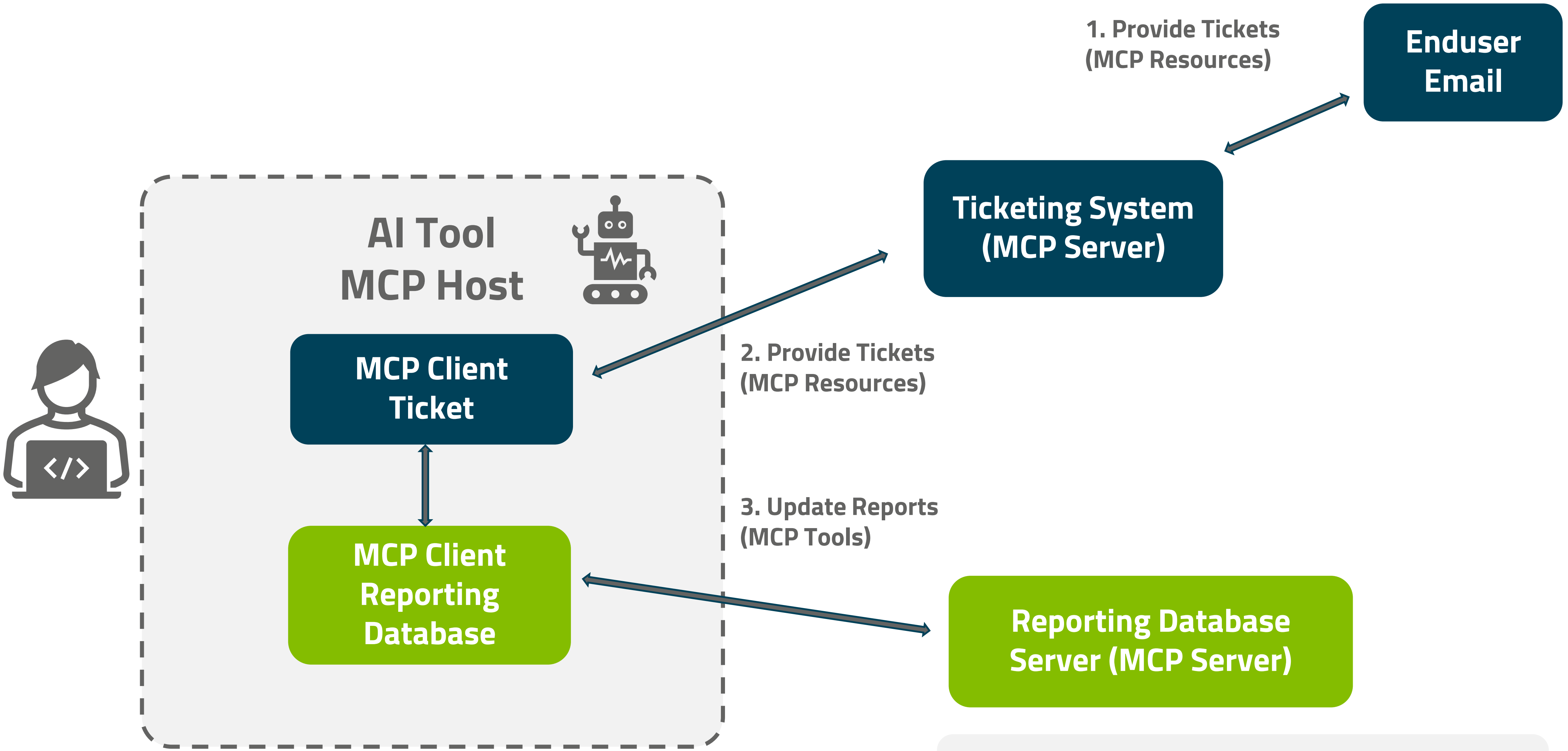
Mitigations
Business Risk



Model Context Protocol

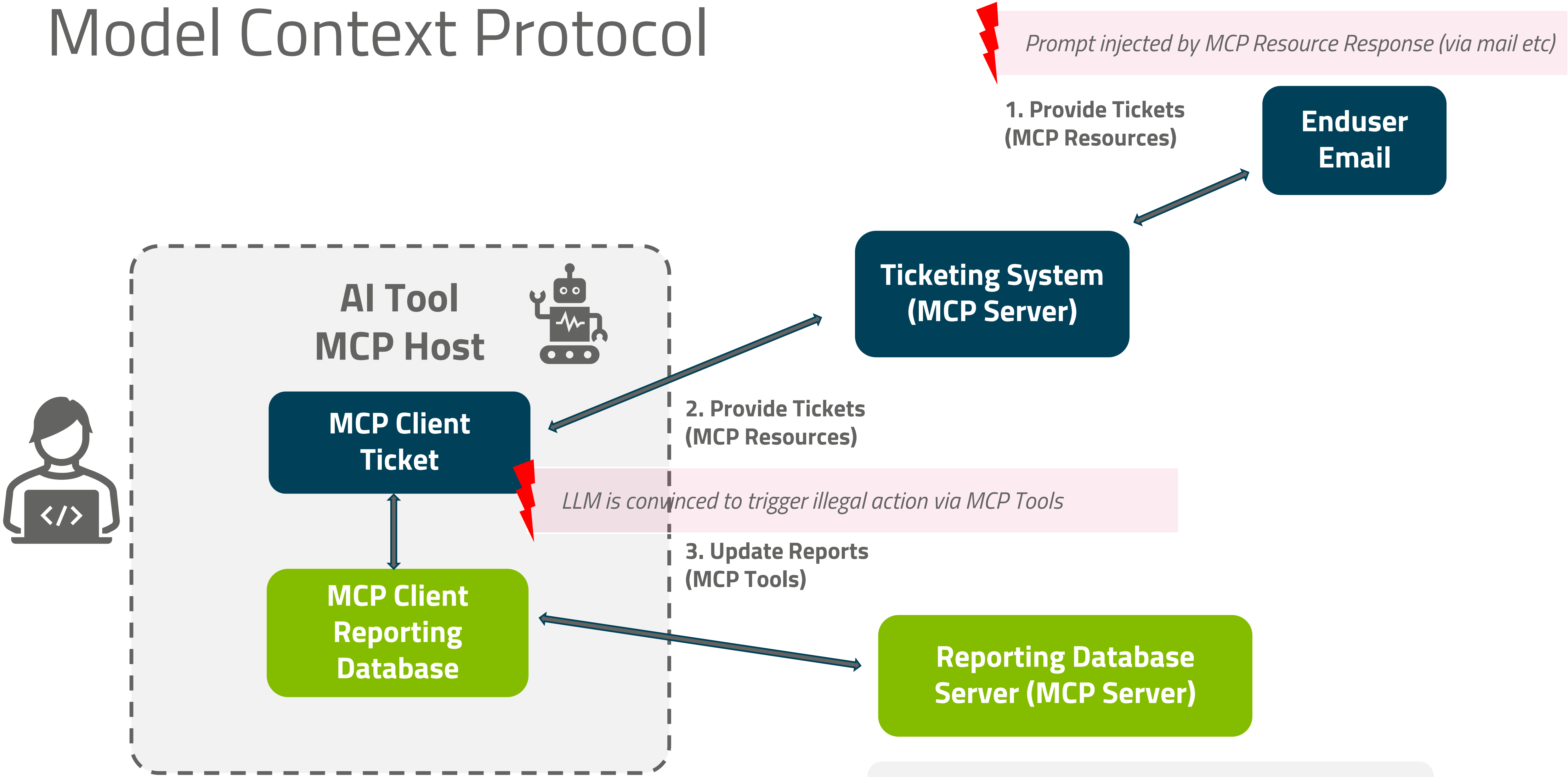


Model Context Protocol



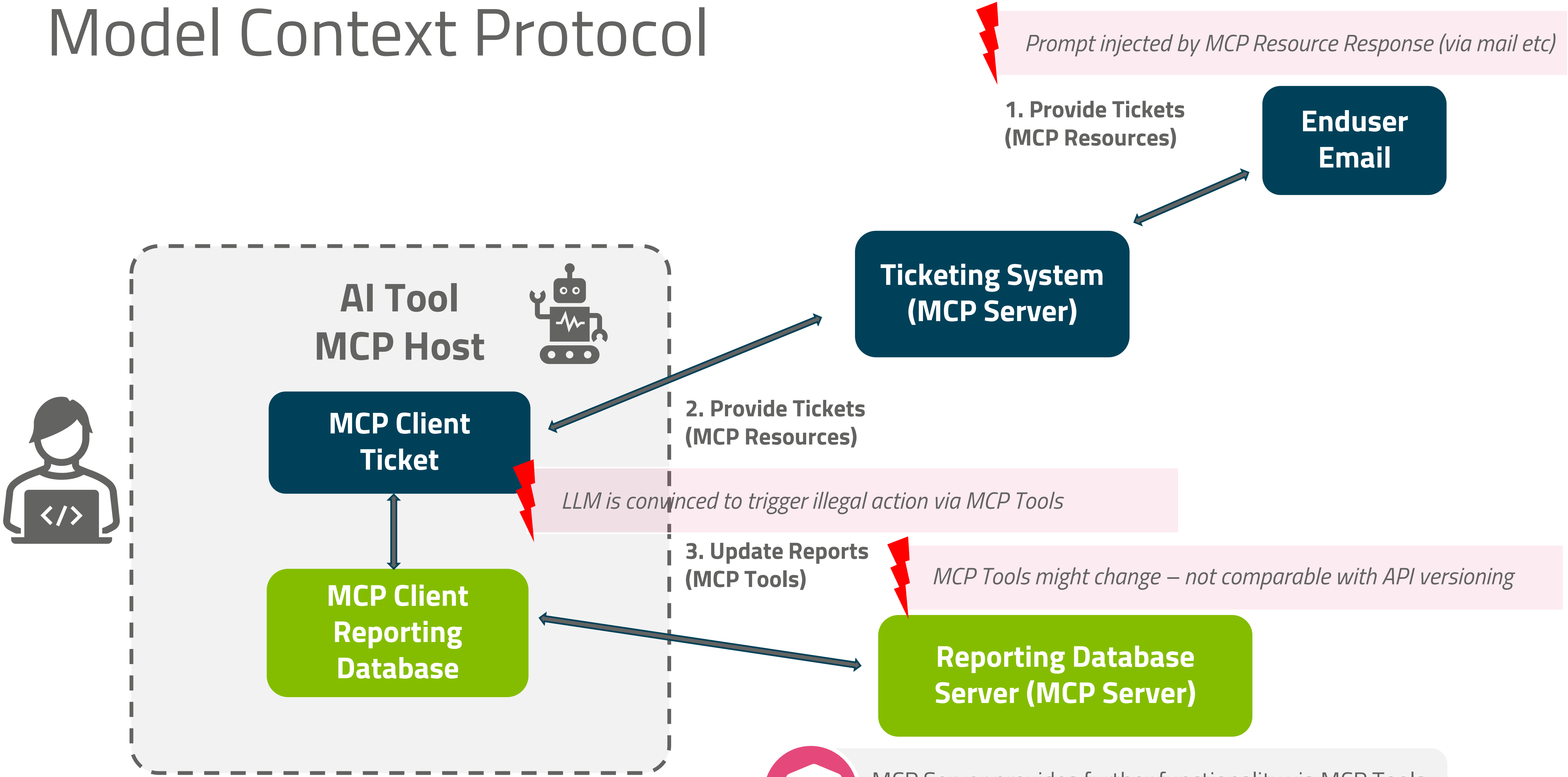
MCP Server provides update reports functionality via MCP Tools

Model Context Protocol


Prompt injected by MCP Resource Response (via mail etc)
1. Provide Tickets (MCP Resources)
Enduser Email
Ticketing System (MCP Server)
AI Tool MCP Host
MCP Client Ticket
2. Provide Tickets (MCP Resources)
LLM is convinced to trigger illegal action via MCP Tools
3. Update Reports (MCP Tools)
MCP Client Reporting Database
Reporting Database Server (MCP Server)

MCP Server provides update reports functionality via MCP Tools

Model Context Protocol



Prompt injected by MCP Resource Response (via mail etc)

1. Provide Tickets (MCP Resources)

Enduser Email

Ticketing System (MCP Server)

AI Tool MCP Host

MCP Client Ticket

2. Provide Tickets (MCP Resources)

LLM is convinced to trigger illegal action via MCP Tools

3. Update Reports (MCP Tools)

MCP Tools might change – not comparable with API versioning

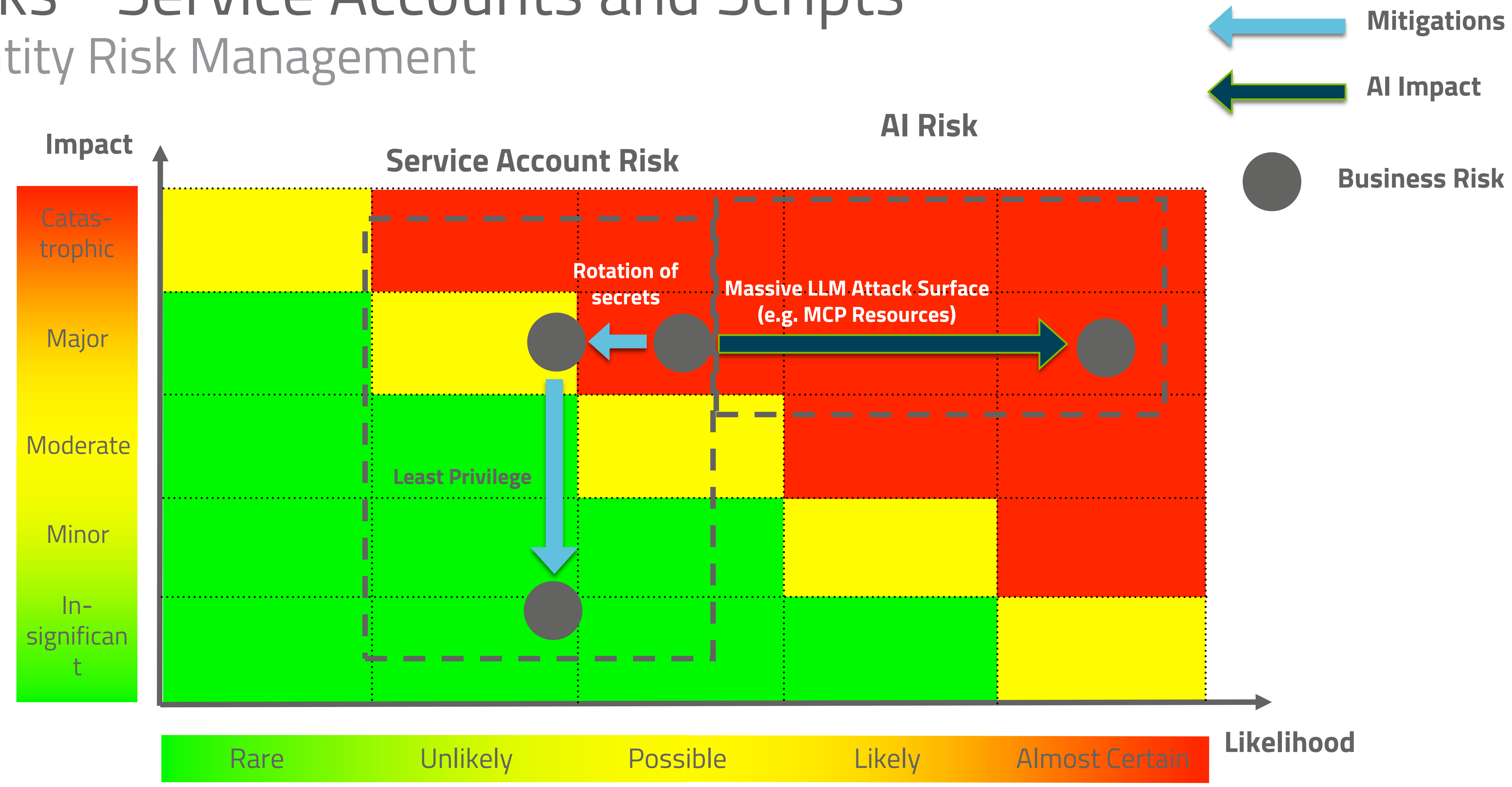
MCP Client Reporting Database

Reporting Database Server (MCP Server)

MCP Server provides further functionality via MCP Tools (e.g. deletion, manipulation, and reading of reports)

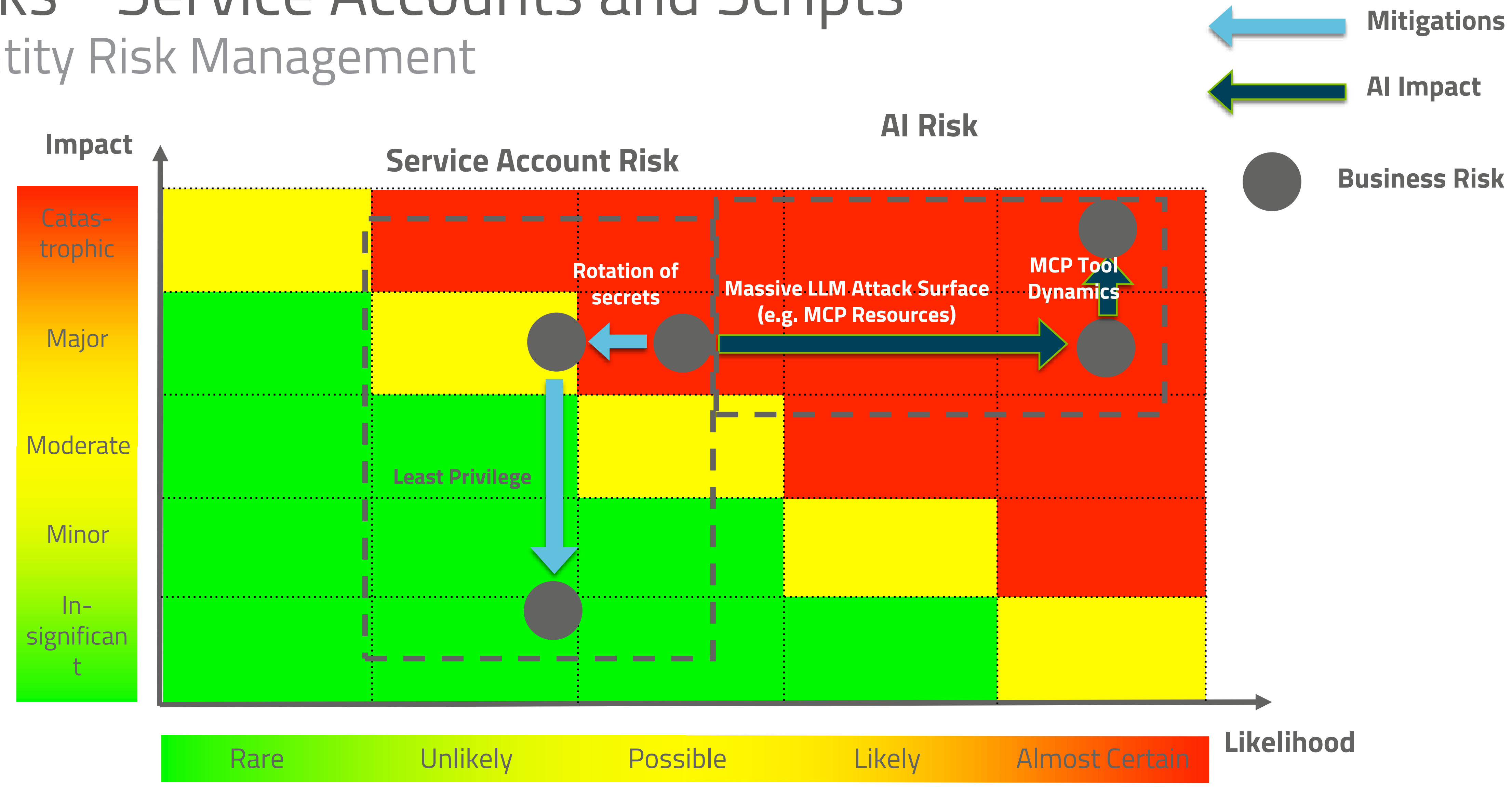
Risks - Service Accounts and Scripts

Identity Risk Management



Risks - Service Accounts and Scripts

Identity Risk Management



Real-World MCP Security Incidents

Prompt Injection, Supply Chain Risks & Broken Access Control in the Wild

01 Anthropic

SQL Injection via MCP

Reference SQLite server contained a SQL injection vulnerability, allowing attackers to store malicious prompts in the database.

Agents executed these prompts during data retrieval, resulting in data theft and unauthorized actions.

Data Exfiltration
Unauthorized Actions

02 Atlassian

Prompt Injection via Jira

Jira Service Management integration faced prompt injection attacks — malicious instructions were embedded in support tickets.

AI agents processed the tickets and executed unauthorized commands, leading to privilege escalation and backend tool misuse.

Privilege Escalation
Backend Tool Misuse

03 Asana

Multi-Tenant Access Failure

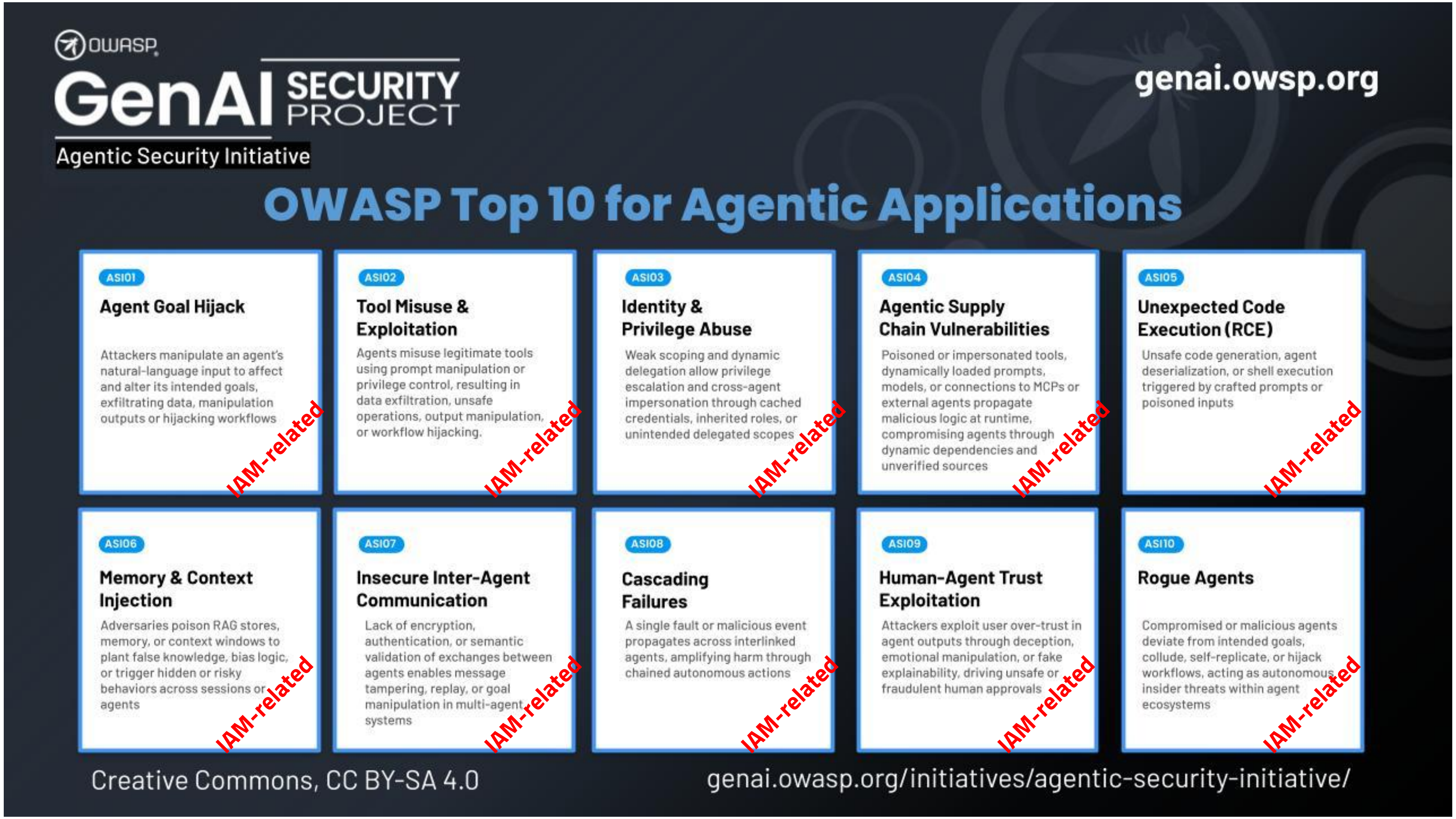
Shared infrastructure lacked proper token isolation, allowing an AI agent from one customer to access data belonging to another.

Sensitive project and user information across multiple tenants was exposed.

Cross-Tenant Data Exposure
Broken Access Control

OWASP Top 10 for Agentic Applications

Published Dec. 2025



OWASP GenAI SECURITY PROJECT

Agentic Security Initiative

genai.owsp.org

OWASP Top 10 for Agentic Applications

ASI01

Agent Goal Hijack

Attackers manipulate an agent's natural-language input to affect and alter its intended goals, exfiltrating data, manipulation outputs or hijacking workflows

IAM-related

ASI02

Tool Misuse & Exploitation

Agents misuse legitimate tools using prompt manipulation or privilege control, resulting in data exfiltration, unsafe operations, output manipulation, or workflow hijacking.

IAM-related

ASI03

Identity & Privilege Abuse

Weak scoping and dynamic delegation allow privilege escalation and cross-agent impersonation through cached credentials, inherited roles, or unintended delegated scopes

IAM-related

ASI04

Agentic Supply Chain Vulnerabilities

Poisoned or impersonated tools, dynamically loaded prompts, models, or connections to MCPs or external agents propagate malicious logic at runtime, compromising agents through dynamic dependencies and unverified sources

IAM-related

ASI05

Unexpected Code Execution (RCE)

Unsafe code generation, agent deserialization, or shell execution triggered by crafted prompts or poisoned inputs

IAM-related

ASI06

Memory & Context Injection

Adversaries poison RAG stores, memory, or context windows to plant false knowledge, bias logic, or trigger hidden or risky behaviors across sessions or agents

IAM-related

ASI07

Insecure Inter-Agent Communication

Lack of encryption, authentication, or semantic validation of exchanges between agents enables message tampering, replay, or goal manipulation in multi-agent systems

IAM-related

ASI08

Cascading Failures

A single fault or malicious event propagates across interlinked agents, amplifying harm through chained autonomous actions

IAM-related

ASI09

Human-Agent Trust Exploitation

Attackers exploit user over-trust in agent outputs through deception, emotional manipulation, or fake explainability, driving unsafe or fraudulent human approvals

IAM-related

ASI10

Rogue Agents

Compromised or malicious agents deviate from intended goals, collude, self-replicate, or hijack workflows, acting as autonomous insider threats within agent ecosystems

IAM-related

genai.owasp.org/initiatives/agentic-security-initiative/

Key Initiatives

1. Discovery
2. Lifecycle (Ownership,…)
   Long-lived
   Temporary
3. Authentication / (SPIFFE)
4. Privileges / Authorization
   - On-Behalf-of
   - Authorization / Micro-Approval
   - Scope - Least Privilege
   - OAuth Extensions (Token Exchange, XAA, PAR/RAR,..)
   - CAEP
5. AI - Protocol Security (MCP, A2A,…)
6. ITDR

OAuth Foundation

- Build the foundation
- Define a roadmap to bring required extensions into production

Authorization Layer

- Fine-grained authorization is required to build guardrails for agents
- OpenID AuthZen is progressing fast

ISPM

- Agent Discovery and Identification is required to build a robust governance layer
- First ISPM Tools are releasing required features

Andre Priebe
Chief Technology Officer
Andre.Priebe@ic-consult.com
+49 172 1425576

iC Consult | sales@ic-consult.com | www.ic-consult.com
The Leader in Identity Security