



CYBERARK®
THE IDENTITY SECURITY COMPANY®

CyberArk Machine Identities (Secrets, Certificates)

Daniel Hetenyi



2024 breaches in numbers

Verizon 2024 Data Breach report

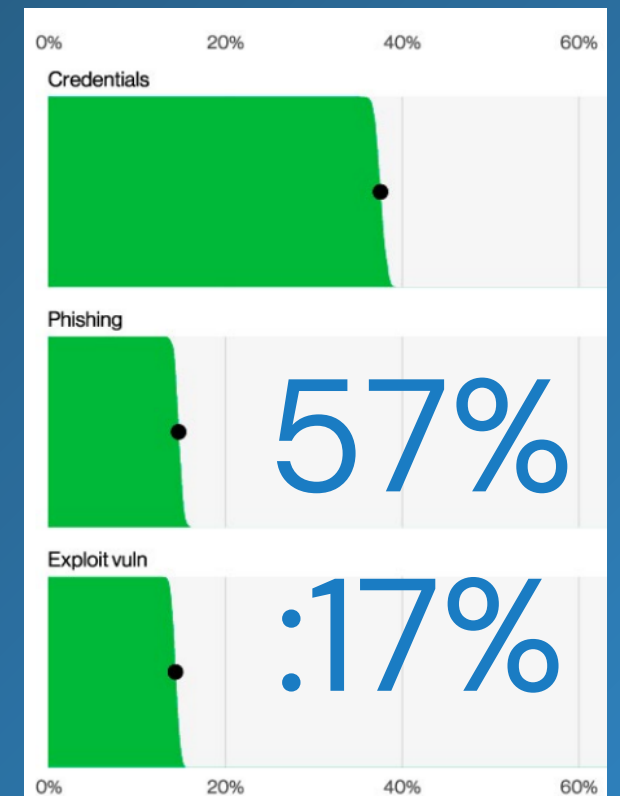
Human Element

68%

Ransomware Extortion

32%

Login vs. vulnerability



<https://www.verizon.com/business/resources/T7b0/reports/2024-dbir-data-breach-investigations-report.pdf>

New Environments Create New Attack Methods

Compromised identities and credentials remain a constant target in cyber attacks.

Malicious Actors

Internal Threats

External Threats

Identities

IT

Developers

Workforce

Machines

Enterprise Resources

Lateral & Vertical Movement

On-Prem

Cloud

DevOps

SaaS

Actions on Objectives

Execute Endgame

Data Exfiltration

Establish Backdoors

Deploy Ransomware

Service Disruption

Credential Theft

Privilege Escalation & Abuse

Understanding the Attack Chain

How do we defend against this attack path?

Identity Compromise (Credential theft)

- Single Sign-On
- Passwordless Authentication
- Adaptive Multifactor Authentication
- Session-less Cookies
- Browser Cookie Protection
- Credential Store Protection
- Complex Passwords/Secrets
- Password/Secret Vaulting
- Password/Secret Rotation
- Credential & Session Isolation
- Removal of Hard-Coded Credentials

Lateral and Vertical Movement

- Zero Standing Privilege
- Just-In-Time Access
- Role-Based Access Control
- Limit Scope of Influence (Blast Radius)
- Randomize/Unique Local Credentials
- Session Protection
- Session Isolation
- Session Monitoring & Analytics
- Identity Threat Detection & Response
- Application Control

Privilege Escalation and Abuse

- Continuous Authentication
- Time-Bound Access
- Session Monitoring & Analytics
- Audit Logging & Session Recording
- Identity Threat Detection & Response
- Privilege Analysis
- Least Privilege Enforcement
- Lifecycle Management
- Compliance Campaigns
- Application Control

Gartner Top 2025 Trends

1. GenAI Data Security Programs – protecting unstructured data

2. Managing Machine Identities

- Rise of machines – 82:1 machine identities vs. humans
- Only 44% of IAM teams are responsible for machine identities
- Zilla: 84% of organizations still rely on manual IGA

3. Tactical AI – initiatives re-prioritization

4. Cybersecurity technology optimization

1. Platformization
 2. Balance between costs, architecture, operations
5. Extending security behavior and culture
6. Addressing Cybersecurity Burnout

<https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025>

Solutions for Securing **Every Identity**



Workforce



IT



Developers



Machines

IDENTITY SECURITY

Securing Workforce Users

Securing High Risk Users

Securing IT Admins

Securing Cloud Operations Teams

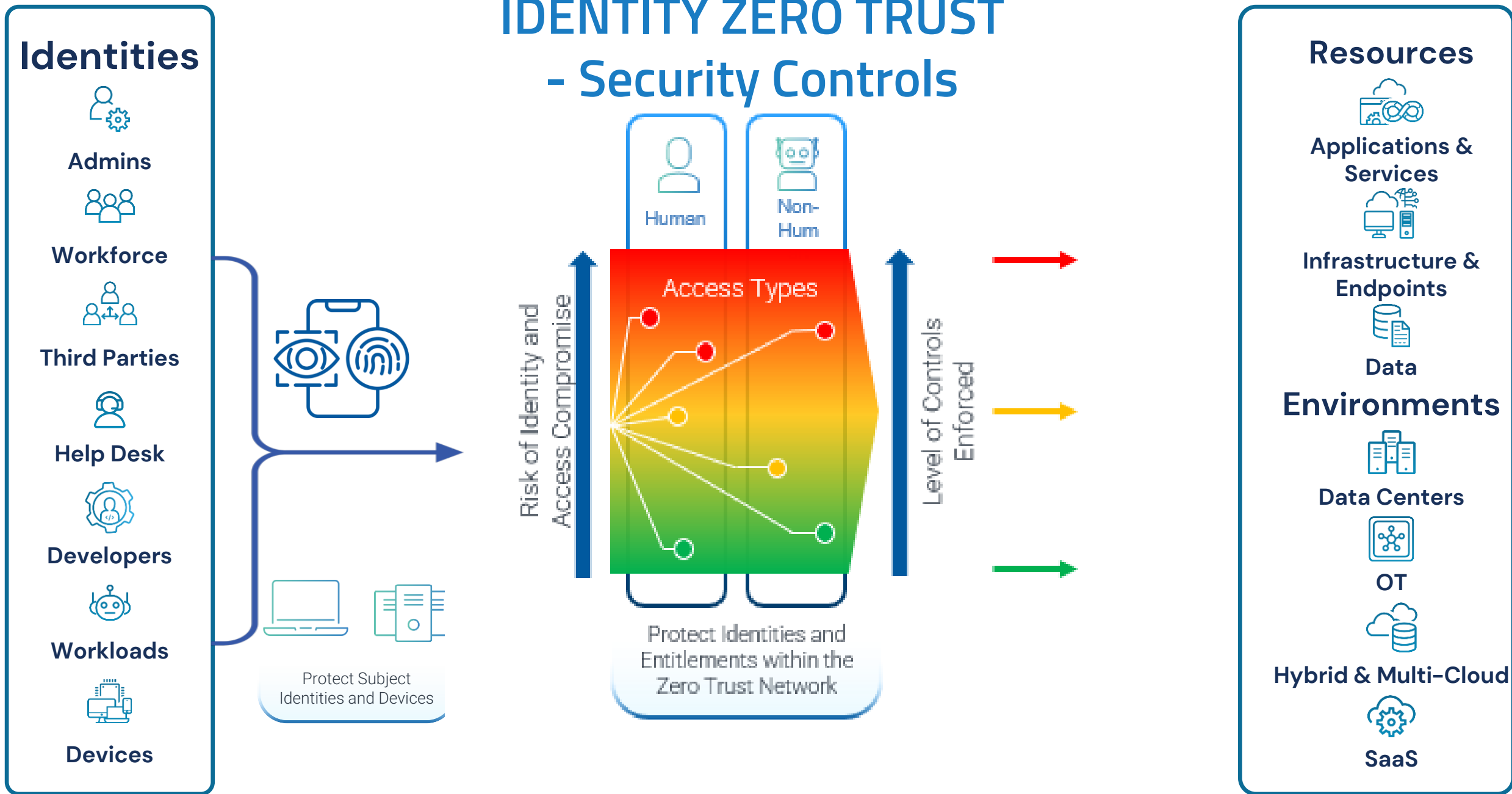
Securing Developers

Securing Machine Identities

Securing Secrets for Hybrid IT

Secure Desktops & Servers

IDENTITY ZERO TRUST - Security Controls



A Zero Trust posture requires people, processes and technology.

Enterprises Must Secure Two Types Of Identities



PEOPLE

Username and Passwords



MACHINES

Machine Identities



Just securing humans is not enough!

Unsecured Machine Identities expose the whole enterprise



Observe, assess risk from, and secure machine identities.



Eliminate the risk from compromised machine identities.



Ensure secure access between machines.

PROBLEMS TO SOLVE

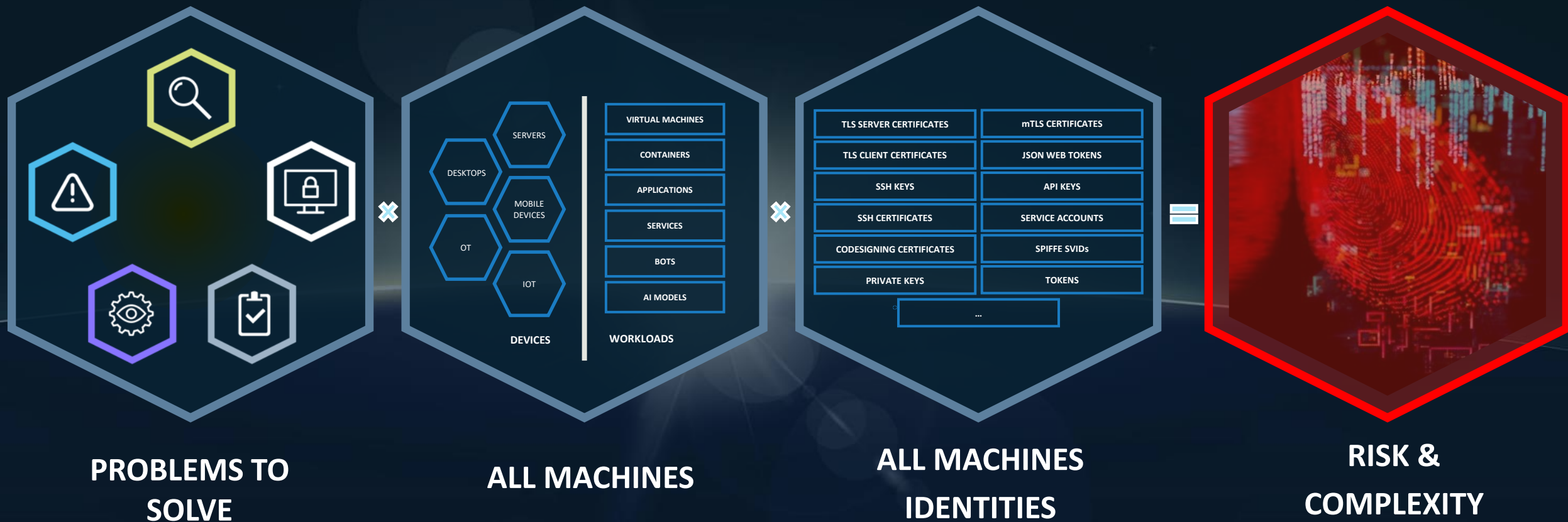


Make lifecycle management of machine identities automated and transparent.



Meet security policy, compliance and regulatory needs.

Across The Full Spectrum of Machine Identities

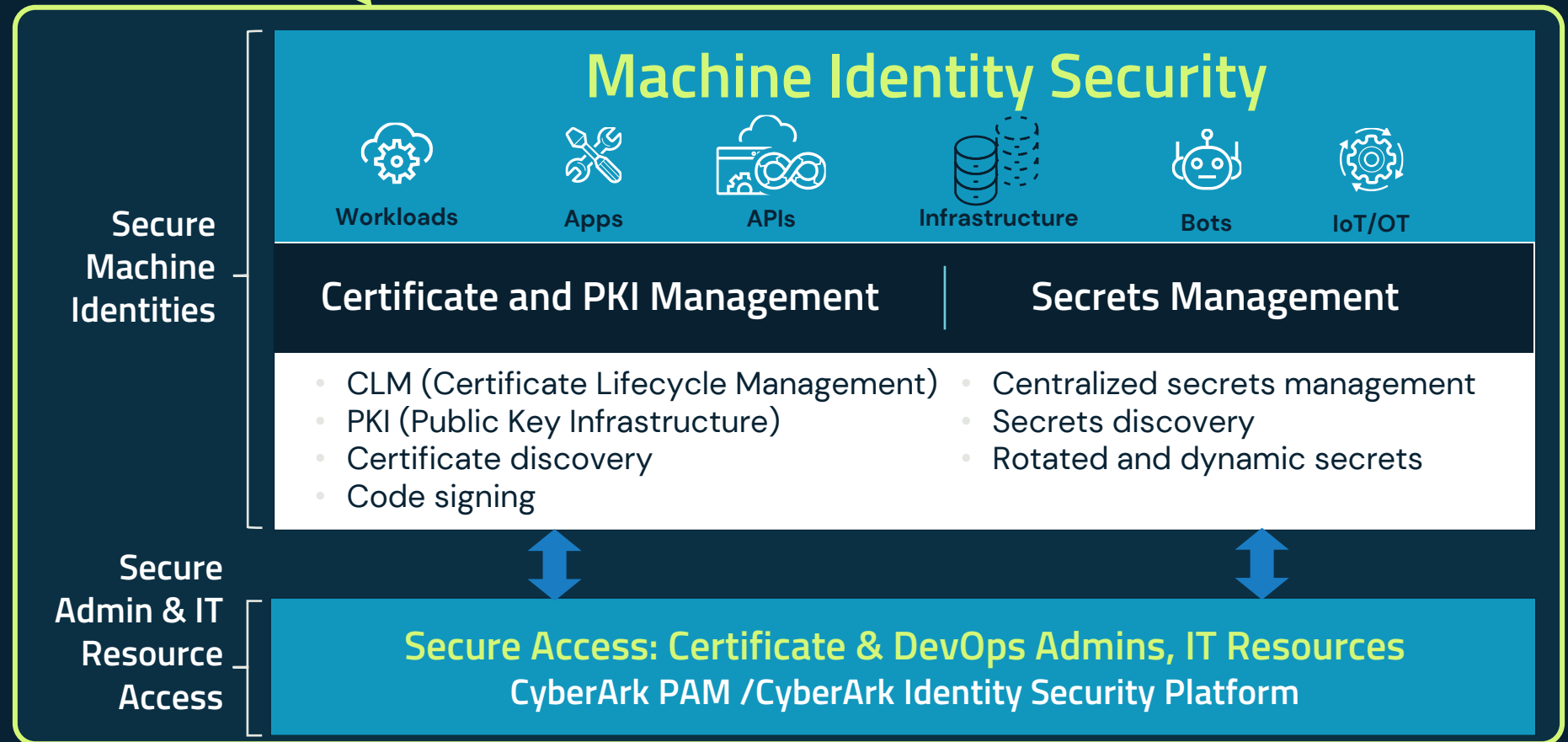


Broad Solution Solves Machine Identity Security Challenges

Secure Certificates, PKI and Secrets. Automate and Prevent Outages



Expanded Capabilities Secure All Machine Identities





CYBERARK®
THE IDENTITY SECURITY COMPANY®

Secrets Management

Challenges with secrets management

They exist **everywhere**
(on prem, cloud)



Secrets are **hard-coded**
in clear-text



Secret values are
static and **aging**



Secrets are stored
locally on system



Secrets **leaked** to
repositories accidentally



Lack of **accountability**
and **governance**



Security islands caused
by vault sprawl



Pursued by **attackers**
(insider and external)



Example Breach: Machine Credentials & Secrets

Attack Vector:

Unprotected and hardcoded secrets in Uber's PAM automation code

Result:

Most of Uber's data and IT infrastructure was compromised

In the attacker's own words:

Tea Pot

last seen just now

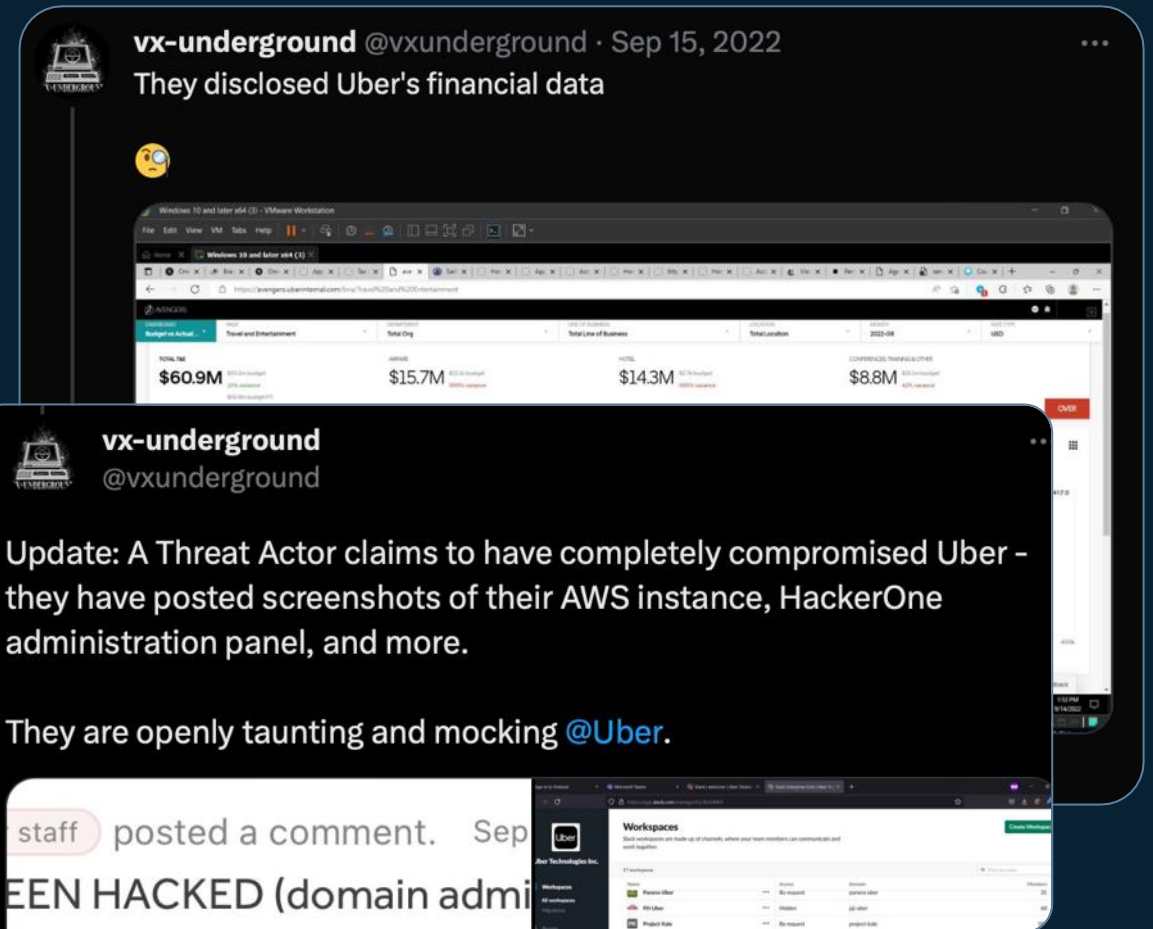
ok so basically uber had a network share \\[redacted]pts. the share contained some powershell scripts.

one of the powershell scripts contained the username and password for a admin user in [redacted] (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, GSuite

8:05 PM

Negative Consequences:


















Stolen data dumped to social media to embarrass and mock the victim



CyberArk Secrets Manager

Remove hard coded credentials and start rotate them

APPLICATION EXAMPLES

Type	System
Application Servers	   
CI/CD Tools Chains	   
Container Platforms /PaaS	  
SDKs & Dev. Libraries	Go, Java, Ruby, Python .NET, C/C++, CLI, REST
Multiple Platforms	Windows, *nix, zOS, Cloud
RPA	   
Security Tools	  
Other Third Party Applications	C3 alliance partners solution with built in integrations



**CyberArk
VAULT**

↓ AFTER ↓

```
UserName = GetUserName()  
Password = GetPassword()  
Host = GetHost()  
ConnectDatabase(Host, UserName, Password)
```

```
UserName = "app"  
Password = "y7qeF$1"  
Host = "10.10.3.56"  
ConnectDatabase(Host, UserName, Password)
```

↑ BEFORE ↑

- Eliminates risk from hard-coded application credentials by calling APIs
- Achieve passwords / keys rotations
- Many forms of APIs and 100+ integrations OOB

ENTERPRISE RESOURCES



SERVERS



MAINFRAMES



DATABASES



APPLICATIONS

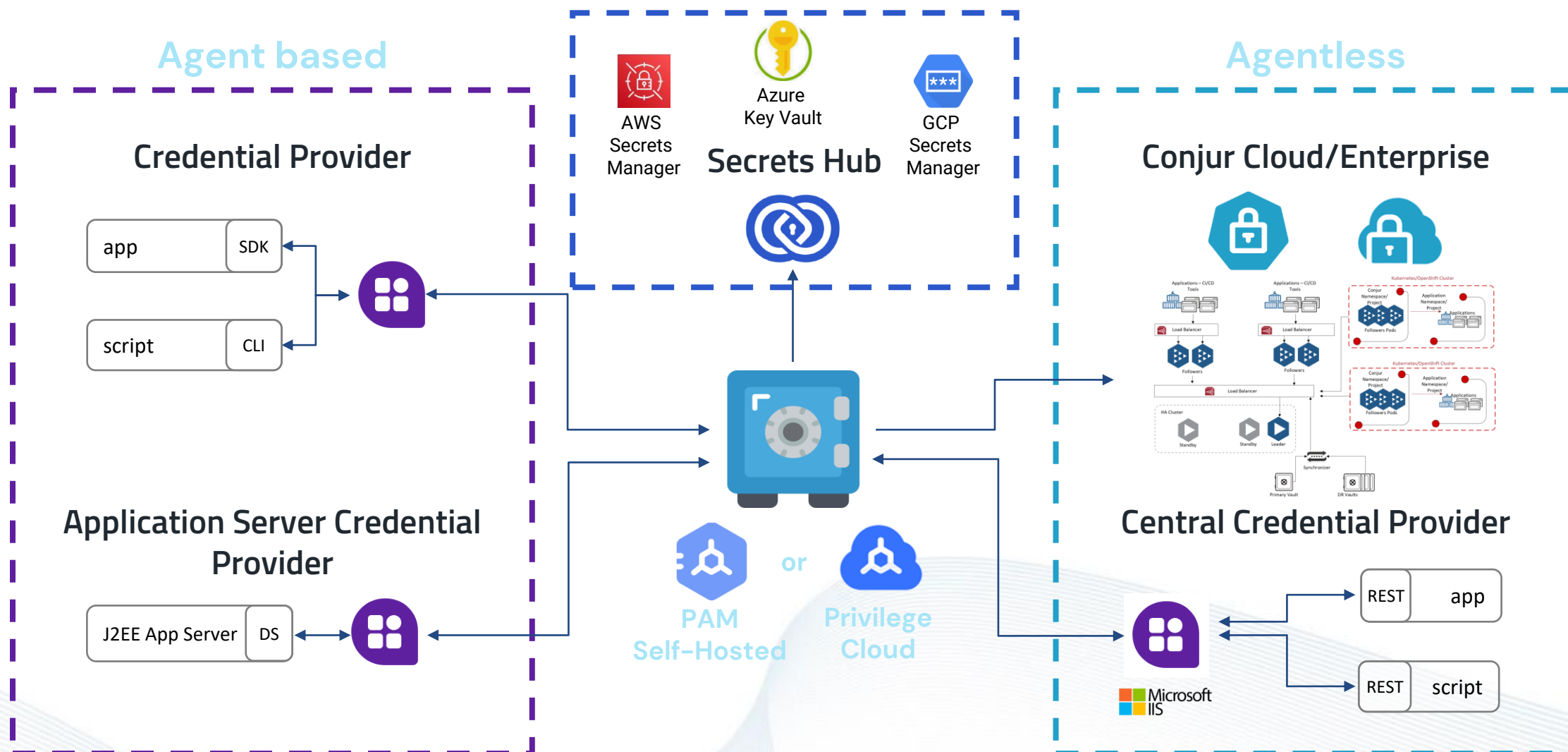


WWW
WEBSITES/
WEBAPPS



CLOUD
INFRASTRUCTURE

CyberArk Secrets Manager Services





CYBERARK®
THE IDENTITY SECURITY COMPANY®

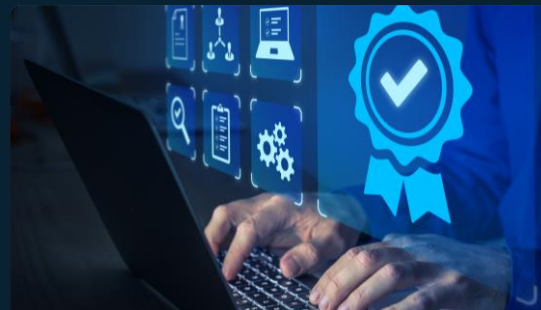
Certificates Management

4 Key Challenges For Securing Certificates and PKI



Outages, downtime, and business disruptions

- Lost revenue and customers, damage to reputation and brand caused by expired certificates



Manual certificate management

- Manual processes lead to human errors and higher costs.
- **Shrinking certificate lifecycles and increased complexity.**
- Issues at Certificate Authorities requiring renewal fire drills.



Legacy PKI costs and risks

- Legacy Windows PKI unable to scale and meet the demands of dynamic cloud environments and mobile devices.
- Unnecessary high risk and cost to operate and maintain.



Security, compliance and audit failures

- Risk of compliance violations, costly downtime, security breaches and potential fines.

Expired Certificates Cause Real Consequences

Just one recent example

EXPIRED CERTIFICATE:

- Cancelled and delayed flights
- FAA Ground Stop
- Telling customers of significant IT outage
- Reputation?

Alaska Airlines Flights Canceled and Delayed After IT Outage Prompts FAA Ground Stop

Alaska Airlines was forced to cancel and delay some flights on Sunday night after an IT outage crippled multiple computer systems at the Seattle-based carrier, prompting the Federal Aviation Administration (FAA) to issue a temporary ground stop.



The airline was quick to reassure worried passengers that the outage was not the result of a cyberattack. Engineers eventually pinned the blame on an out-of-date security certificate which needed to be updated.


Not the result of a cyberattack.

Engineers eventually pinned the blame on an out-of-date security certificate which needed to be updated.


[LEARN MORE](#)

CA/Browser Forum & Public Trust

Browser & OS Companies



Public CA Vendors



CA/Browser Forum is a voluntary gathering of Certificate Issuers (CAs) and suppliers of Internet browser software and other applications that use certificates.

CA/B Forum Working Groups

Server Certificate

Network Security

Code Signing Certificate

Definitions

S/MIME Certificate



Changes are proposed via ballot from a working group, and must be voted on by both certificate issuers and consumers

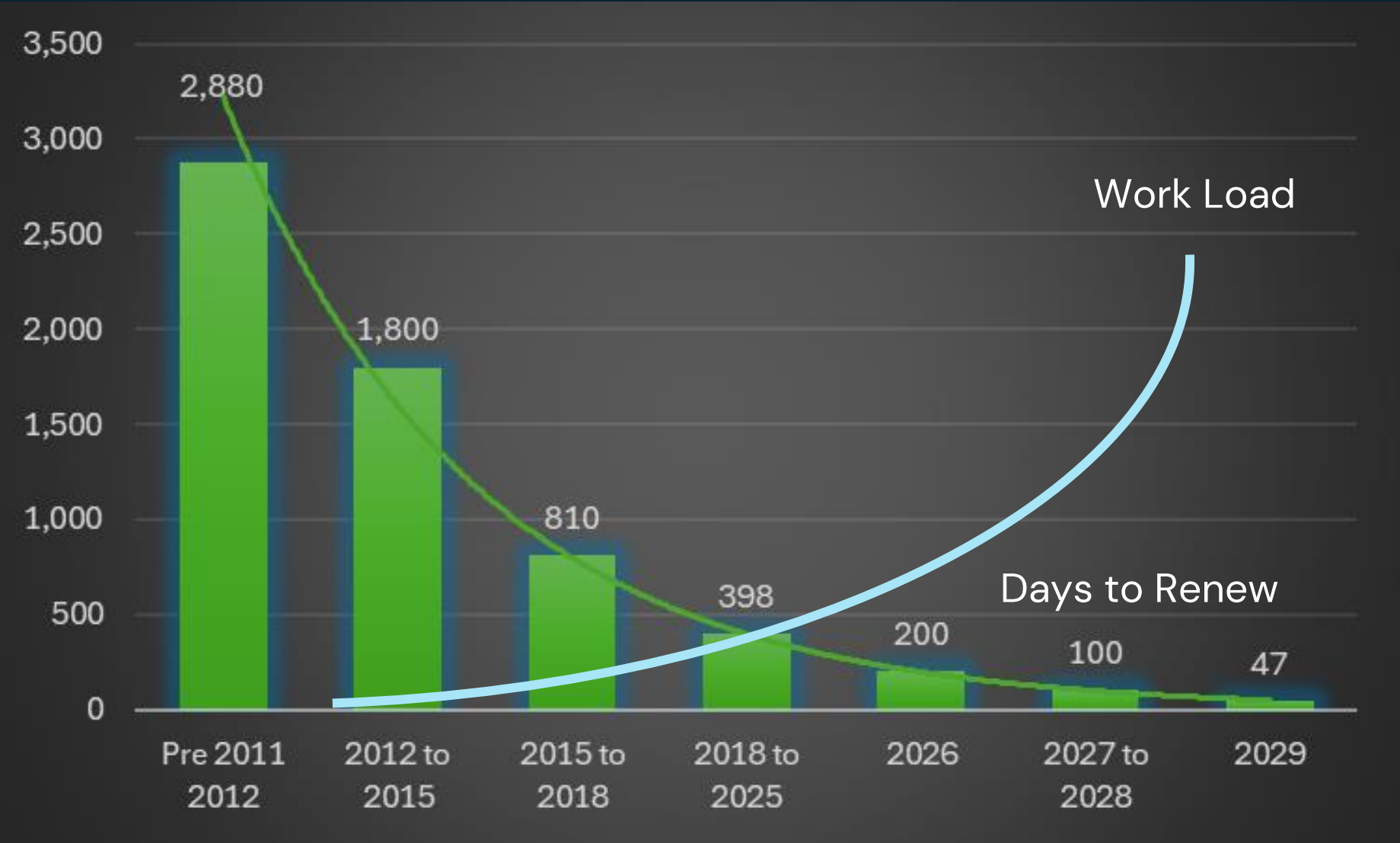
Certificate validity Decrease

Here is the confirmed phased [rollout](#):

- **March 15, 2026:** Certificates capped at **200 days**
- **March 15, 2027:** Reduced further to **100 days**
- **March 15, 2029:** Certificates limited to **47 days**, with Domain Control Validation (DCV) periods shortened to **10 days**

<https://www.root.cz/clanky/certifikaty-pro-https-zkrati-postupne-do-roku-2029-svou-zivotnost-na-47-dni/>

Countdown has started



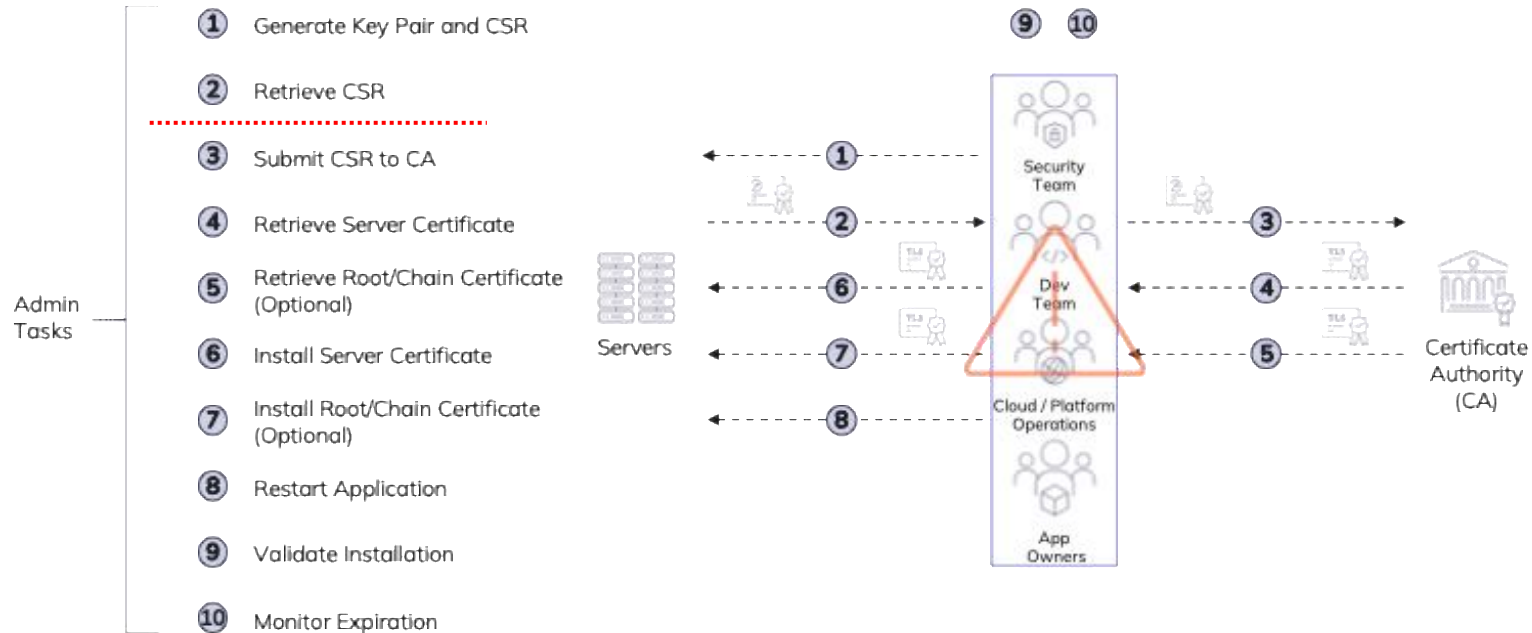
March 2026: Validity capped at 200 days

March 2027: Drops to 100 days

March 2029: Final reduction to 47 days

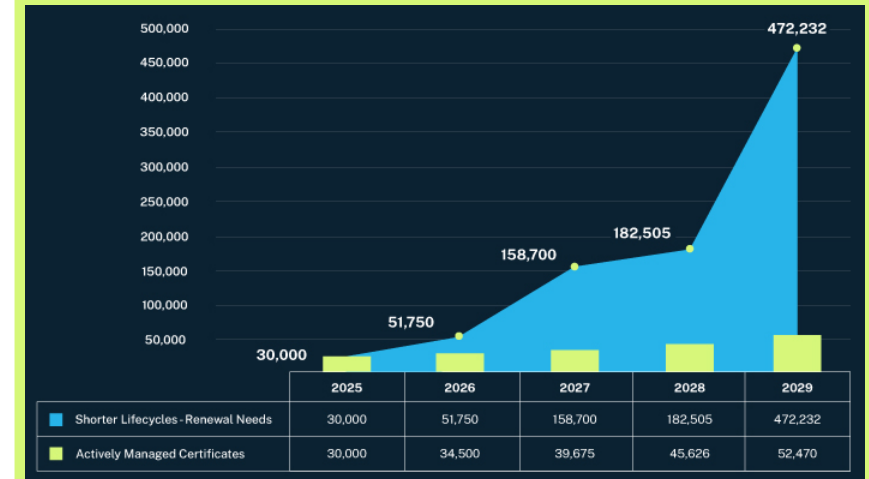
DCV windows also shrinks to 10 days by 2029

Current Manual Processes *Do Not* Scale



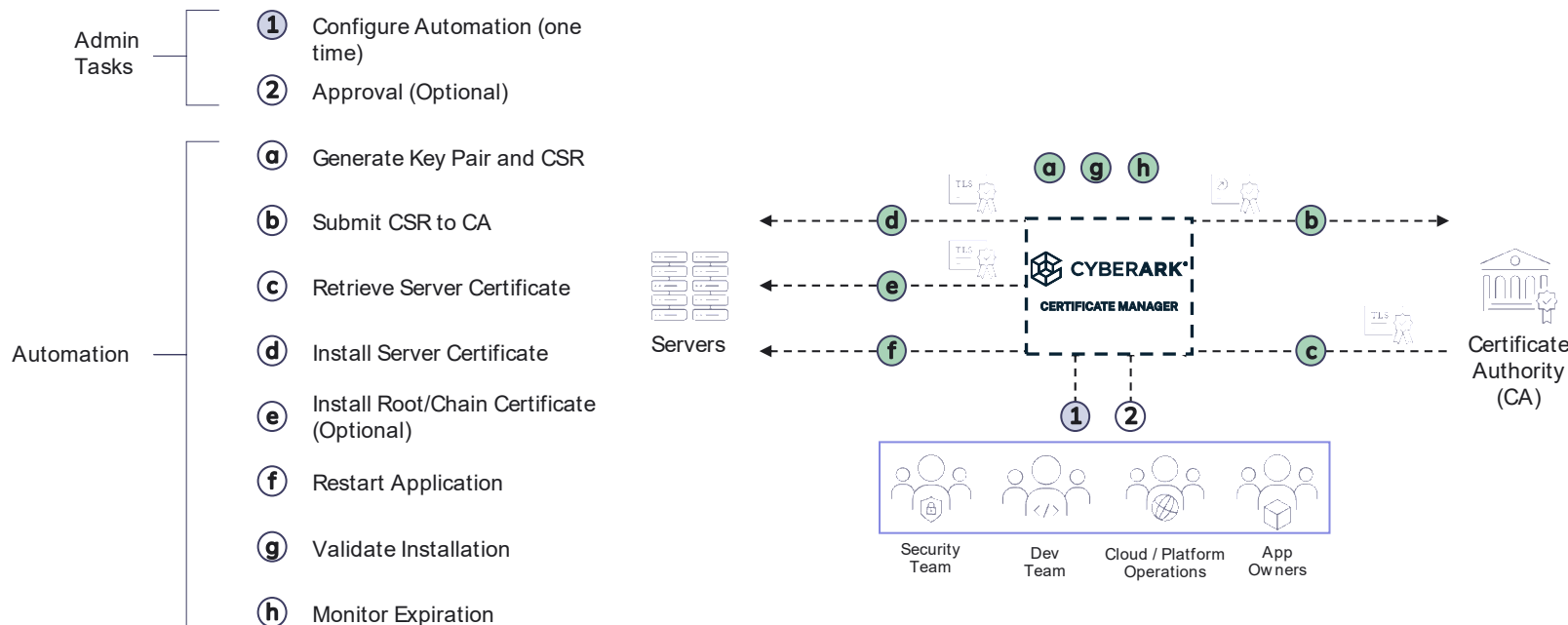
It's not simple. It is complex and error prone.

8X



- Move to 47 days = 8x more renewals
- 52K certificates = 472K renewal events/year
- 1 hour per renewal = 472,000 hours = 54 years of labor

Automation. The Ideal State.



<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf>

NIST 1800-16



"Automation should be used wherever possible for the enrollment, installation, monitoring, and replacement of certificates..."

Certificate Services Team

Provide a central system that supports resource owners in automating management of certificates

Resource Owners

Automate the management of their certificates

NIST 1800-16

CyberArk enables enterprises to address TLS server certificate security and operational risks.

CyberArk Certificate Manager



• Discovery

- Network Discovery
- Certificate Authority Import

• Inventory

- Continuous Monitoring
- Reporting
- Notification & Alerts

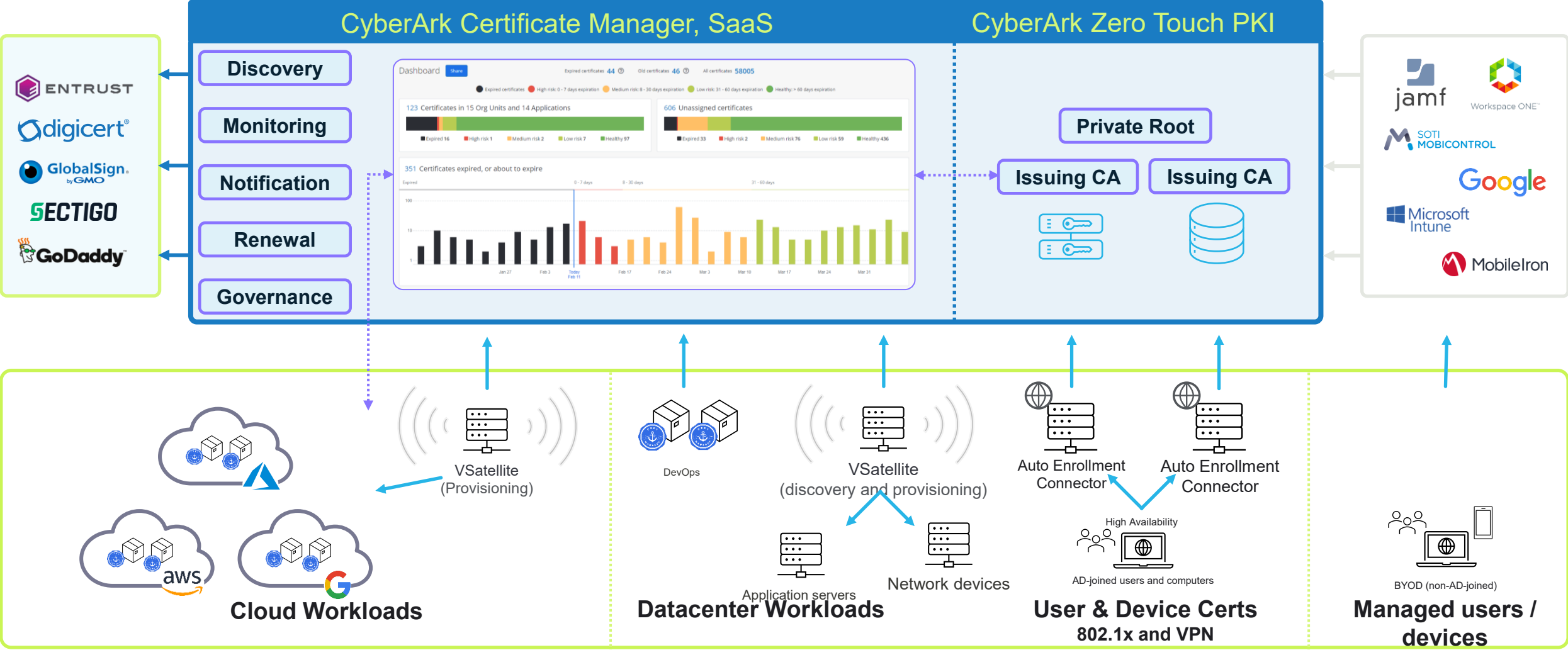
• Policy

- Ownership & Accountability
- Policy Enforcement
- Approvals & Governance

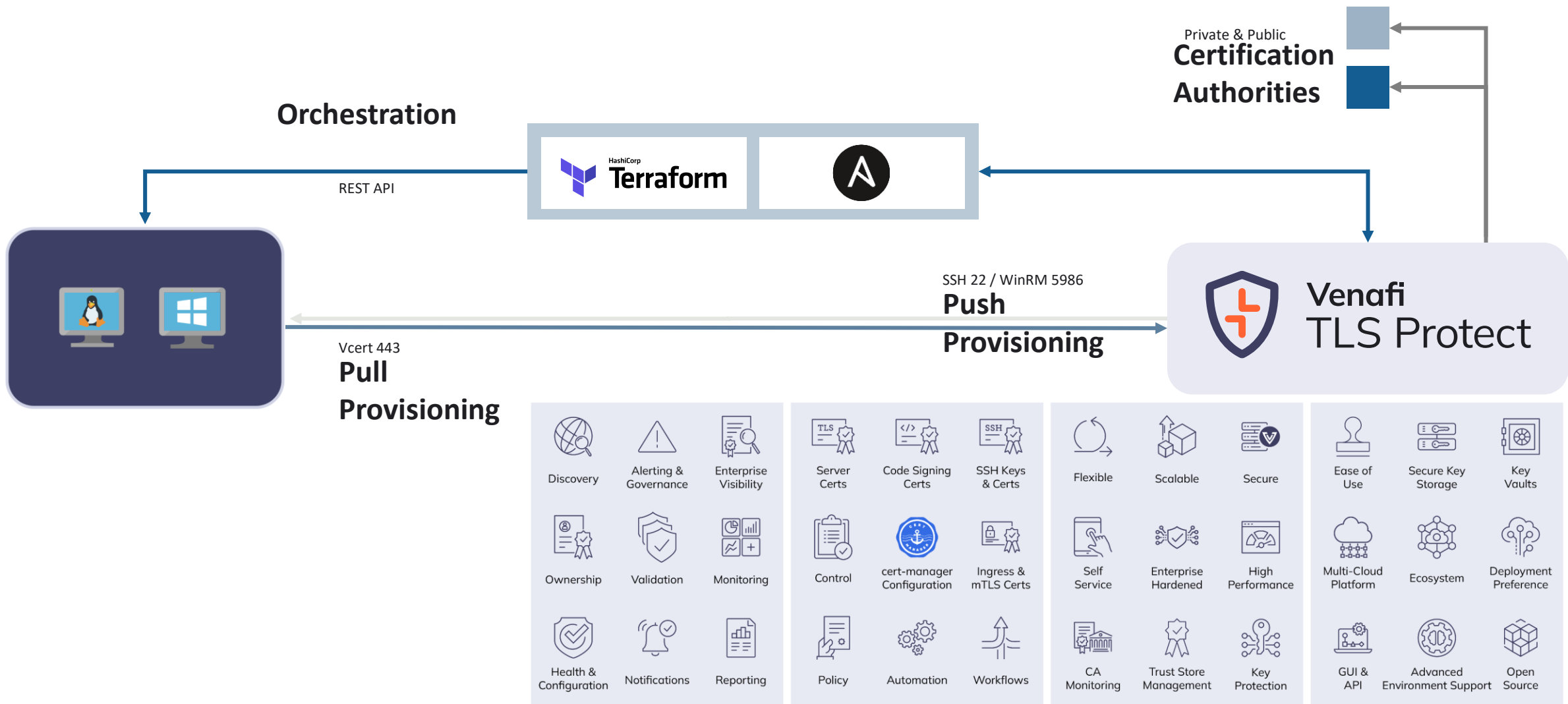
• Renewals

- Automatic renewal
- Automatic deployment
- Verification
- Cloud / DevOps / Legacy

Securing Certificates and PKI Architecture



Autotomatic Renewals





CYBERARK®
THE IDENTITY SECURITY COMPANY®

ECOSYSTEM

Extend the protection and automation of your machine identities with an unparalleled ecosystem of partner solutions.

MACHINE IDENTITY SECURITY

CAs



DevOps



ADC



SOAR



DDoS



WAF



NGFW/SSLVPN



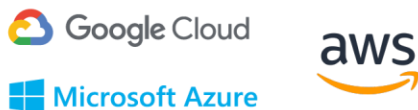
HSM



SIEM/Analytics



Cloud



EMM



ITSM



PAM/IAM

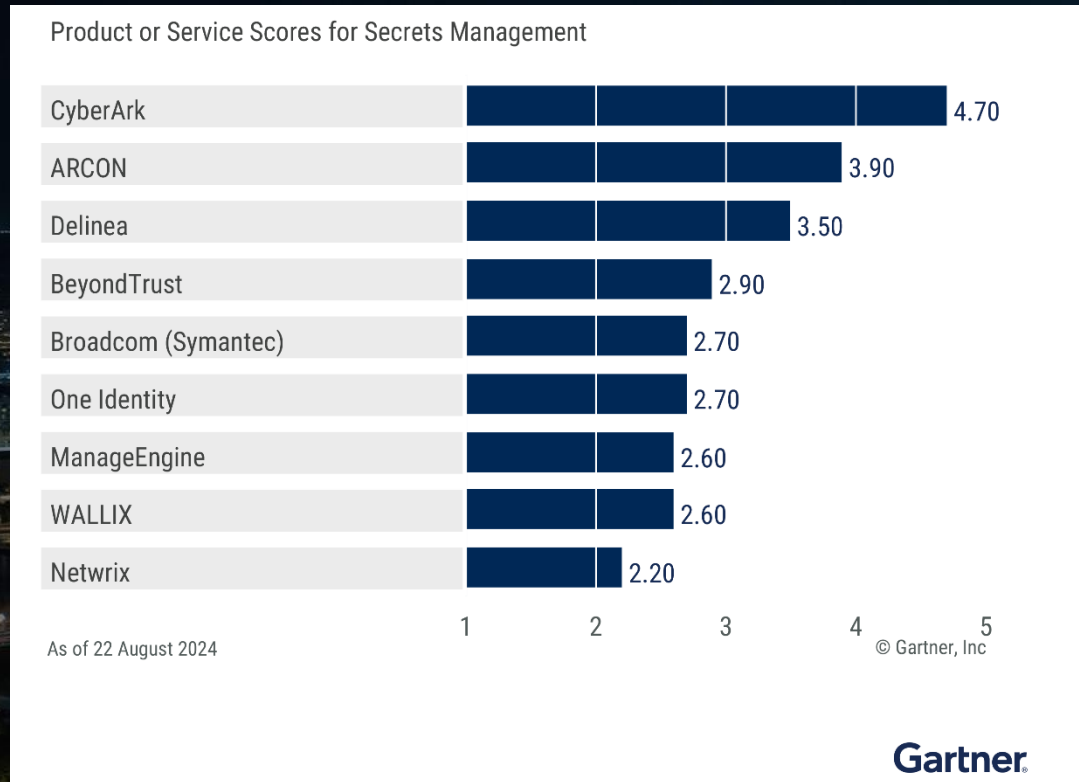


Application Servers



Visit marketplace.venafi.com

CyberArk Ranked 1st in the Secrets Management Use Case in the 2024 Gartner® Critical Capabilities for PAM



CyberArk Secrets Management centrally discovers, secures and rotates secrets across cloud and hybrid environments. Learn how different vendors were evaluated and why CyberArk ranked 1st

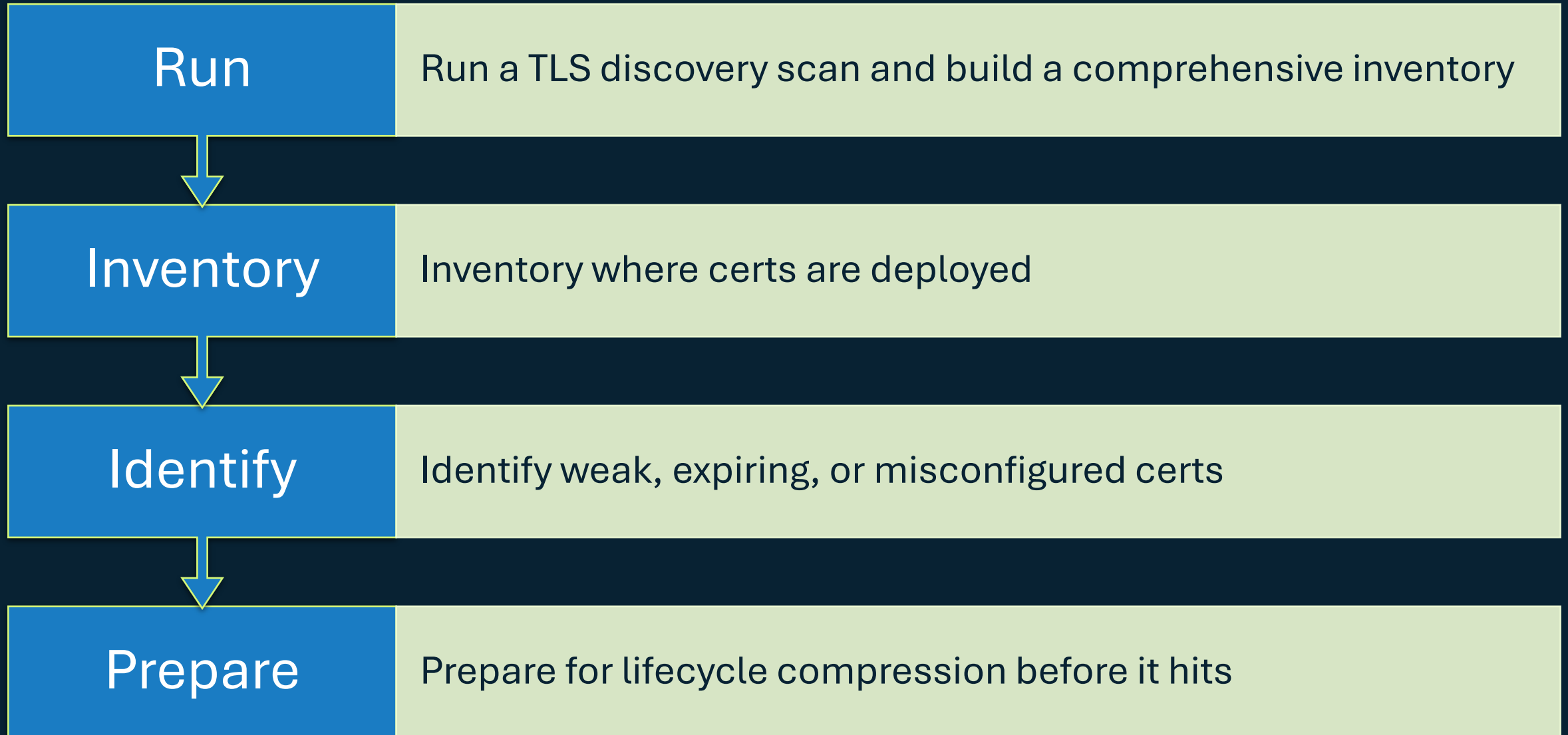
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CyberArk.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner® Critical Capabilities for Privileged Access Management, by Paul Mezzera, Abhyuday Data, Michael Kelley, Nayara Sangiorgio, Felix Gaehtgens, 9 September 2024

Don't Wait for 2029. Get Ahead Now.





Thank you

