

# Entrust Certificate Management

---

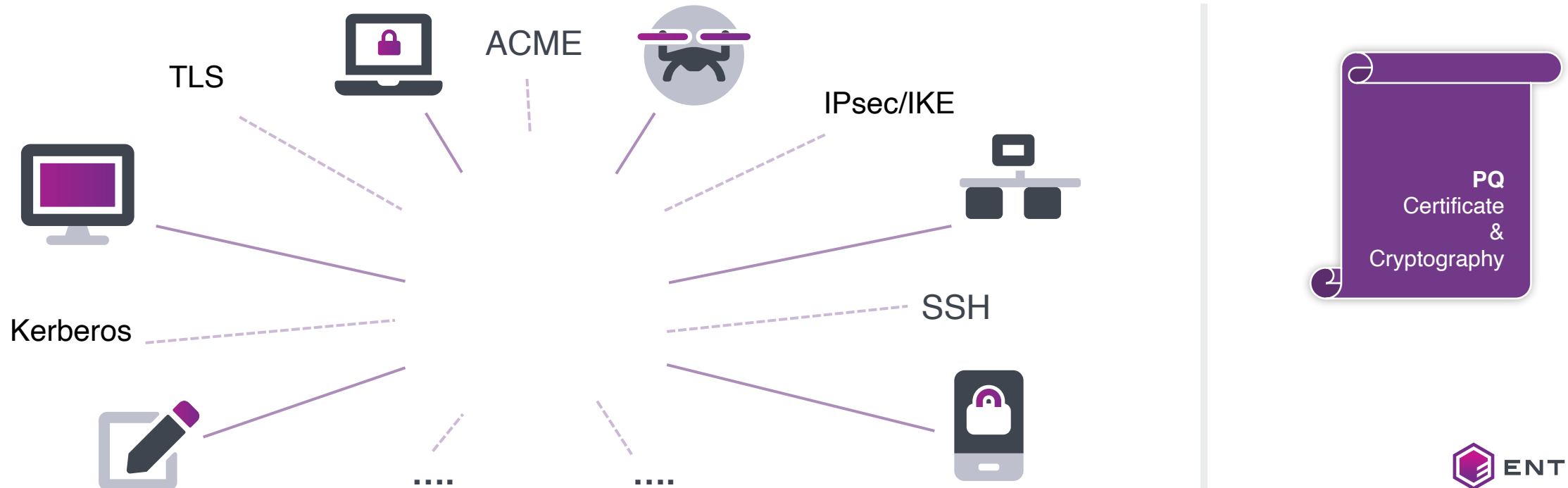
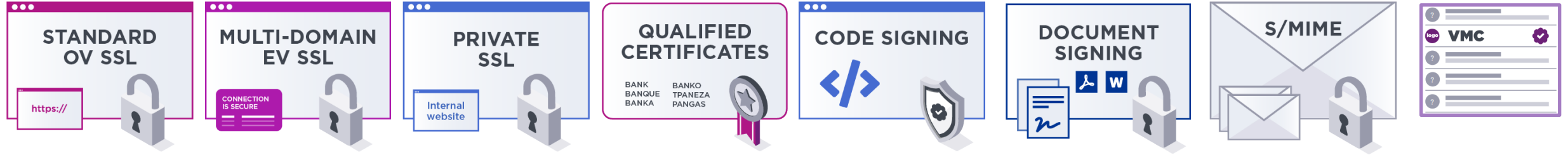
Richard Palmer  
Territory Manager CEE

April 2026



**ENTRUST**  
SECURING A WORLD IN MOTION

# Digital Certificate & Cryptography – A complex ecosystem



# Machine identity evolution and business impact

*Over the past few years, the Ponemon Study has shown a 50% increase in the number of certificates being issued – a lot of which could be a direct result of machines*

  
**~60 : 1**

Average **Machine Identity** to **Human Identity Ratio**

Enabling remote & hybrid workforces



IoT

National ID



DevOps

Mobile applications/5G

Smart meters

**Driving Increased Adoption**

## Common use cases

- TLS/SSL
- Digital signing
- Email
- Code signing
- VPN
- Mobile Device

“Worldwide economic **losses from unprotected machine identities** estimated at **\$51B to \$72B**”

# Impact of expired certificates

- Certificate expirations are a leading cause of costly **outages** and can severely impact **business operations, reputation, and revenue**.
- Reliance on spreadsheets and calendar reminders often leads to missed expirations
- Organizations (e.g., 40% in one CSC research, 45% in another survey) experience service downtime due to certificate-related incidents, with 37.5% specifically due to expired certificates



**\$5K-9K/min**

with severe outages potentially costing more than **\$ 500K** per hour

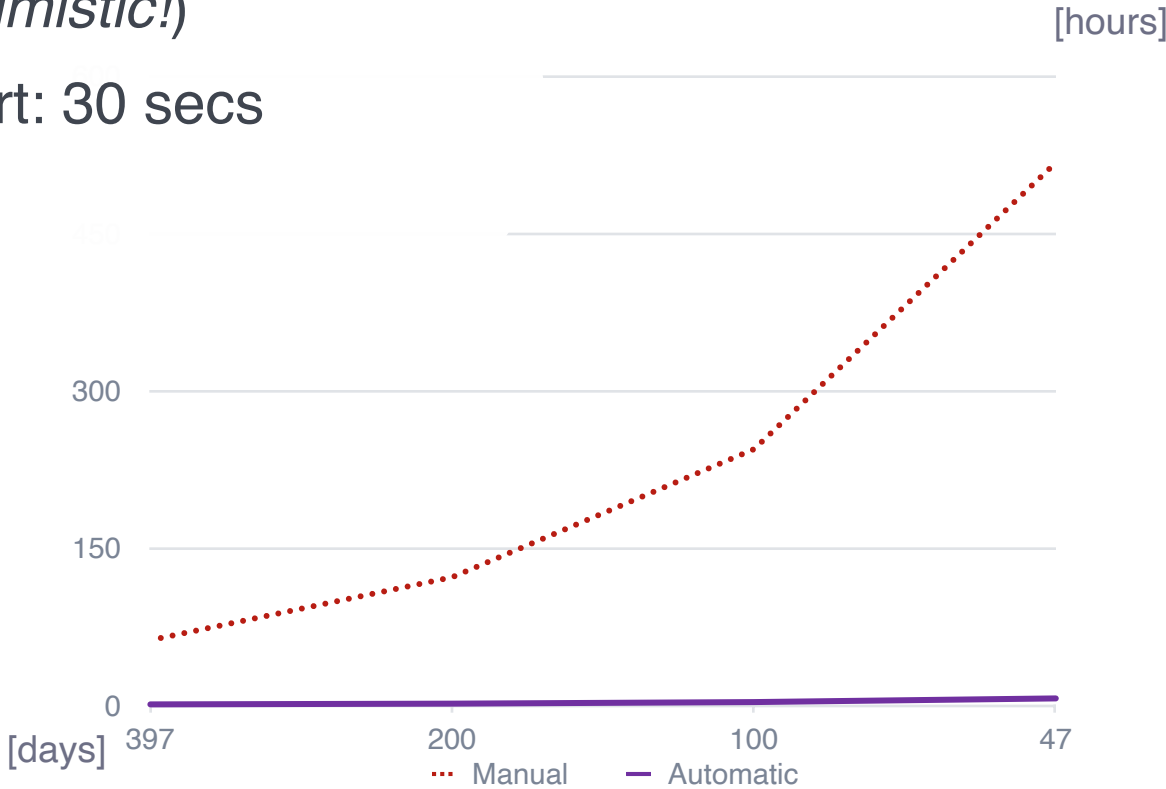
**5-24 hrs**

**Downtime** and 15.4% experienced 25 hours or more from certificate-related issues

# Time Spent on Certificate Management (Annual)

- Organization's Certificates: 100
- Avg. Manual Operation Time/cert: 40 mins (*optimistic!*)
- Avg. Automatic Operation Time (monitoring)/cert: 30 secs

| Time Spent on Certificate Management (Annual) |   | Manual (hours) | Automatic (hours) |
|-----------------------------------------------|---|----------------|-------------------|
| Today (397 days)                              | ⚠ | 62             | 0,8               |
| March 15, 2026 (200 days)                     | ⚠ | 122            | 1,5               |
| March 15, 2027 (100 days)                     | ⚠ | 244            | 3,0               |
| March 15, 2029 (47 days)                      | ⚠ | 518            | 6,5               |



# Efficiency and Cost saving with Certificate Lifecycle Management

---

- Adopting a modern Certificate Lifecycle Management (CLM) solution with features like discovery, CA integration, **automated renewal**, and **deployment** to destinations can yield substantial benefits in **operational efficiency**, **cost reduction** and **service reliability**

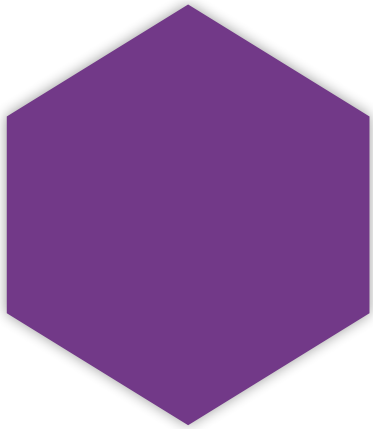
|                                          | Manual Management | Automated CLM                  | Impact                                    |
|------------------------------------------|-------------------|--------------------------------|-------------------------------------------|
| Labor required per 100 certificates/year | ~500+ hours       | 10 hours or less               | ~96% time saved                           |
| Outage risk due to certificate expiry    | High              | Near zero                      | Service reliability dramatically improved |
| Operator intervention per event          | Multiple steps    | Single click/minimal/no action | Less human error, streamlined ops         |
| Ability to scale as environment grows    | Difficult         | High                           | Future-ready, more scalable               |

# Significant Outages Due to TLS/SSL Certificate Expiration

| Years | Organization      | Cause                                                                                                                          | Impact                                                                                                                                       |
|-------|-------------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 2020  | Microsoft Teams   | An <b>expired authentication certificate</b> .                                                                                 | A <b>three-hour outage</b> preventing approximately 20 million daily users from signing in or accessing the collaboration service            |
| 2021  | Google Voice      | An <b>expired TLS certificate</b> in the Google Voice frontend systems due to a failure in updating certificate configurations | A global outage lasting over <b>four hours</b> , preventing users from making or receiving Voice over Internet Protocol (VoIP) calls         |
| 2023  | Starlink (SpaceX) | An <b>expired ground station certificate</b> for a system component                                                            | A <b>several-hour global service outage</b> affecting users of the satellite internet service                                                |
| 2024  | Bank of England   | Caused by an <b>expired SSL/TLS certificate</b> . (It was reportedly the second certificate-related outage in 2024)            | A global outage to its automated high-value payment system, <b>CHAPS</b> , halting retail settlement transactions for over <b>90 minutes</b> |

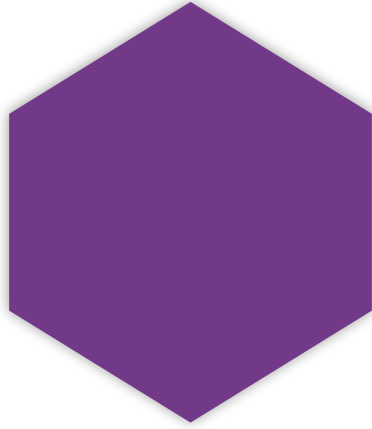
# Certificate Management - Automating Machine Identity Management With Zero-Trust Principle

---



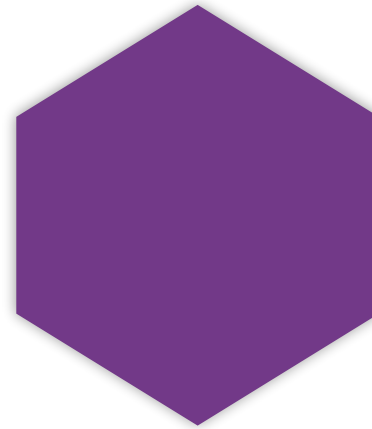
## Automated inventory and visibility

- Cert discovery from different source points (Vaults, CAs, Networks)
- Centralized inventory
- Self service ability



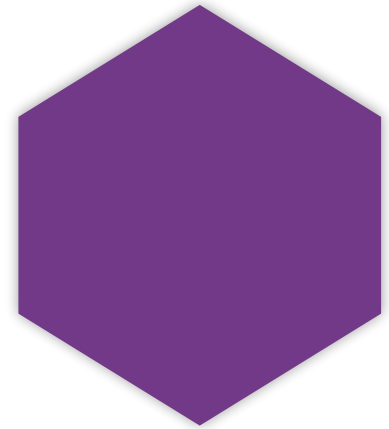
## Policy Enforcement

- Centralized policy configuration and management
- Binding security policy & ownership to groups
- Role based controls
- Policy led manual / automated approvals for Enrollments and Code/Firmware signing requests



## Automated Renewals and Destination

- Automated renewal as per the security policy
- Plugins - Automated push to a destination
- Provision, Issue, Renew, Revoke management

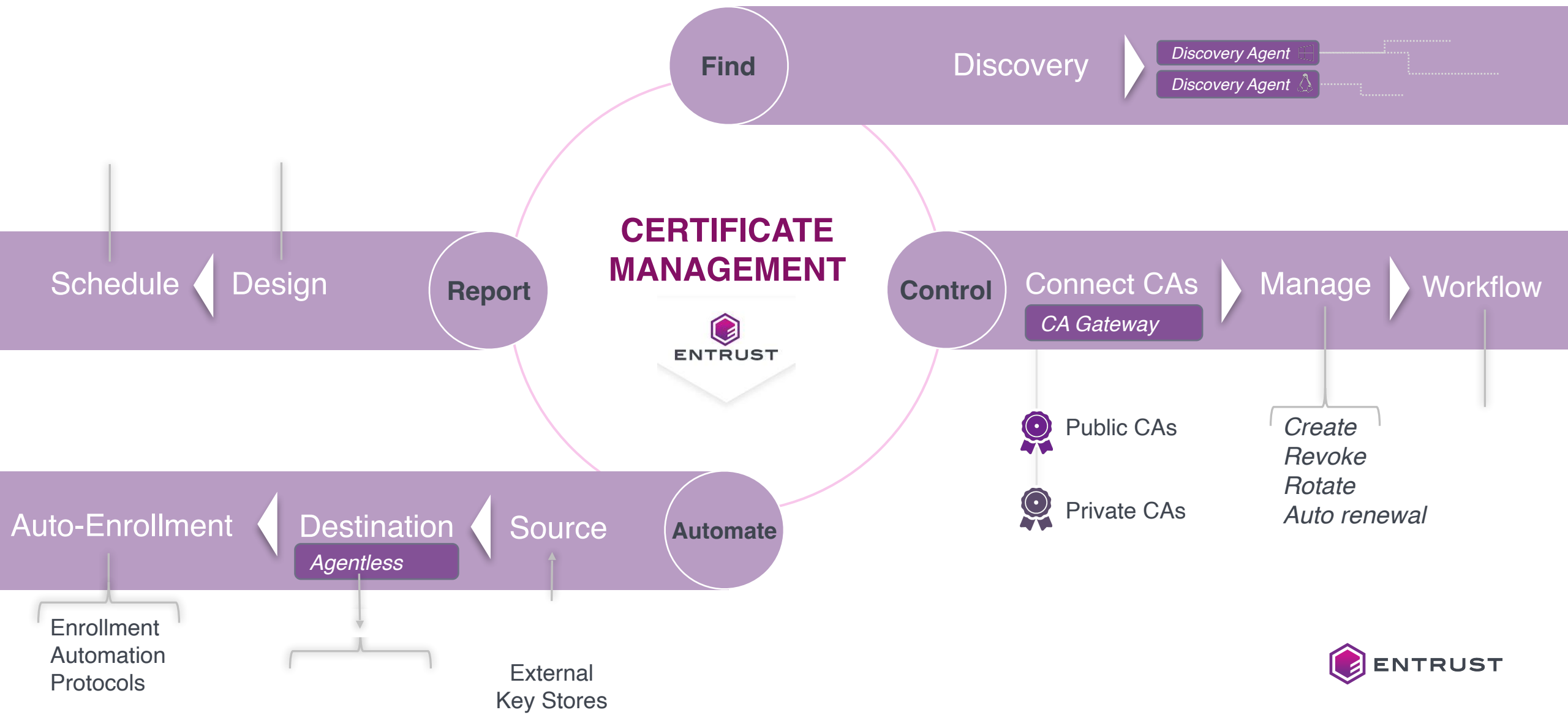


## Monitoring – Alerts and Notifications

- Event driven Alerts / Notification
- Expiry reminders
- Compliance insights (Identities with obsolete crypto)
- Meta data, RBAC



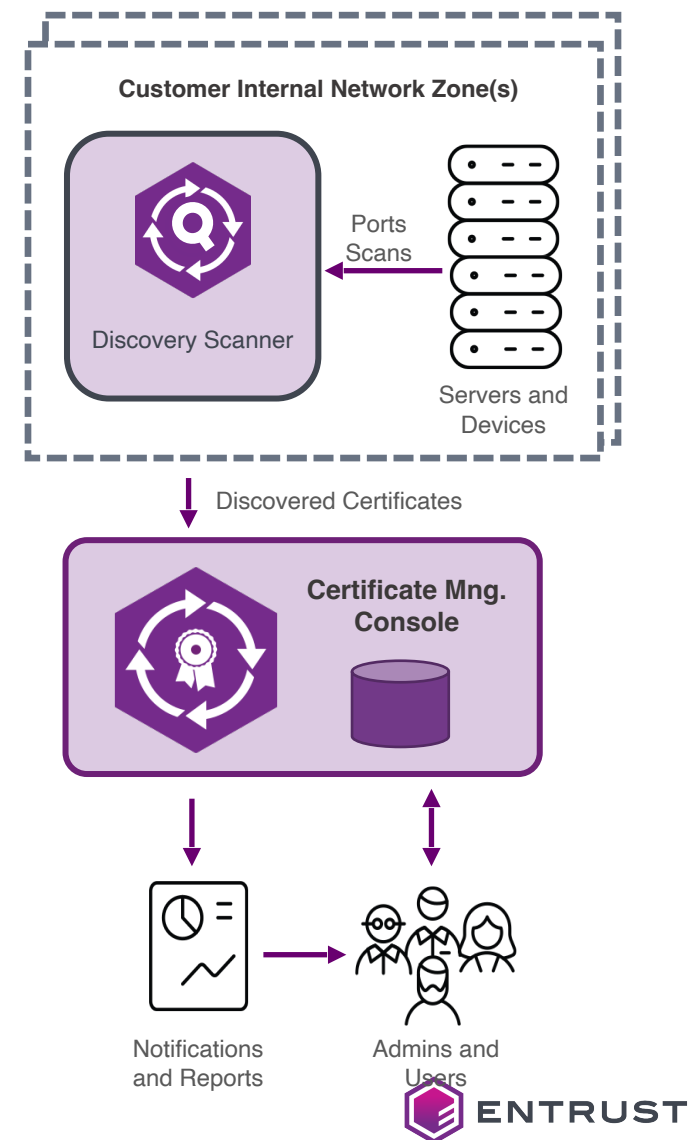
# CSP – Certificate Management



# Certificate Management — Find Your Certificates

You can't manage what you do not know about. Discover certificates deployed in your enterprise...

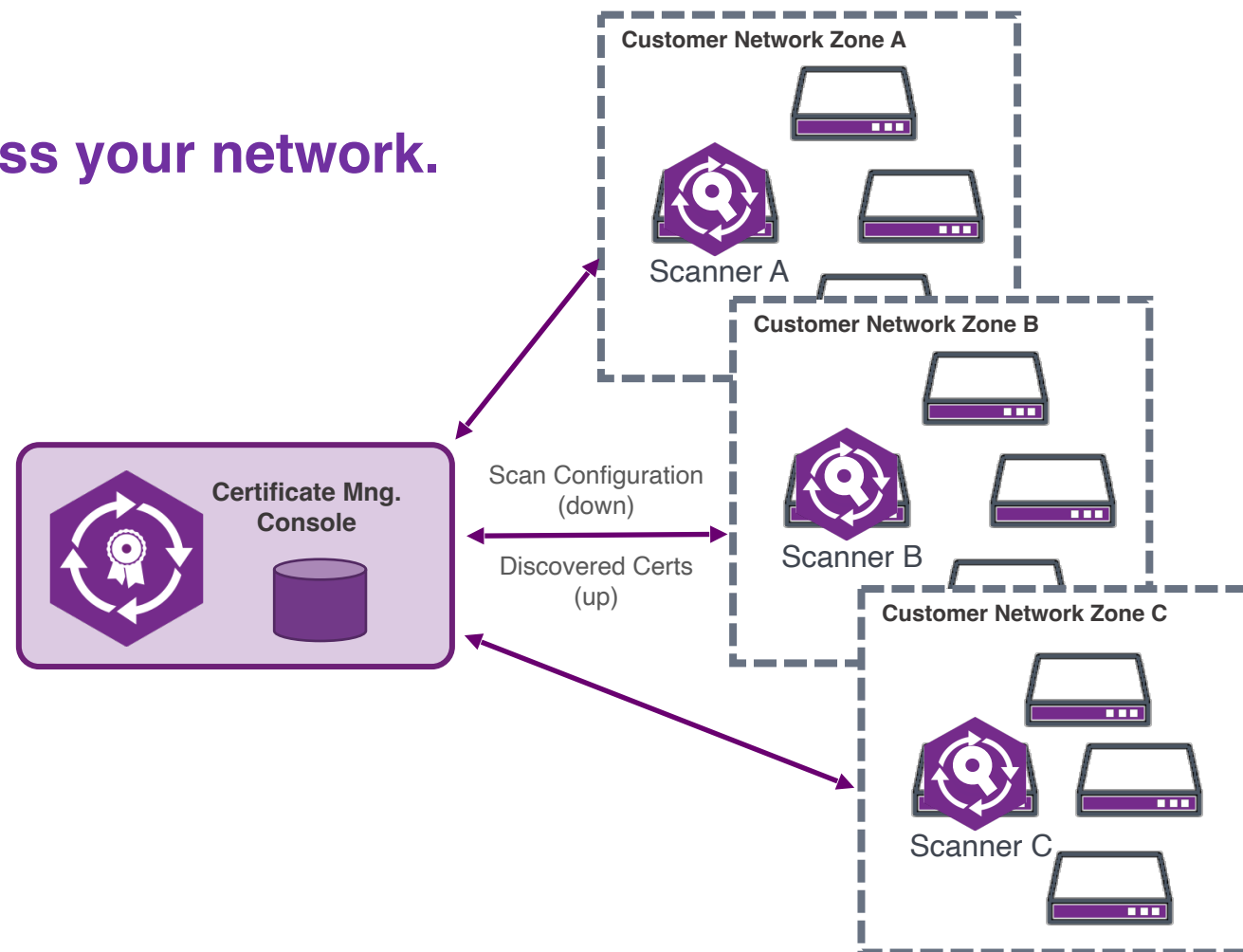
- Configure Discovery Scanners in one centralized place
- Define Custom Fields and tag certificates to integrate with your business practices & reports
- Customized Automated Reporting of activity, policy violations or anything else you choose
- Set up expiry notifications
- Deploys as two separate components – **Certificate Management Console** and the **Discovery Scanner**
  - The Console can be in your cloud or premise
  - The Discovery Scanner is usually inside your controlled network zones.
  - Deploy one Scanner or many to search internal and external networks



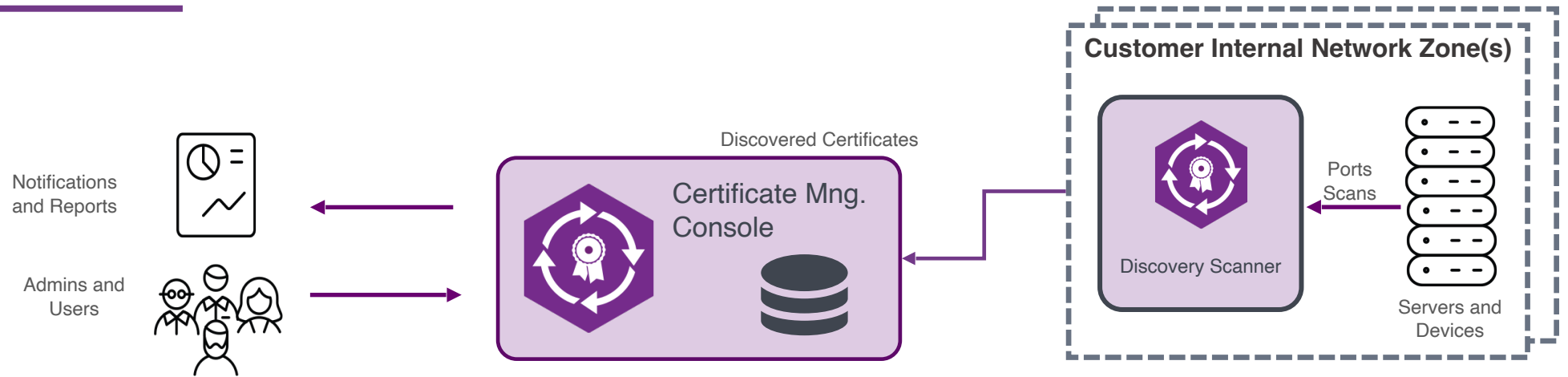
# Certificate Management – Discovery Scanner

**Find x.509 certificates on servers across your network.**

- › Uses NMAP network scans to find certificates exposed to the network
- › Deploy multiple Discovery Scanners, one for each network segment
- › Centrally manage from the management console
- › Run each Scanner as a simple, stateless, Docker container
- › Scans allow for custom ports, IP ranges and schedules
- › Scanners run on [Windows and Docker](#)



# Certificate Management – Find

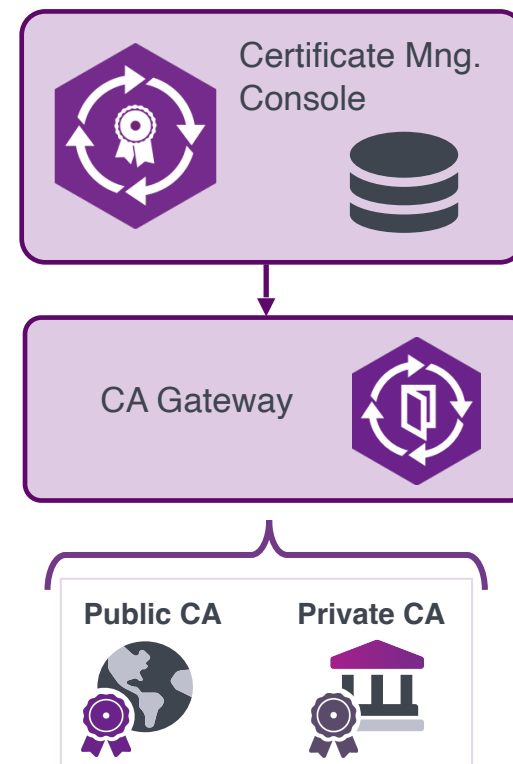


# Certificate Management — Establish Control of the CAs

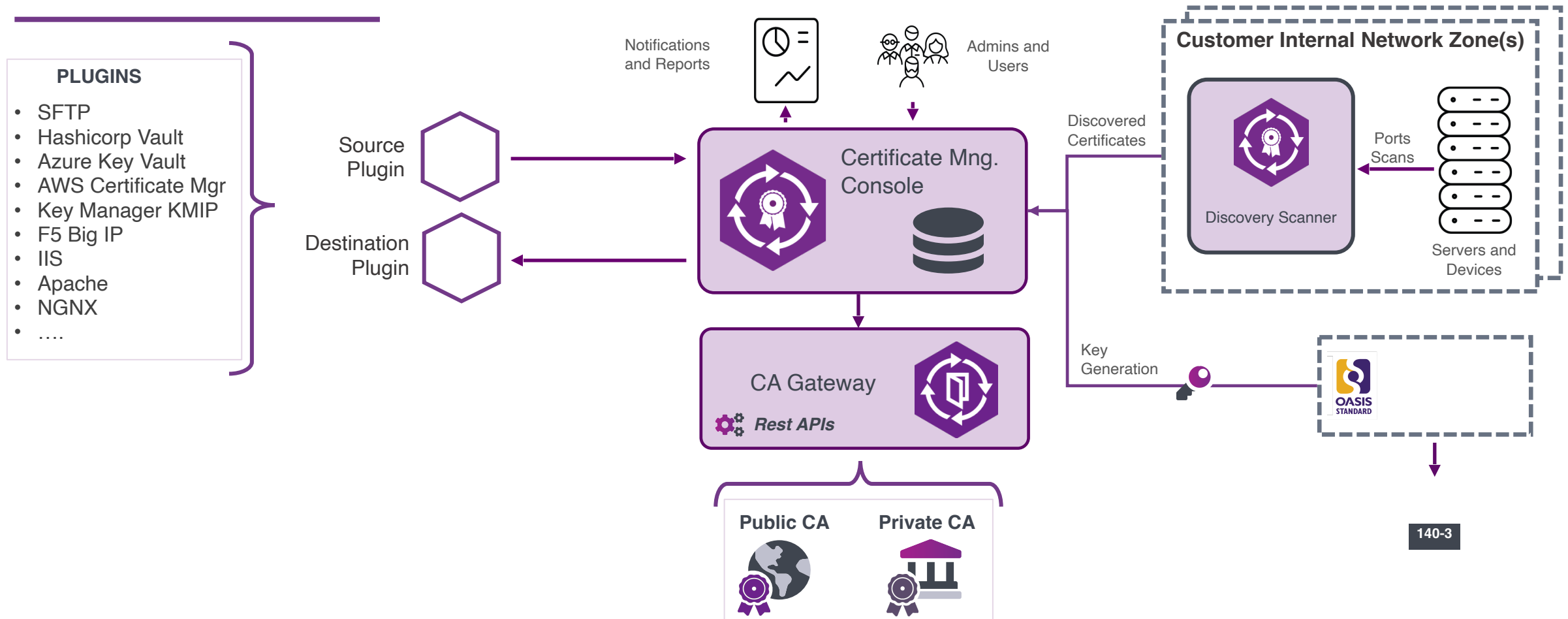
---

You need a Single Plane of Glass for all your Certificate Authorities

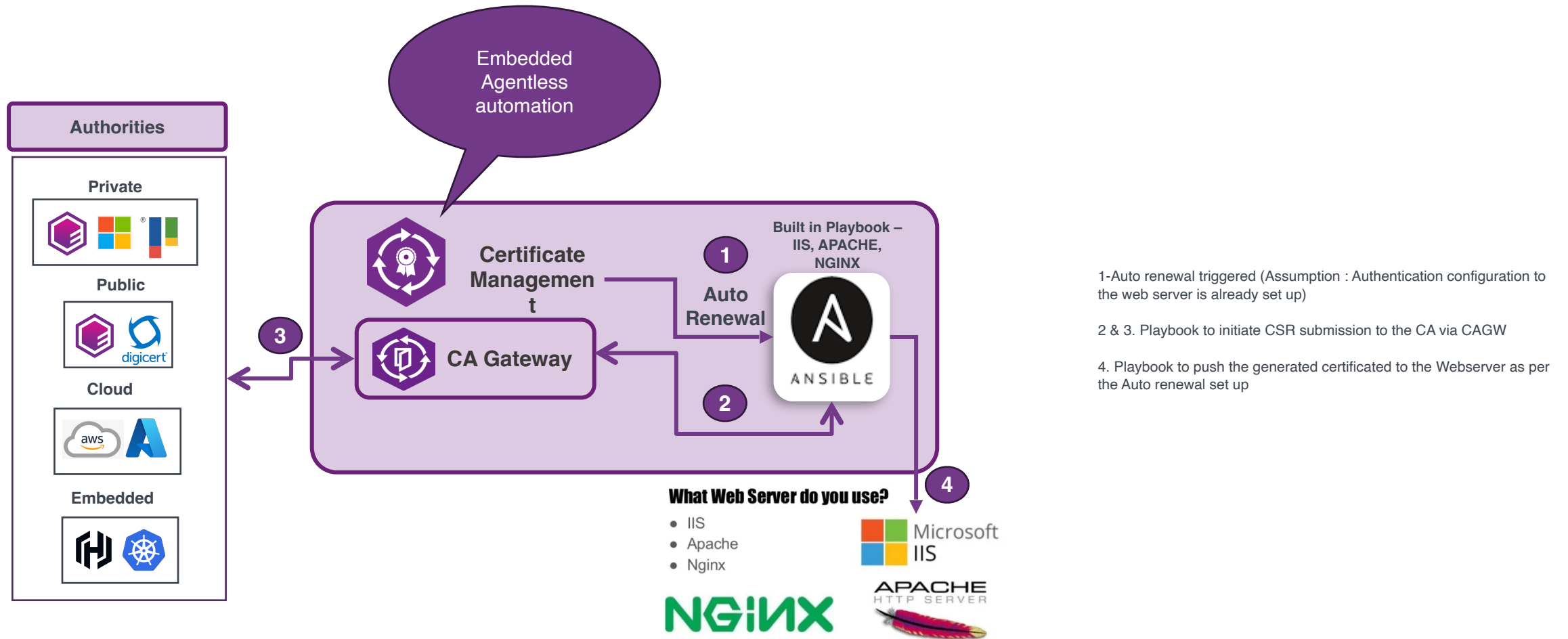
- Uses CA Gateway as the connection to Authorities
- Consolidate all certificate activity to a single view
- Link Discovered certificates to issuing connected CAs
- Manually issue and renew certs through web browser
- See all certificate updates regardless of integration through the Source Scanner connection to CAs.



# Certificate Management – Control



# Agentless Certificate Management

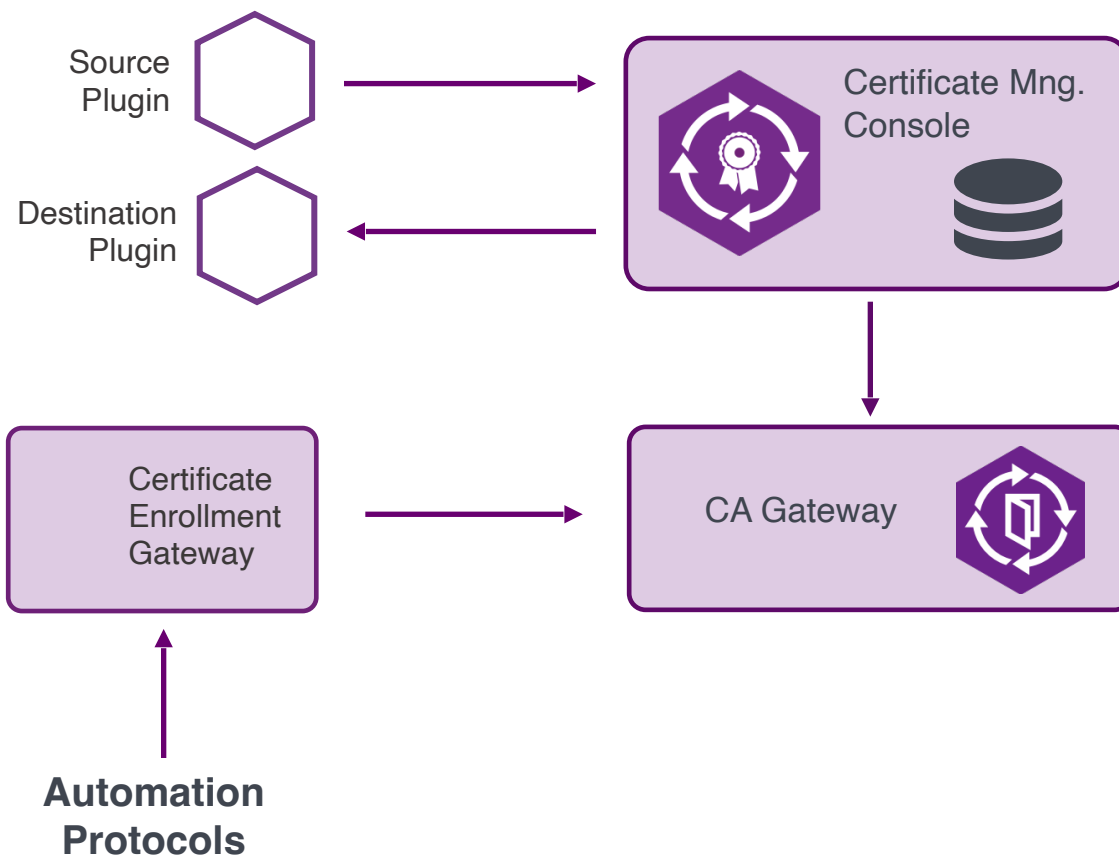


Agentless = Customers don't need to install any additional infrastructure/agents

# Certificate Management — Automate Issuance and Renewal

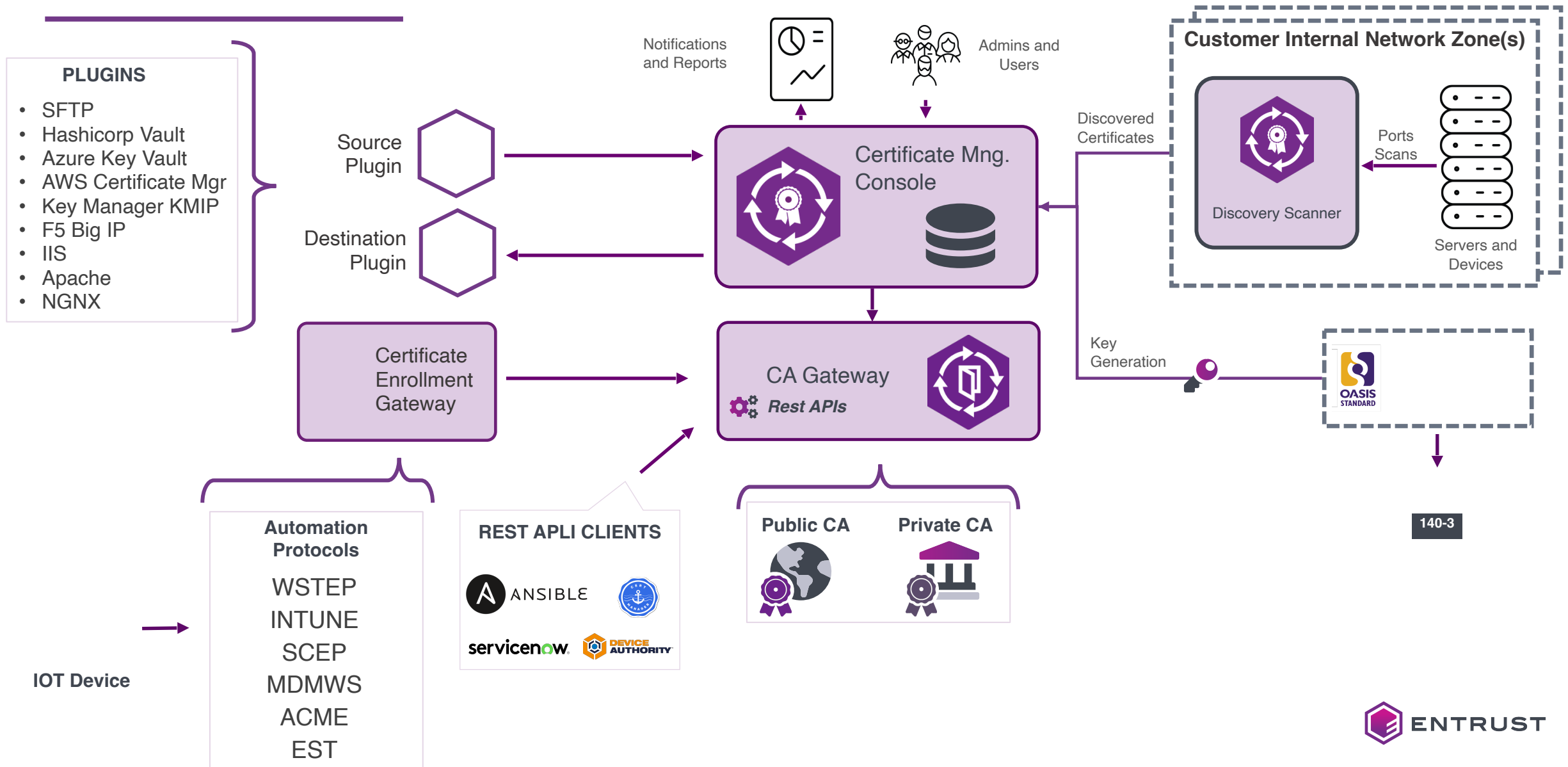
## Automation is Key to Preventing Outages and Exposures

- Push certificates to defined destinations
- Automate the renewal of certificates
- Utilize pre-built Entrust Enrollment Gateway or custom CAGW automation integrations
- Associate custom data to certs issued through other integrations using Auto-tagging
- Utilizes CA Gateway integrations as part of the total solution





# Certificate Management – Automate

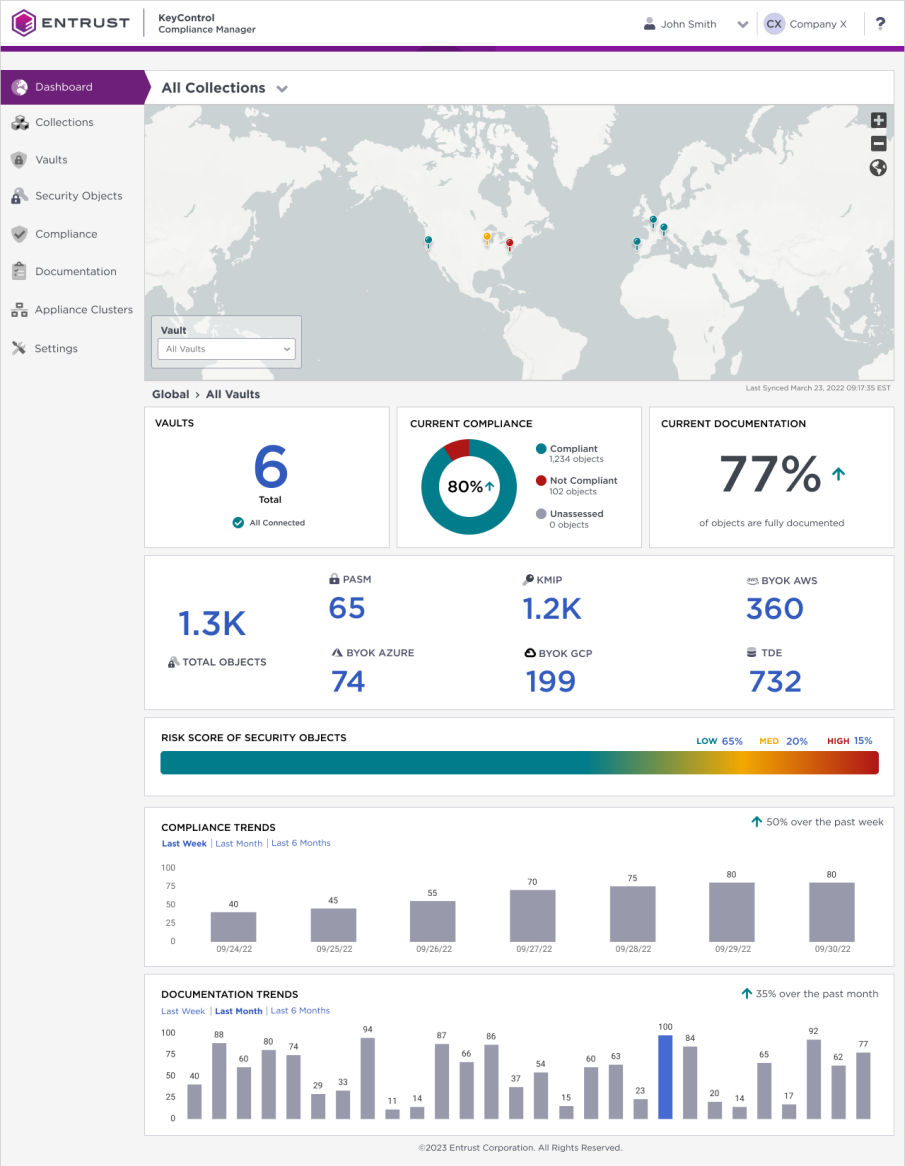


# Beyond just CLM

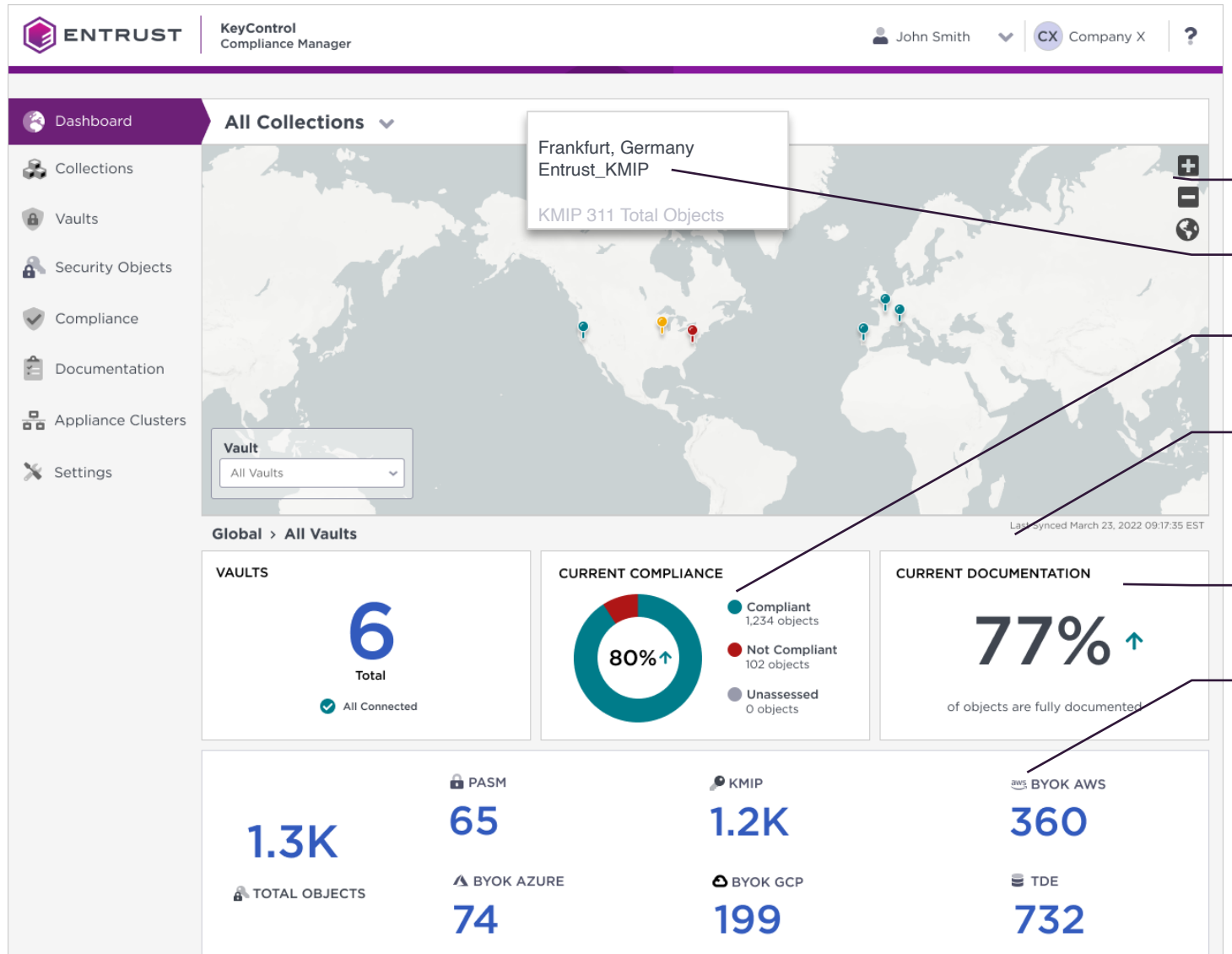


ENTRUST

# Enterprise-Wide Cryptographic Visibility



# Global view of keys and secrets



Protect and manage lifecycle of decentralized keys and secrets with centralized visibility and control

View where your Vaults are deployed

Zoom into any Vault to view its content

Assess compliance against policy

Apply Compliance Packs to add templates to dashboard to meet organizations' compliance needs

Assess level of documentation

Display properties of key and secrets

# CSP - Risk Management

ENTRUST

KeyControl  
Compliance Manager

John Smith

CX Company X

Dashboard

Collections

Vaults

Security Objects

Compliance

Documentation

Appliance Clusters

Settings

US HR Key

Cloud Key Management

Details

Compliance

Documentation

Vault

Vault One

Collection

US Account

HSM Protected

✓ Yes

Exportable

✓ No

Purpose

Test / Evaluation

Expires

August 9, 2023

Last Rotated

August 9, 2022 12:02 PM

Rotation Duration

Never

Cryptographic Algorithm

AES

Cryptographic Length

128

Generated

Local Cluster

Key Length

2048 Bit

TLS Version

1.2

GUID

12kd-343223-332-1124-4432

Created

Jan 1, 2022

Created By

jane.anderson@entrust.com

Risk Score

LOW

What does this mean?

✓ Compliant

View Compliance Results

✓ Documented

View Documentation

©2023 Entrust Corporation. All Rights Reserved.

ENTRUST

KeyControl  
Compliance Manager

John Smith

CX Company X

Dashboard

Collections

Vaults

Security Objects

Compliance

Documentation

Appliance Clusters

Settings

Security Objects

Keys and Secrets

Collection: All

Vault: All

Risk: All

More...

Search

Contains...

Columns

| Object Name | Collection | Vault          | Created (Age)           | Risk    |
|-------------|------------|----------------|-------------------------|---------|
| US HR Key   | Group US   | Vault One      | Jun 22, 2022 (3 months) | 92 HIGH |
| My Secret   | Group US   | Oracle Secrets | Jan 1, 2021 (1.8 years) | 85 HIGH |
| US Test Key | Group US   | KMIP Vault     | Aug 20, 2022 (2 days)   | 72 MED  |
| US Test Key | Group US   | Oracle GCP     | Aug 20, 2022 (2 days)   | 45 MED  |
| TDE Key     | Group US   | Oracle TDE     | Aug 20, 2022 (2 days)   | 10 LOW  |

1 - 5 Of 5

©2023 Entrust Corporation. All Rights Reserved.



# CSP- Documentation

Security Objects

Compliance

Documentation

Reports

Settings

Category: BYOK AWS

Created By: System

Last Modified: Jan 23, 2023 3:00 PM

Version: 1

Edit Metadata

This information is determined by the security objects metadata

Add or remove metadata

Key Length Expires Created Created By

User Input

This information is added by the objects owner or another user

Referenced by Compliance

Owner's Email Address

Referenced by Compliance

What is the purpose of this key?

Test / Evaluation

Development

Production

Why was this key created?

Max 300 characters

Key Usage Type

Select

What kind of compliance regulations are needed for this key?

Check all that apply

HIPAA

GDPR

CFI

FINMA

PCI-DSS

+ Add Field

Reorder Fields

Save as... Cancel

ENTRUST

KeyControl  
Compliance Manager

Dashboard

Collections

Vaults

Security Objects

Compliance

Documentation

Settings

Documentation

Manage templates to document security objects

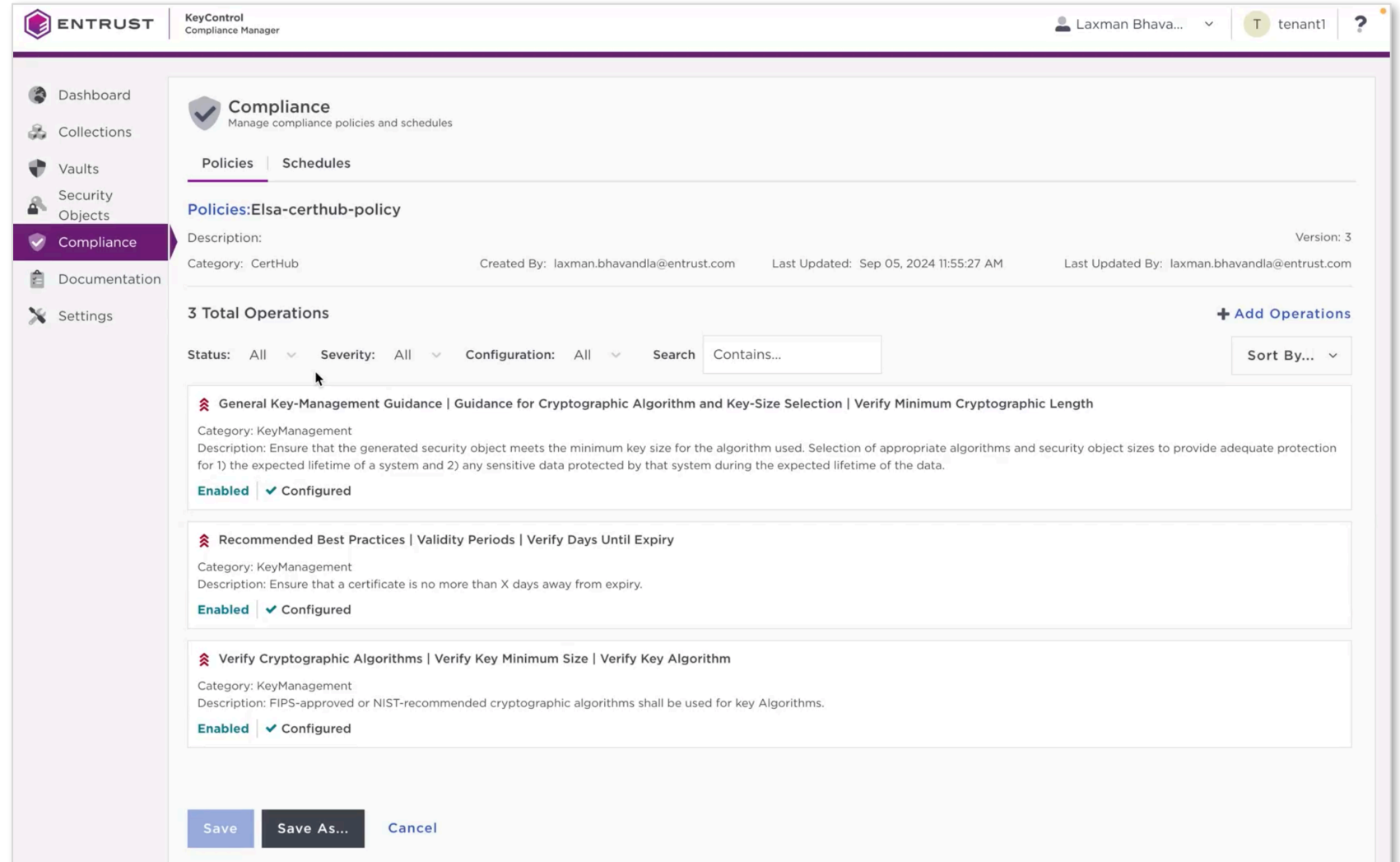
Templates

| Name                  | Description                   | Category     | Created By |
|-----------------------|-------------------------------|--------------|------------|
| AWS documentation     | documentation for AWS BYOK    | BYOK (AWS)   | System     |
| Azure documentation   | documentation for Azure BY... | BYOK (AZURE) | System     |
| KMIP documentation    | documentation for KMIP        | KMIP Objects | System     |
| Secrets documentation | documentation for Secrets     | Secrets      | System     |



# Automated Compliance Enforcement

- Configurable policy audit automatically run on customer-defined schedules
- With reporting & visibility segregated and distinct from operations



The screenshot displays the ENTRUST KeyControl Compliance Manager interface. The left sidebar contains navigation links: Dashboard, Collections, Vaults, Security Objects, Compliance (selected), Documentation, and Settings. The main content area is titled 'Compliance' with the subtitle 'Manage compliance policies and schedules'. It features tabs for 'Policies' and 'Schedules'. Under the 'Policies' tab, the selected policy is 'Elsa-certhub-policy'. The policy details include a description, category (CertHub), creator (laxman.bhavandla@entrust.com), and creation/last updated dates (Sep 05, 2024 11:55:27 AM). Below the details, it shows '3 Total Operations' with a '+ Add Operations' button. A filter section includes 'Status: All', 'Severity: All', 'Configuration: All', a search box with 'Contains...', and a 'Sort By...' dropdown. The list of operations includes:

- General Key-Management Guidance | Guidance for Cryptographic Algorithm and Key-Size Selection | Verify Minimum Cryptographic Length**  
Category: KeyManagement  
Description: Ensure that the generated security object meets the minimum key size for the algorithm used. Selection of appropriate algorithms and security object sizes to provide adequate protection for 1) the expected lifetime of a system and 2) any sensitive data protected by that system during the expected lifetime of the data.  
Status: Enabled | Configured
- Recommended Best Practices | Validity Periods | Verify Days Until Expiry**  
Category: KeyManagement  
Description: Ensure that a certificate is no more than X days away from expiry.  
Status: Enabled | Configured
- Verify Cryptographic Algorithms | Verify Key Minimum Size | Verify Key Algorithm**  
Category: KeyManagement  
Description: FIPS-approved or NIST-recommended cryptographic algorithms shall be used for key Algorithms.  
Status: Enabled | Configured

At the bottom, there are buttons for 'Save', 'Save As...', and 'Cancel'.

# Enterprise-Wide Cryptographic Visibility

01

## Comprehensive Visibility

Unified dashboards deliver complete visibility and governance across your entire cryptographic ecosystem.

02

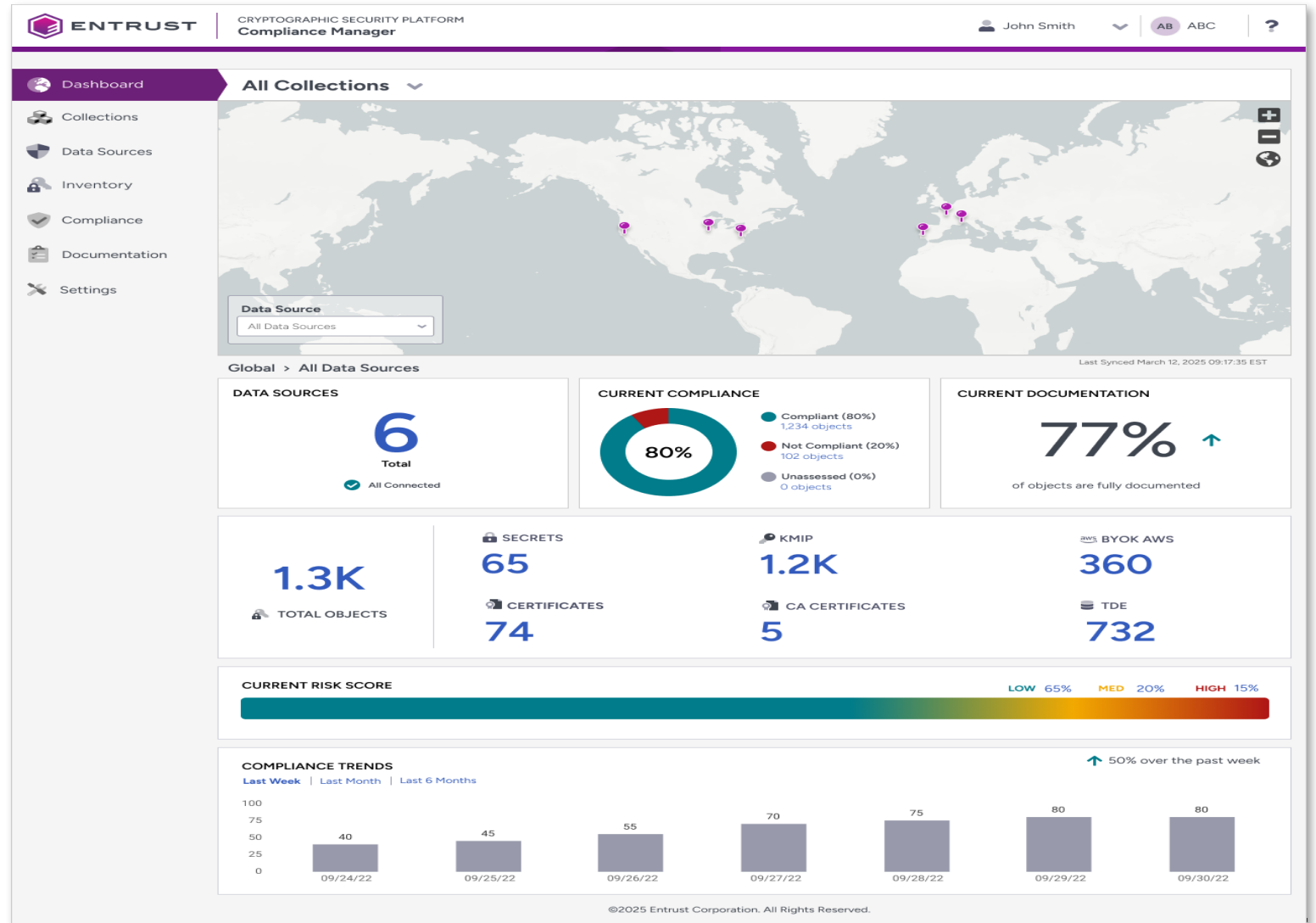
## Data Sources

CSP delivers extensive integrations capabilities across PKI, secrets management, and vault solutions, simplifying your security operations and enhancing agility.

03

## Robust Reporting

Gain continuous visibility by tracking and monitoring changes in your cryptographic security posture, enabling proactive risk management and enhancing compliance.





# Out-of-the-Box Compliance Policies

01

## Out-of-the-Box Policy

Configurable policy audits automatically (on customer-defined schedules), with reporting and visibility segregated and distinct from operations.

02

## Industry Standards

Standards-based and best-practice policies tailored to cryptographic objects (e.g. keys and certificates) and their context (e.g., cloud storage, HSMs, VMs).

03

## Extensible Operations

Capability to incorporate additional security operations tailored to customer requirements.

The screenshot displays the Entrust Compliance Manager interface. The top navigation bar includes the Entrust logo, the title 'CRYPTOGRAPHIC SECURITY PLATFORM Compliance Manager', and user information 'John Smith'. A sidebar on the left contains navigation links: Dashboard, Collections, Data Sources, Security Objects, Compliance (selected), Documentation, Appliance Clusters, and Settings. The main content area is titled 'Compliance' and 'Manage compliance policies and schedules'. It features tabs for 'Policies' and 'Schedules'. The 'Schedules' tab is active, showing a breadcrumb trail: 'Schedules > Last Run Summary > Vault Results'. Below this, the selected policy is 'CSP - CLM'. The report details the 'Policy' as 'Entrust Best Practice Reference Policy - CertHub' and the 'Schedule' as 'Certificate-Compliance'. It shows the 'Start Time' as 'Mar 20, 2025 08:15:57 AM' and the 'Elapsed Time' as '00:01:06'. A progress indicator shows '0%' completion. The 'Total Operations (14)' are listed with a search bar and a 'View' link. A table summarizes the results:

| Operation                                | Failed Objects | Passed Objects | Skipped Objects |
|------------------------------------------|----------------|----------------|-----------------|
| Verify Minimum Cryptographic Length      | 0              | 1805           | 0               |
| Verify Cryptographic Algorithm           | 0              | 1805           | 0               |
| Verify Owner Existence                   | 0              | 1805           | 0               |
| Verify Certificate Type Version          | 0              | 1805           | 0               |
| Verify Empty Subject                     | 0              | 1805           | 0               |
| Verify Weak or Disallowed Algorithms     | 0              | 1805           | 0               |
| Verify Approved Subject DNs              | 1805           | 0              | 0               |
| Verify Days Until Expiry                 | 1805           | 0              | 0               |
| Verify Max Validity Period               | 1799           | 6              | 0               |
| Verify Approved SAN                      | 1804           | 1              | 0               |
| Verify Approved Issuer                   | 1805           | 0              | 0               |
| Verify CRL Distribution Points Existence | 1805           | 0              | 0               |
| Verify OCSP Existence                    | 1805           | 0              | 0               |
| Validate Wildcard SAN                    | 1805           | 0              | 0               |

# Global Compliance Oversight for your Cryptographic Estate

## 1. Unified Visibility

Gain centralized insight into all cryptographic assets—keys, secrets, and certificates—across cloud and on-prem environments.

## 2. Automated Compliance

Enforce standards like PCI DSS and NIST automatically, with customizable policy support for continuous compliance.

## 3. Multi-Cloud Ready

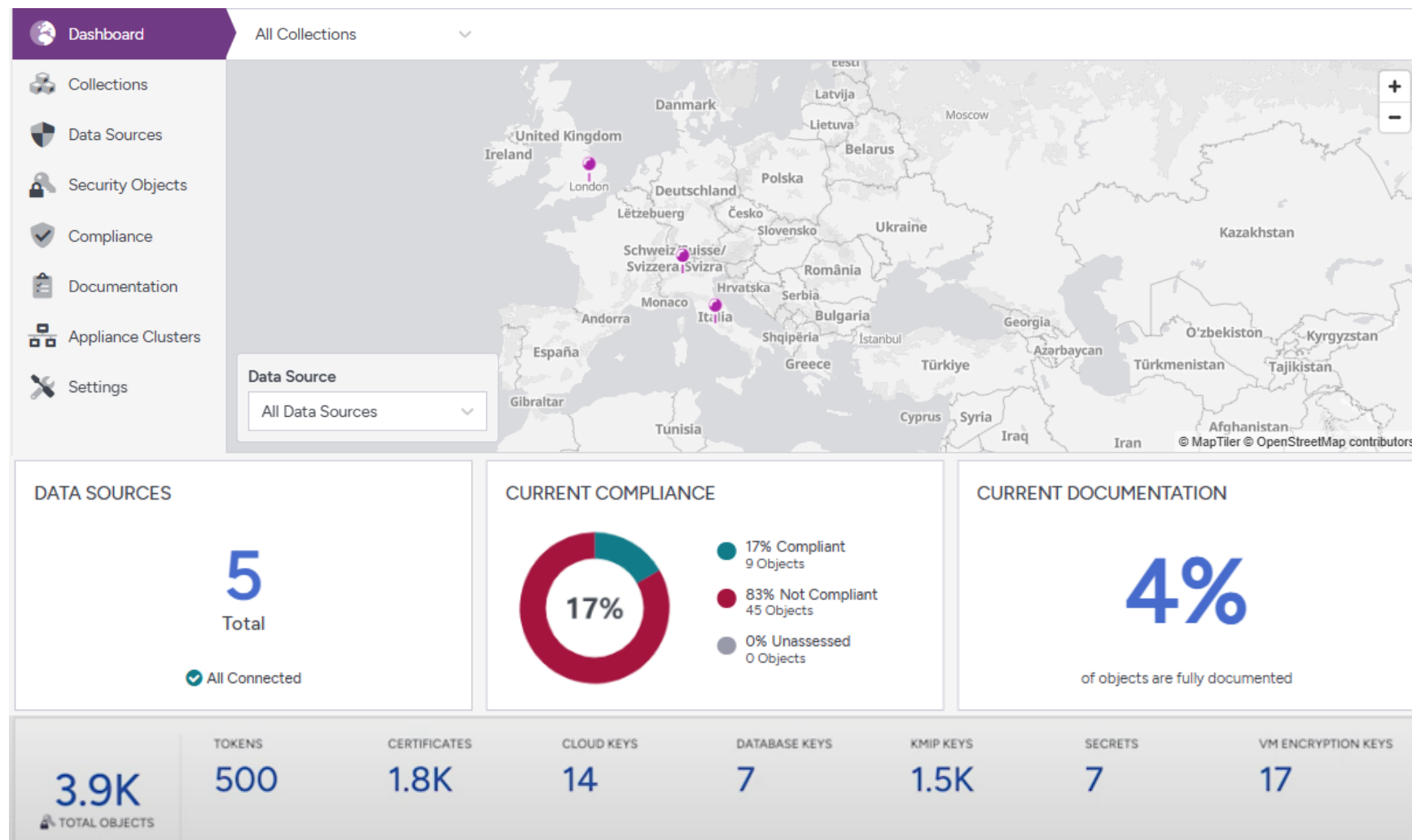
Seamlessly integrates with AWS, Azure, Google Cloud, Oracle, and Salesforce for consistent policy enforcement.

## 4. Enterprise-Grade Security

Features include high availability, role-based access, dual control, and multitenancy for secure operations.

## 5. Audit & Forensics

Maintain detailed logs and export forensic data to simplify audits and support incident investigations.



# Risk Scoring

## 1. Clear Visibility into Cryptographic Risk

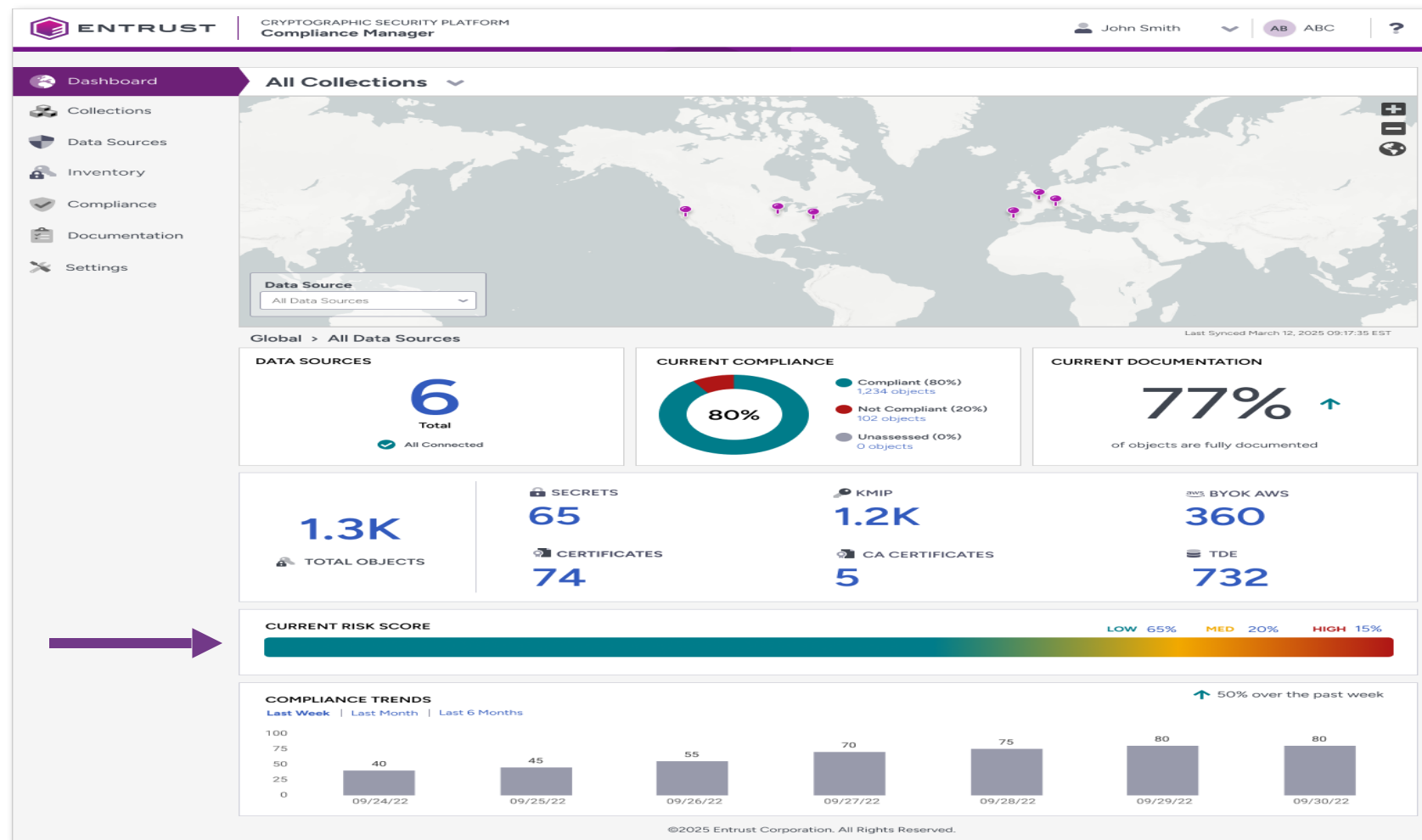
Gain a quantifiable view of your cryptographic posture, enabling data-driven decisions and prioritization of high-risk assets.

## 2. Automated, Policy-Based Risk Detection

Continuously monitor and flag non-compliant or vulnerable assets using customizable policies—reducing manual oversight and human error.

## 3. Streamlined Operations and Audit Readiness

Improve efficiency across teams and geographies with automated assessments, ensuring faster response times and simplified audit preparation.



# Köszönöm

**entrust.com**

© Entrust Corporation



**ENTRUST**

SECURING A WORLD IN MOTION