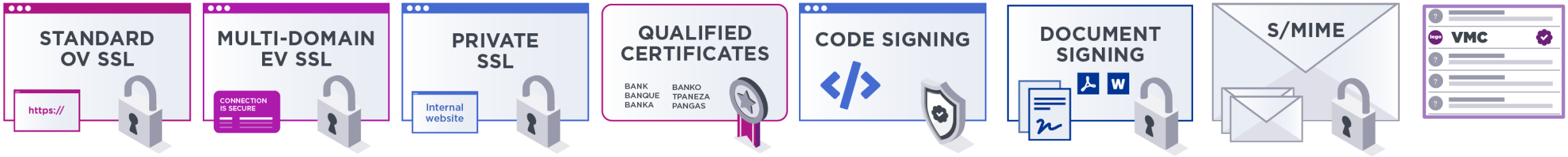
Entrust Certificate Management

Richard Palmer
Territory Manager CEE

April 2026

ENTRUST
SECURING A WORLD IN MOTION

Digital Certificate & Cryptography – A complex ecosystem



PQ
Certificate
&
Cryptography

ENTRUST

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

National ID

DevOps

IoT

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**"

ENTRUST

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

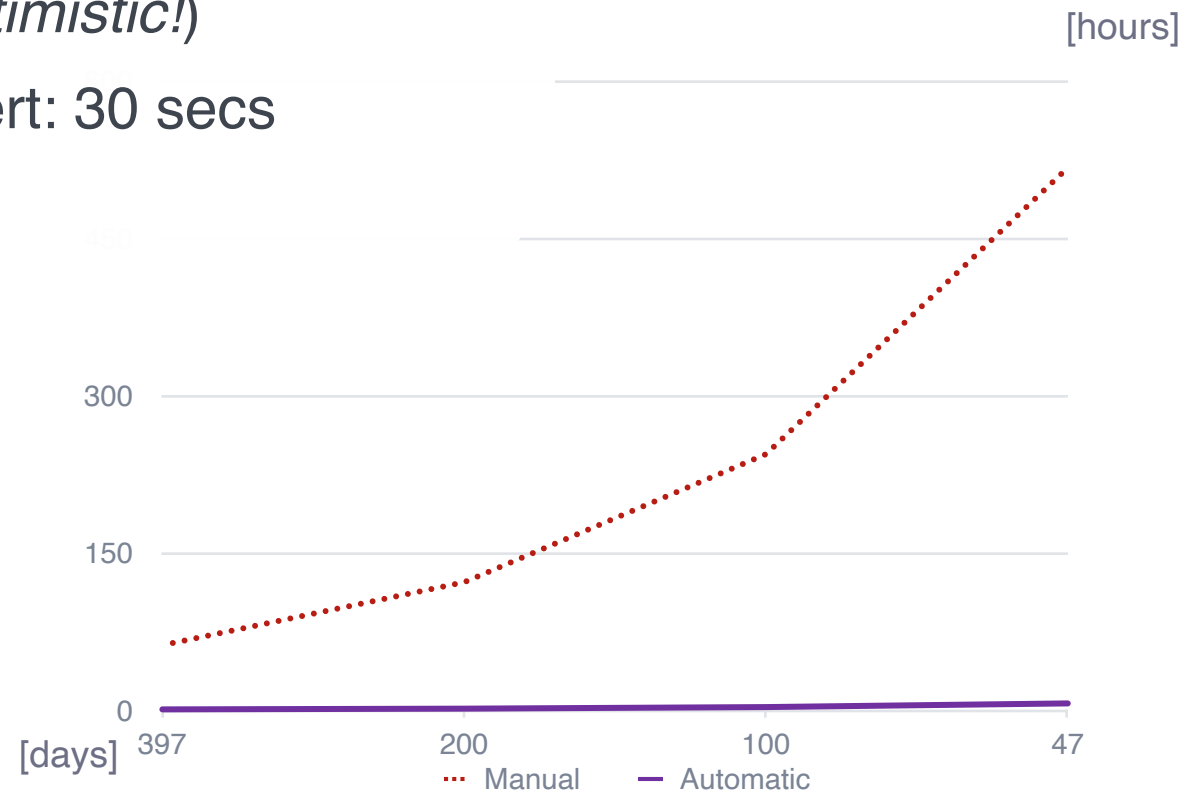
Downtime and 15.4% experienced 25 hours or more from certificate-related issues

ENTRUST

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



ENTRUST

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**

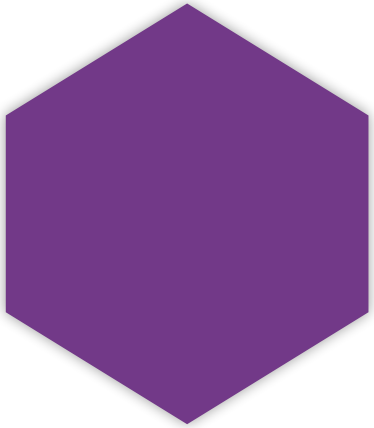
	Manual Management	Automated CLM	Impact
Labor required per 100 certificates/year	**~500+ hours**	**10 hours or less**	~96% time saved
Outage risk due to certificate expiry	**High**	**Near zero**	Service reliability dramatically improved
Operator intervention per event	**Multiple steps**	**Single click/minimal/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

ENTRUST

Significant Outages Due to TLS/SSL Certificate Expiration

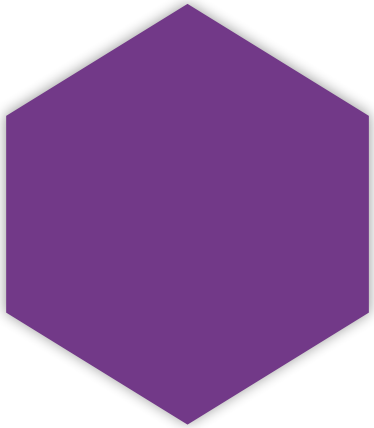
Years	Organization	Cause	Impact
2020	Microsoft Teams	An **expired authentication certificate**.	A **three-hour outage** preventing approximately 20 million daily users from signing in or accessing the collaboration service
2021	Google Voice	An **expired TLS certificate** in the Google Voice frontend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

Certifiate Management - Automating Machine Identity Management With Zero-Trust Principle



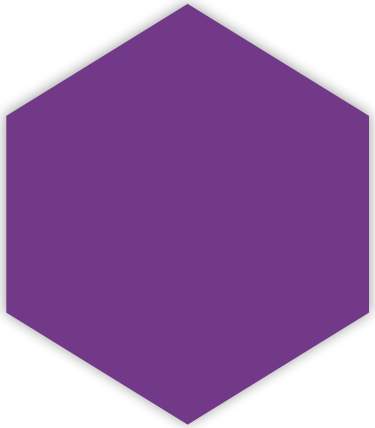
Automated inventory and visibility

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



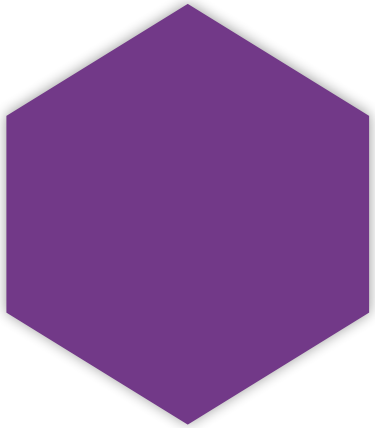
Policy Enforcement

- 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

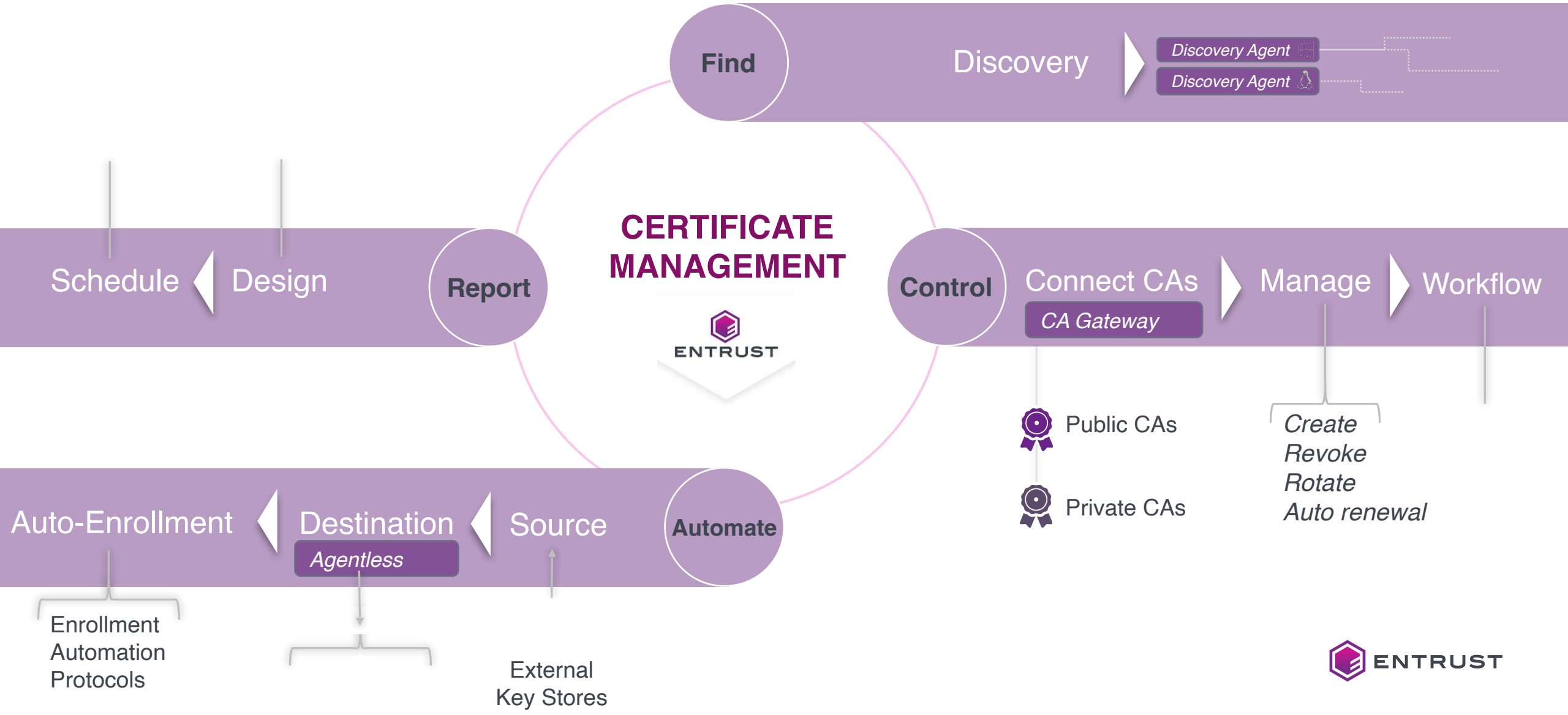


Monitoring – Alerts and Notifications

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

ENTRUST

CSP – Certificate Management

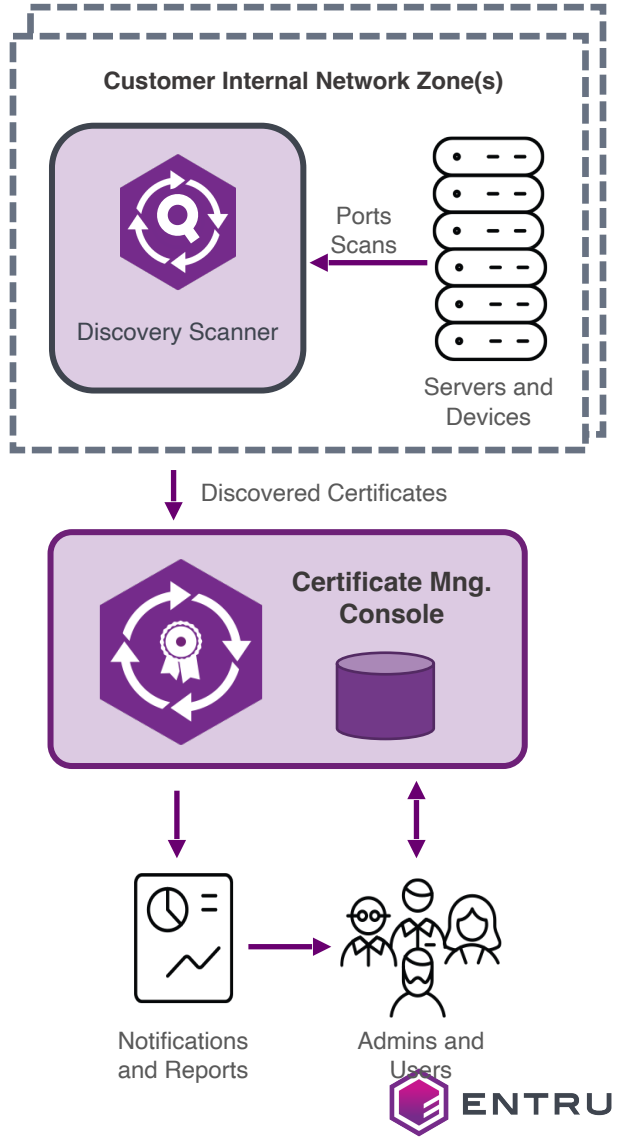


ENTRUST

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

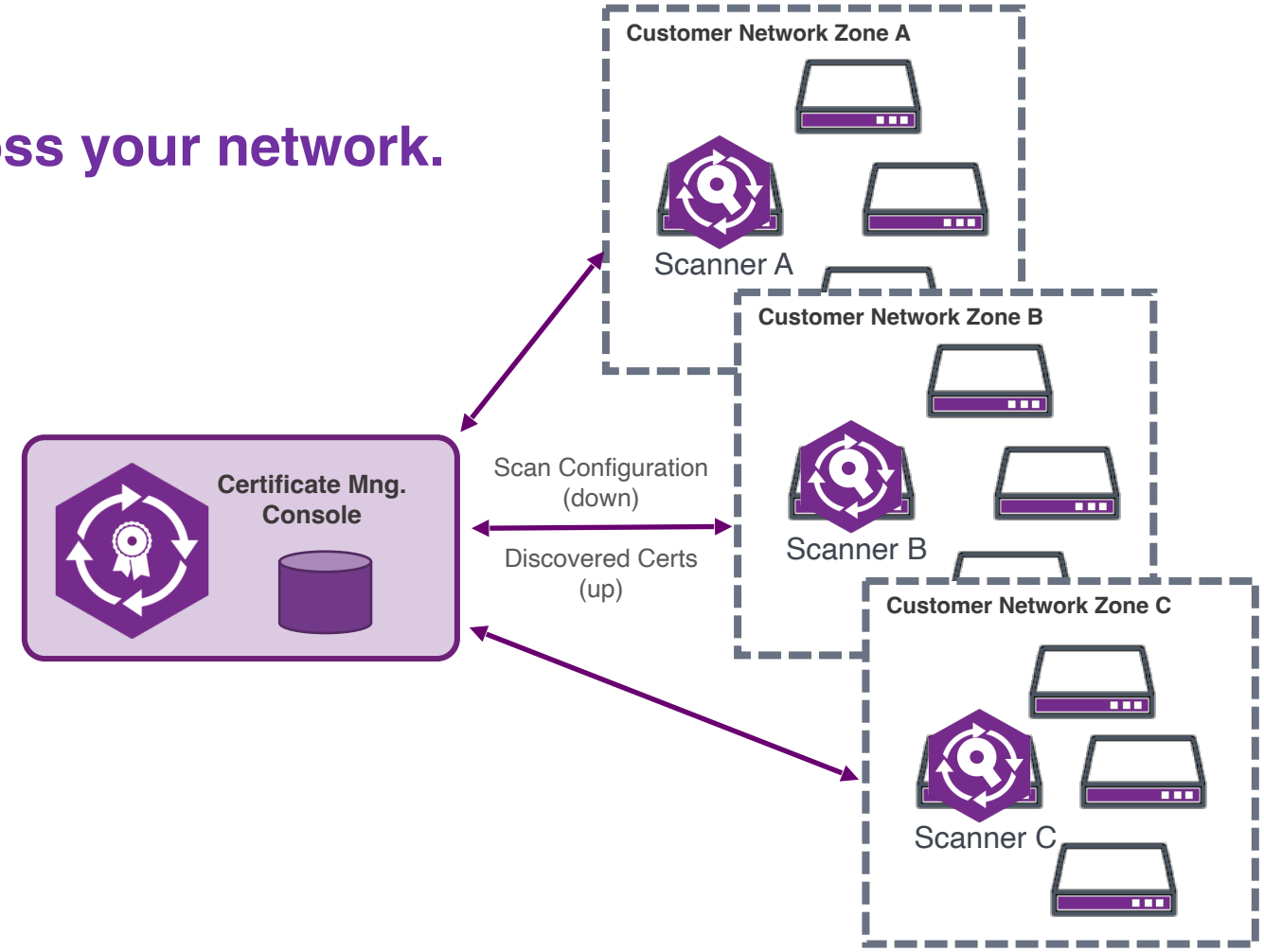


ENTRUST

Certificate Management – Discovery Scanner

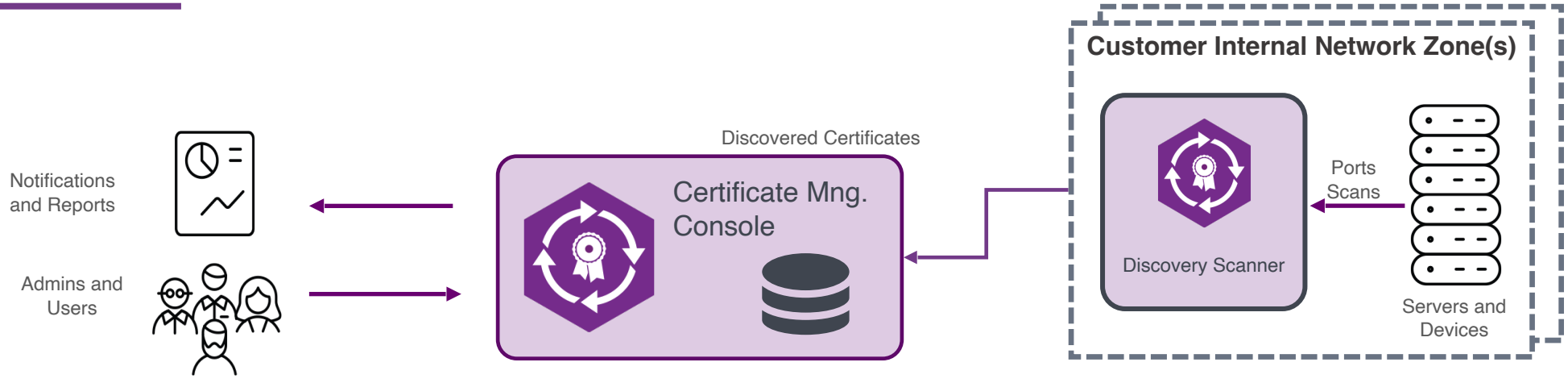
Find x.509 certificates on servers across your network.

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



ENTRUST

Certificate Management – Find

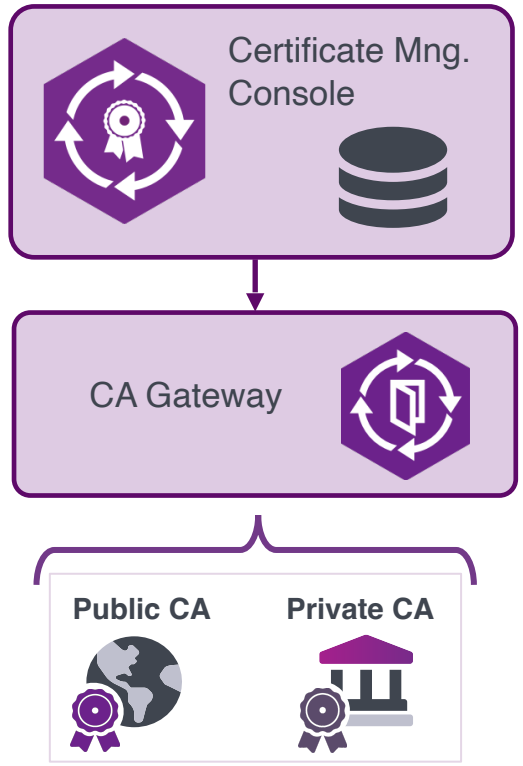


ENTRUST

Certificate Management — Establish Control of the CAs

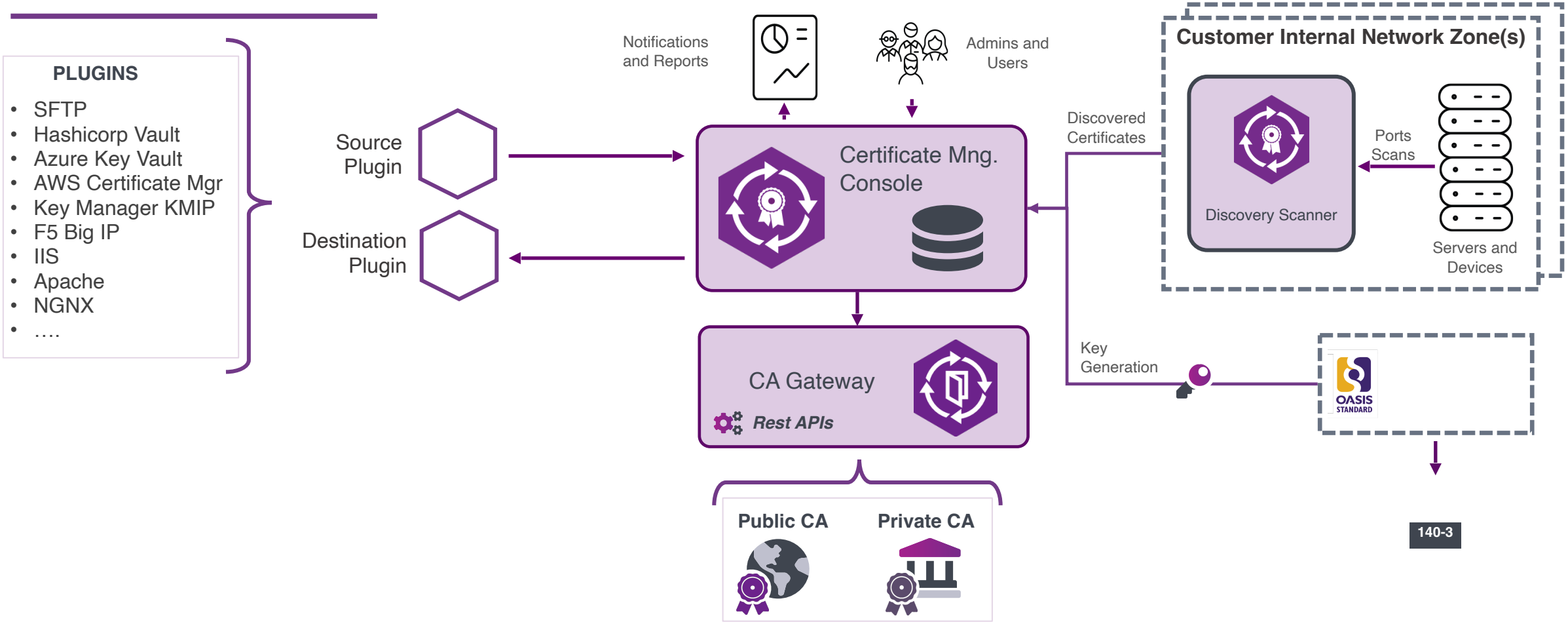
You need a Single Plane of Glass for all your Certificate Authorities

- 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.



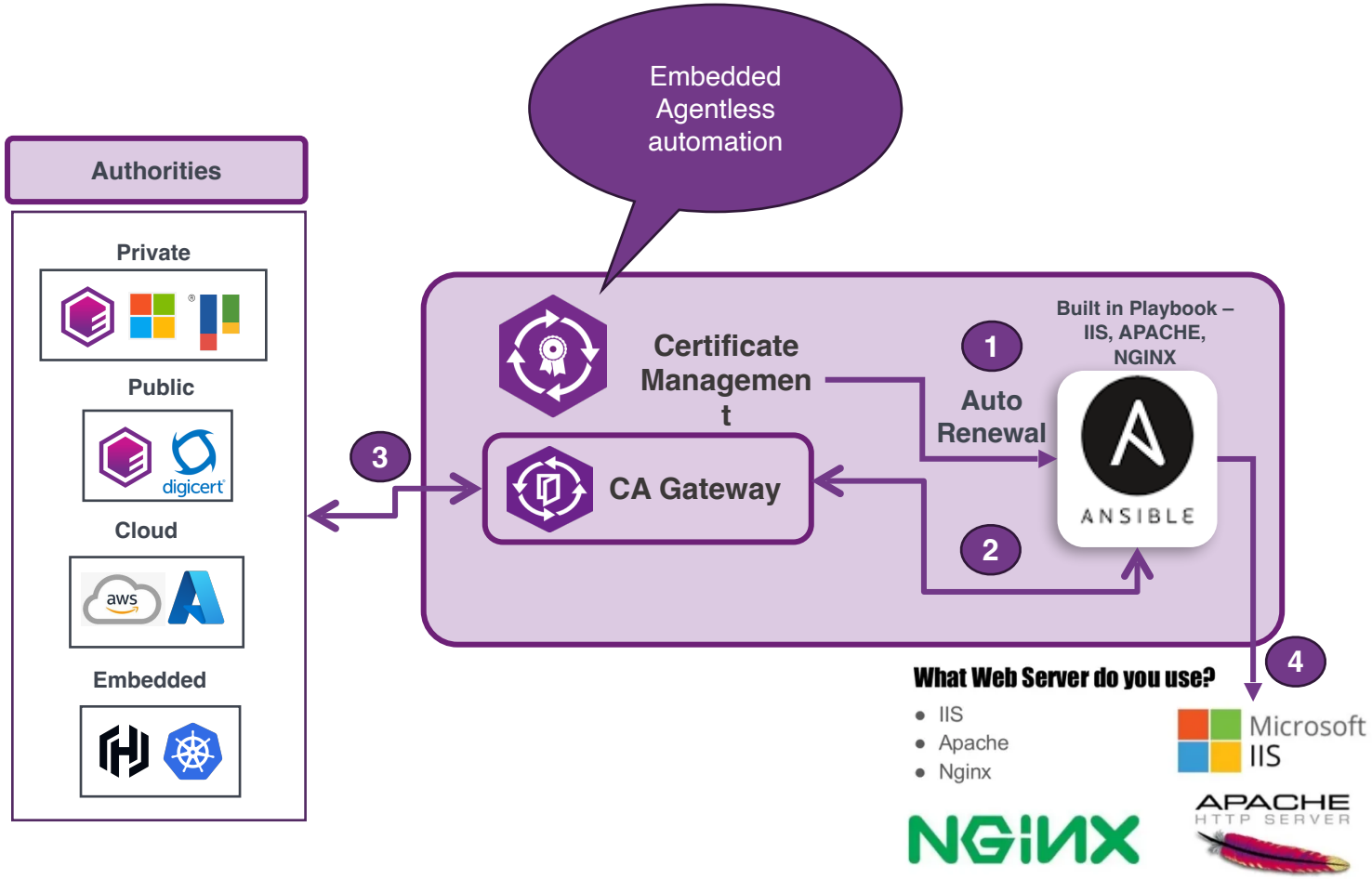
ENTRUST

Certificate Management – Control



ENTRUST

Agentless Certificate Management



1-Auto renewal triggered (Assumption : Authentication configuration to the web server is already set up)

2 & 3. Playbook to initiate CSR submission to the CA via CAGW

4. Playbook to push the generated certificated to the Webserver as per the Auto renewal set up

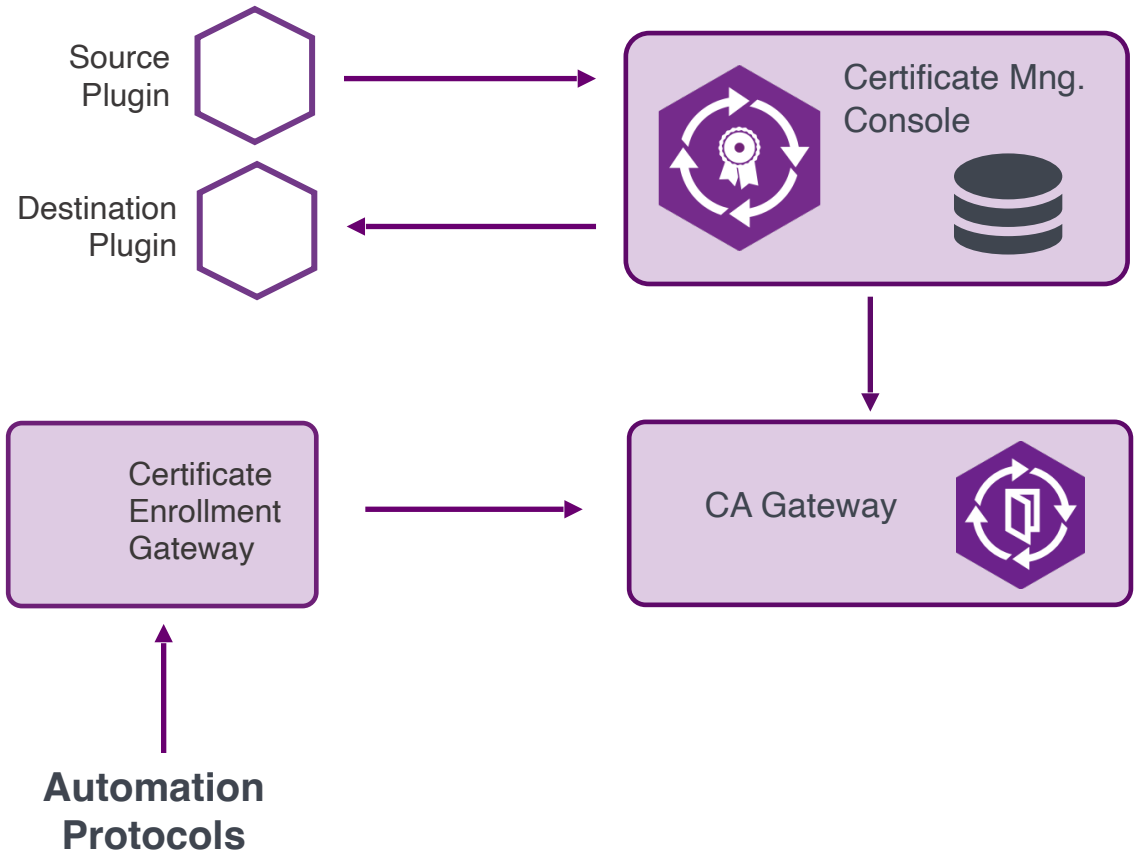
Agentless = Customers don't need to install any additional infrastructure/agents

ENTRUST

Certificate Management — Automate Issuance and Renewal

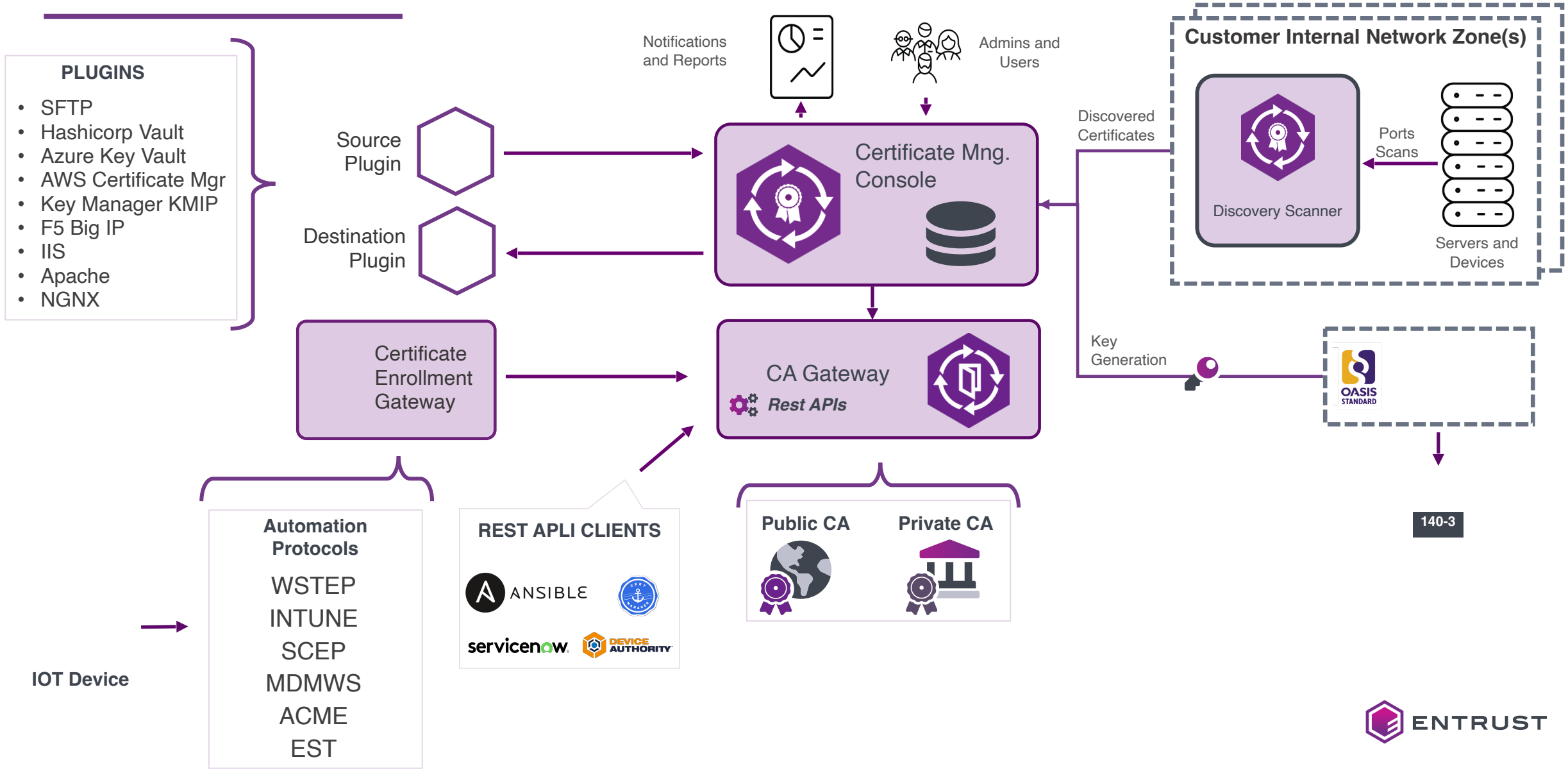
Automation is Key to Preventing Outages and Exposures

- 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



ENTRUST

Certificate Management – Automate



ENTRUST

Beyond just CLM

ENTRUST

Enterprise-Wide Cryptographic Visibility

Policy management

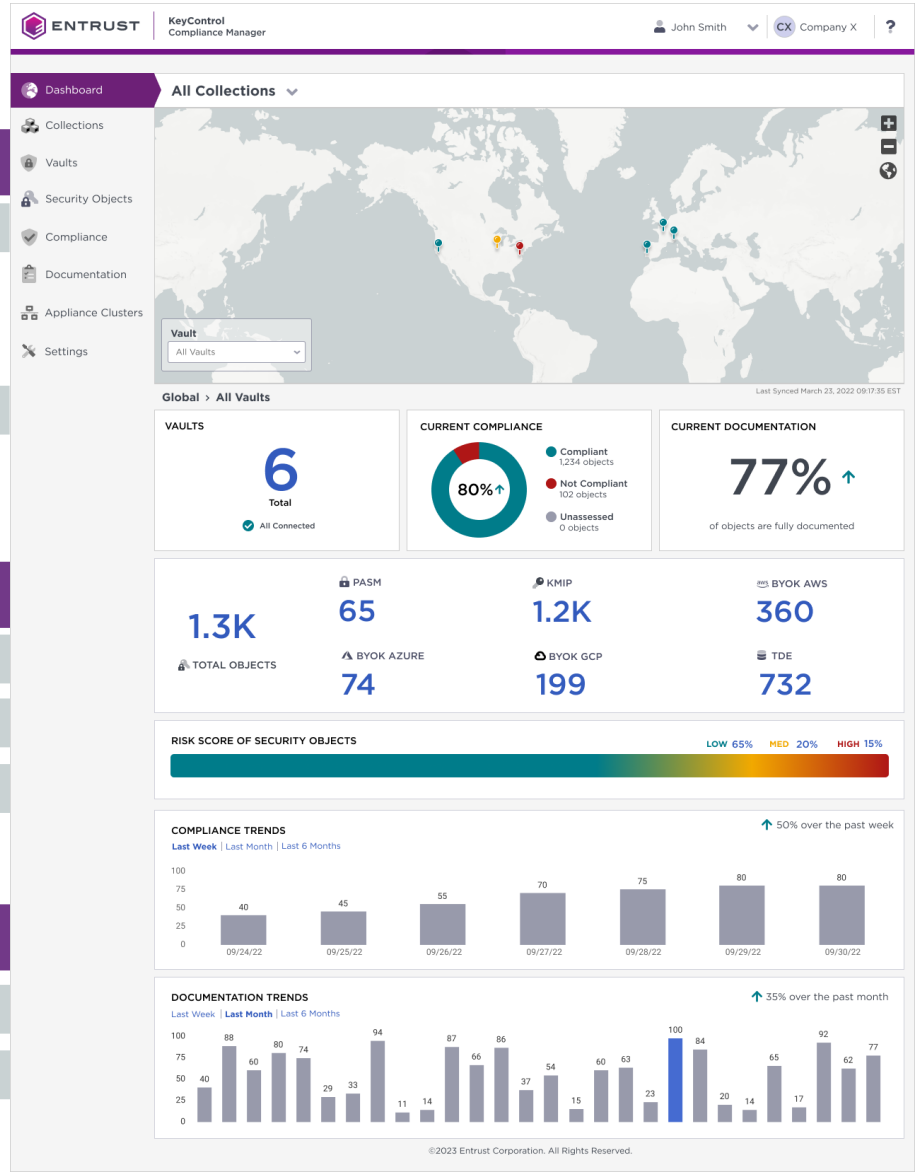
- Industry Standard Policies
- Own written Policies

Risk management

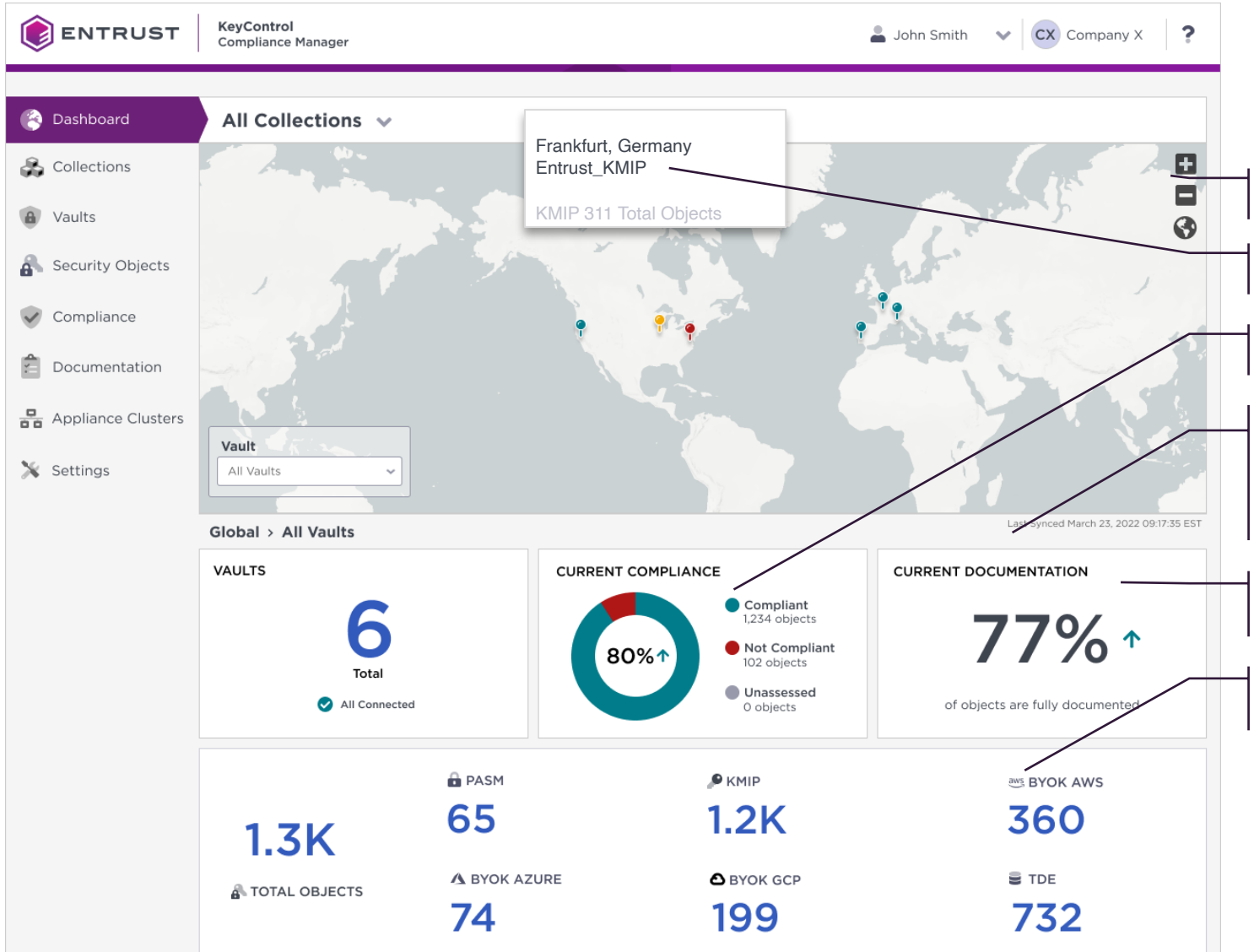
- Calculate risk
- Compliance level
- Compliance trending

Process enablement

- Request Documentation
- Info & Alert



Global view of keys and secrets

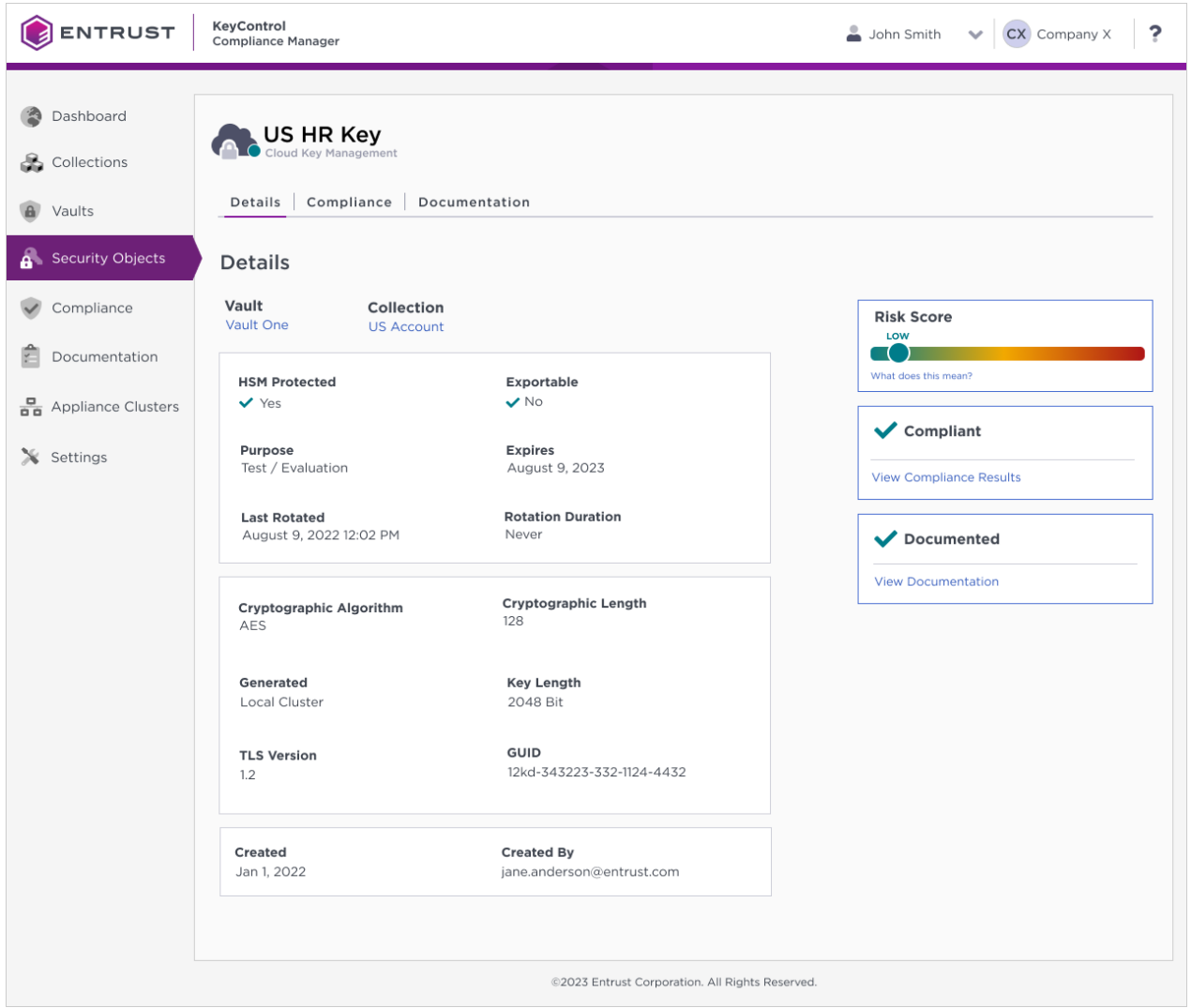


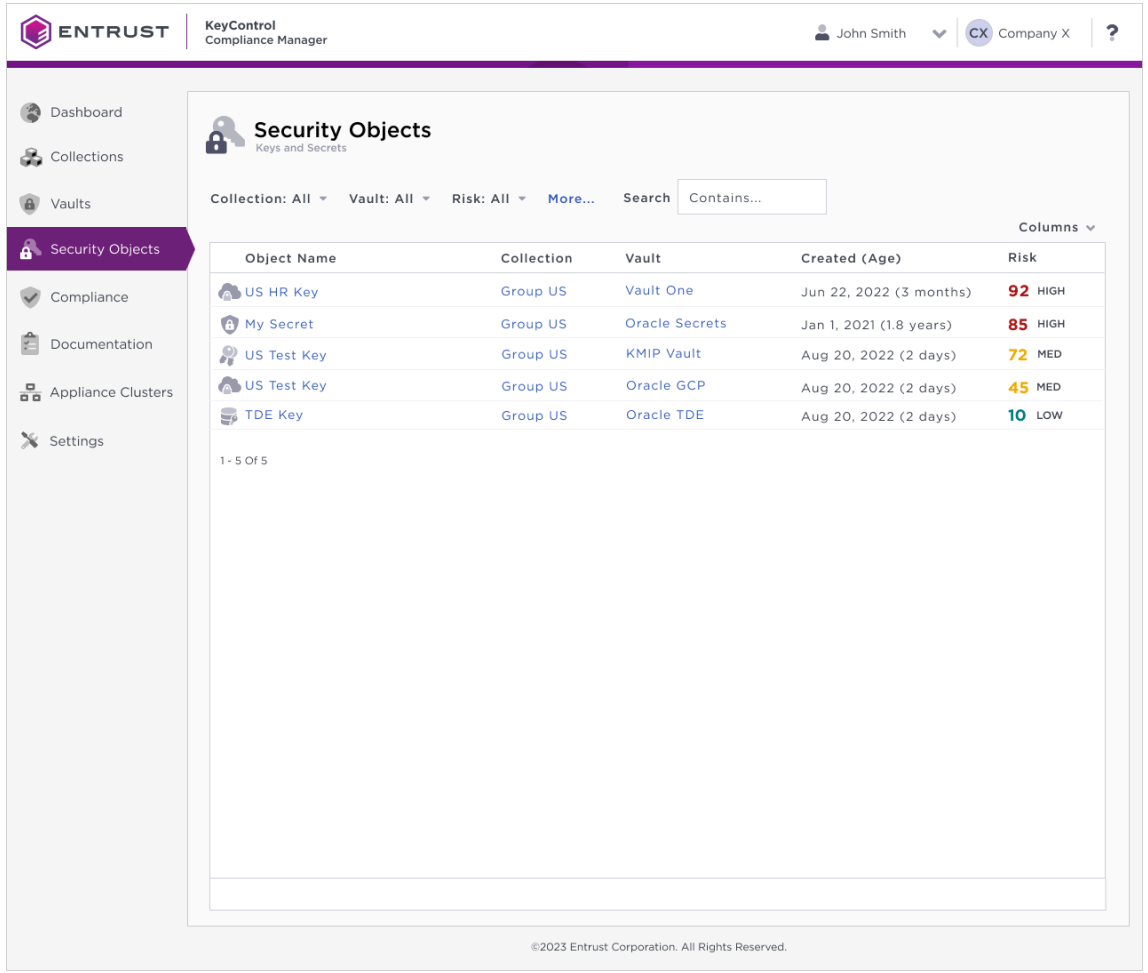
Protect and manage lifecycle of decentralized keys and secrets with centralized visibility and control

- 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

ENTRUST

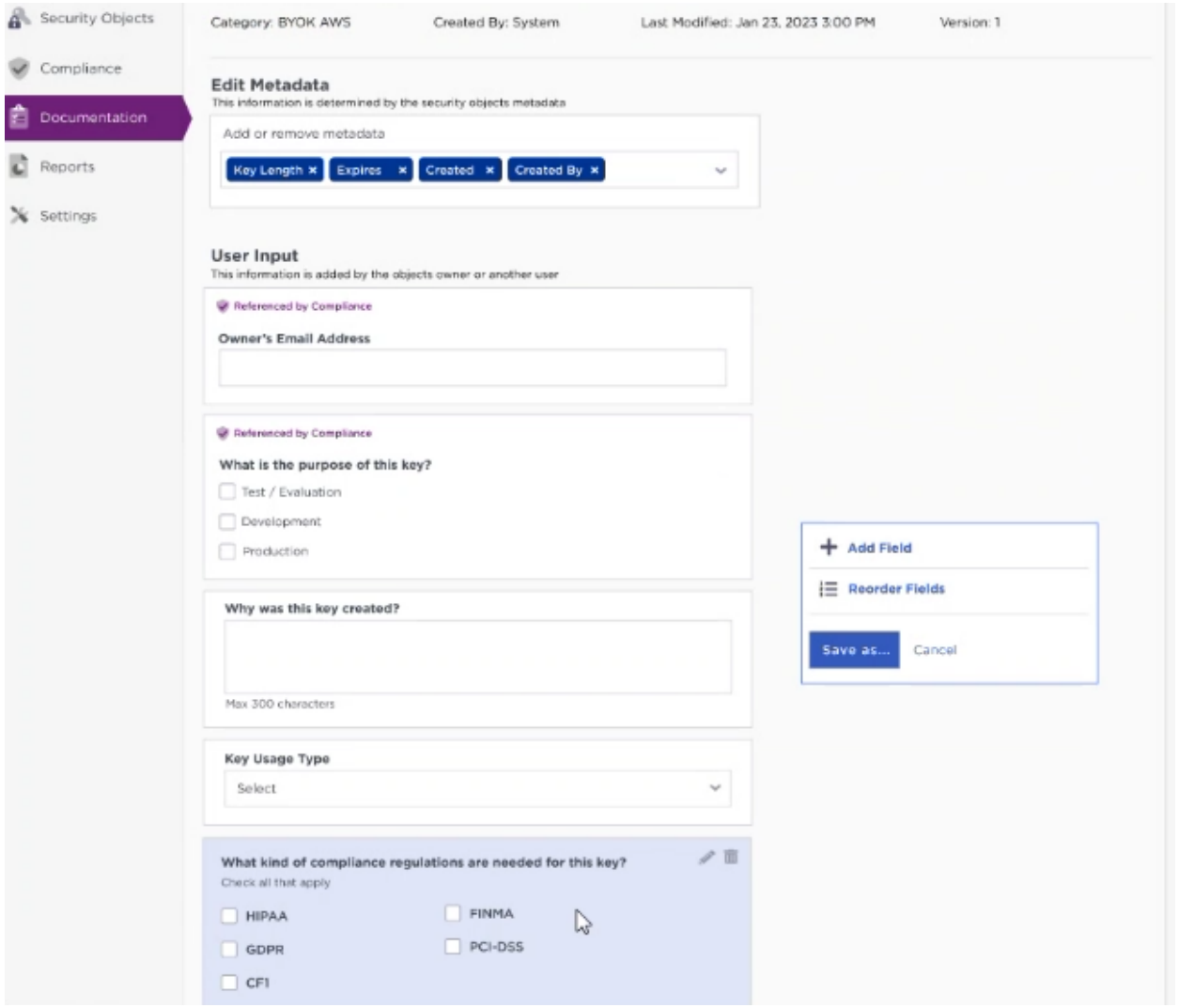
CSP - Risk Management

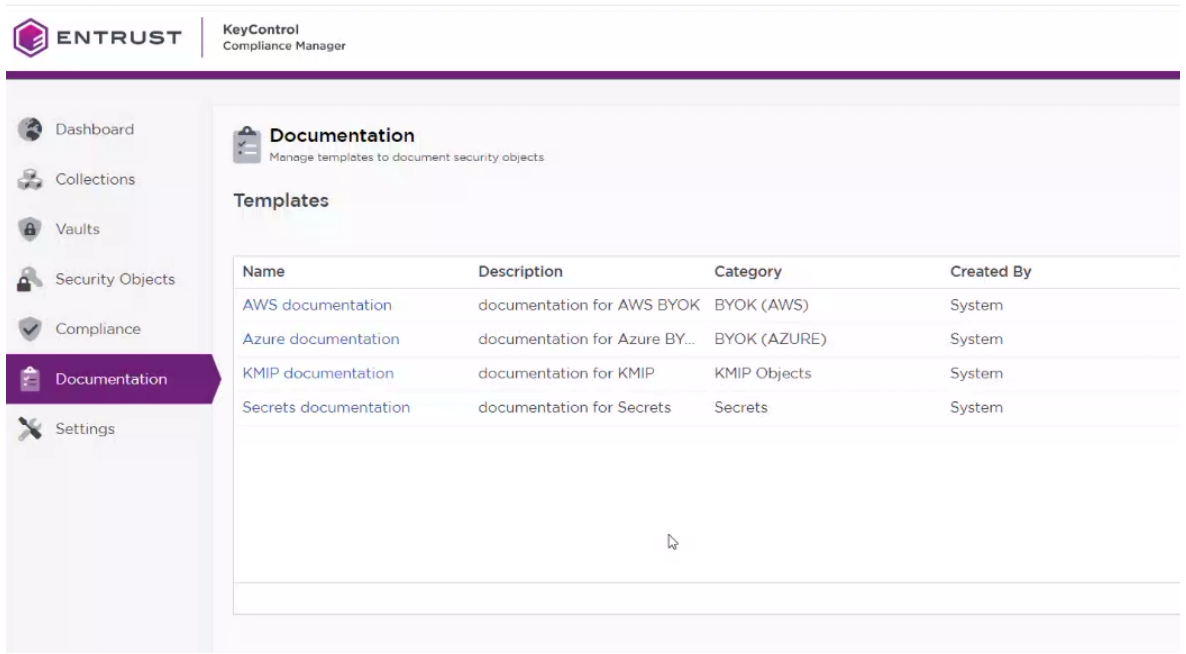




ENTRUST

CSP- Documentation

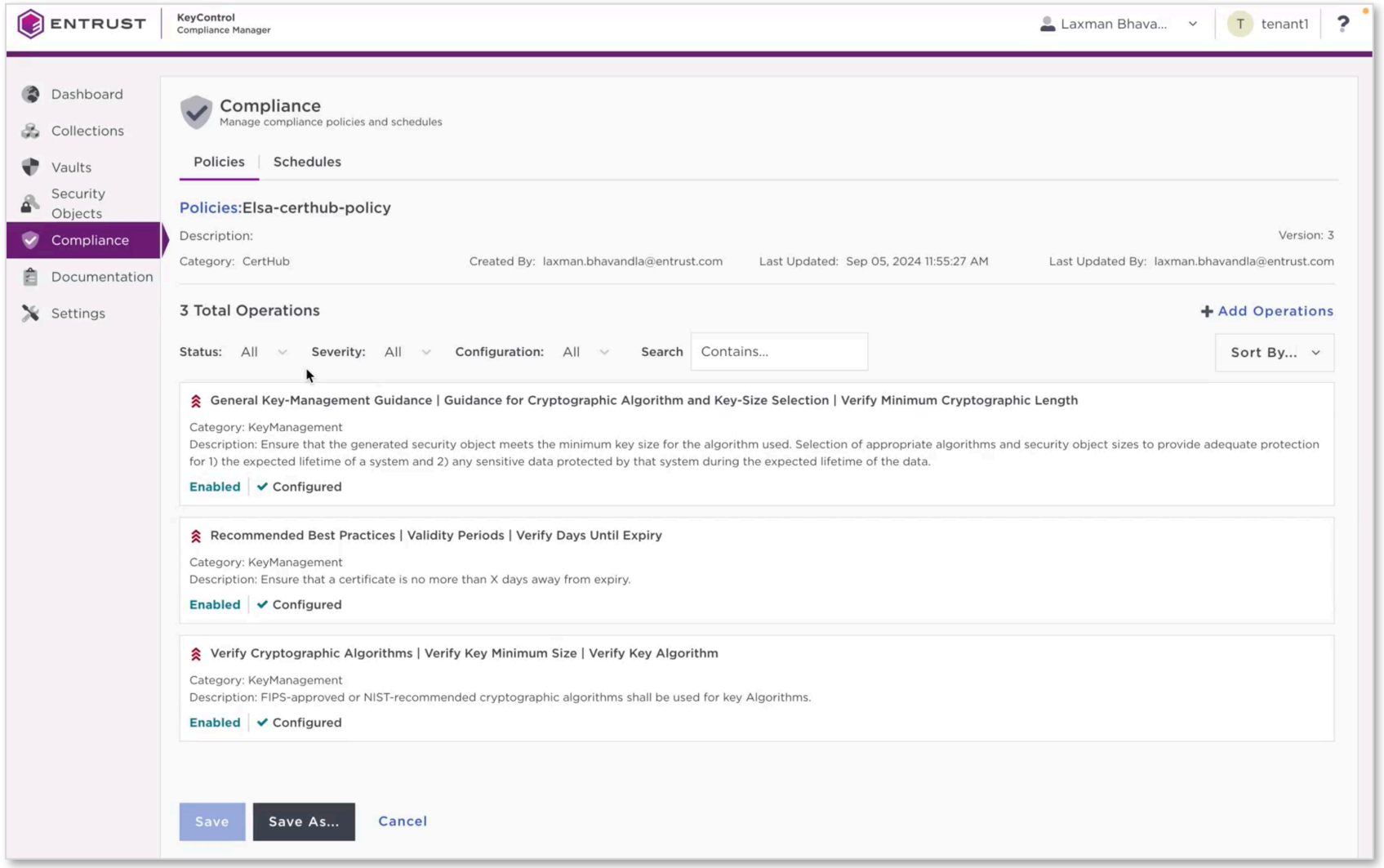




ENTRUST

Automated Compliance Enforcement

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



ENTRUST

Enterprise-Wide Cryptographic Visibility

01

Comprehensive Visibility

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

02

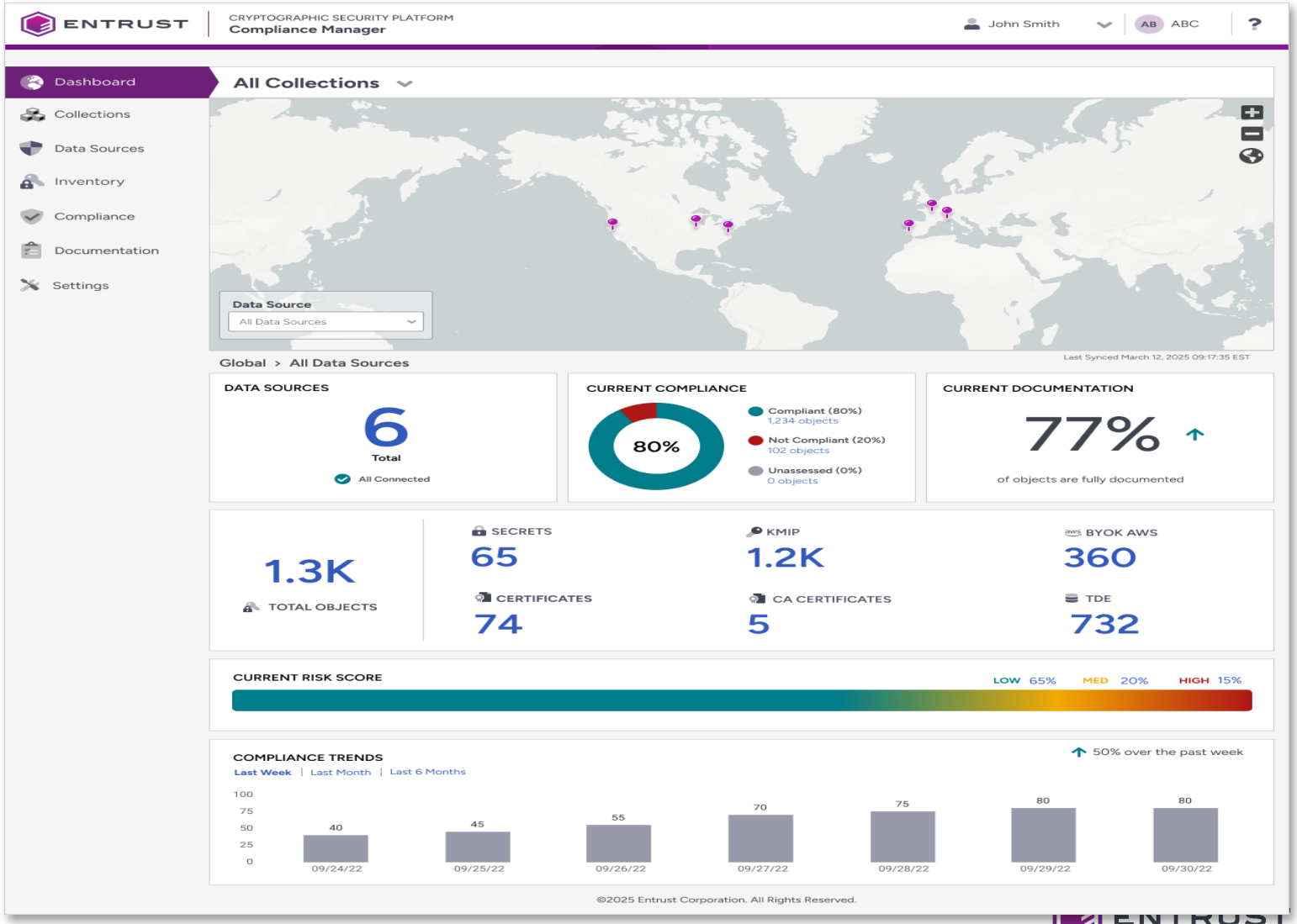
Data Sources

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

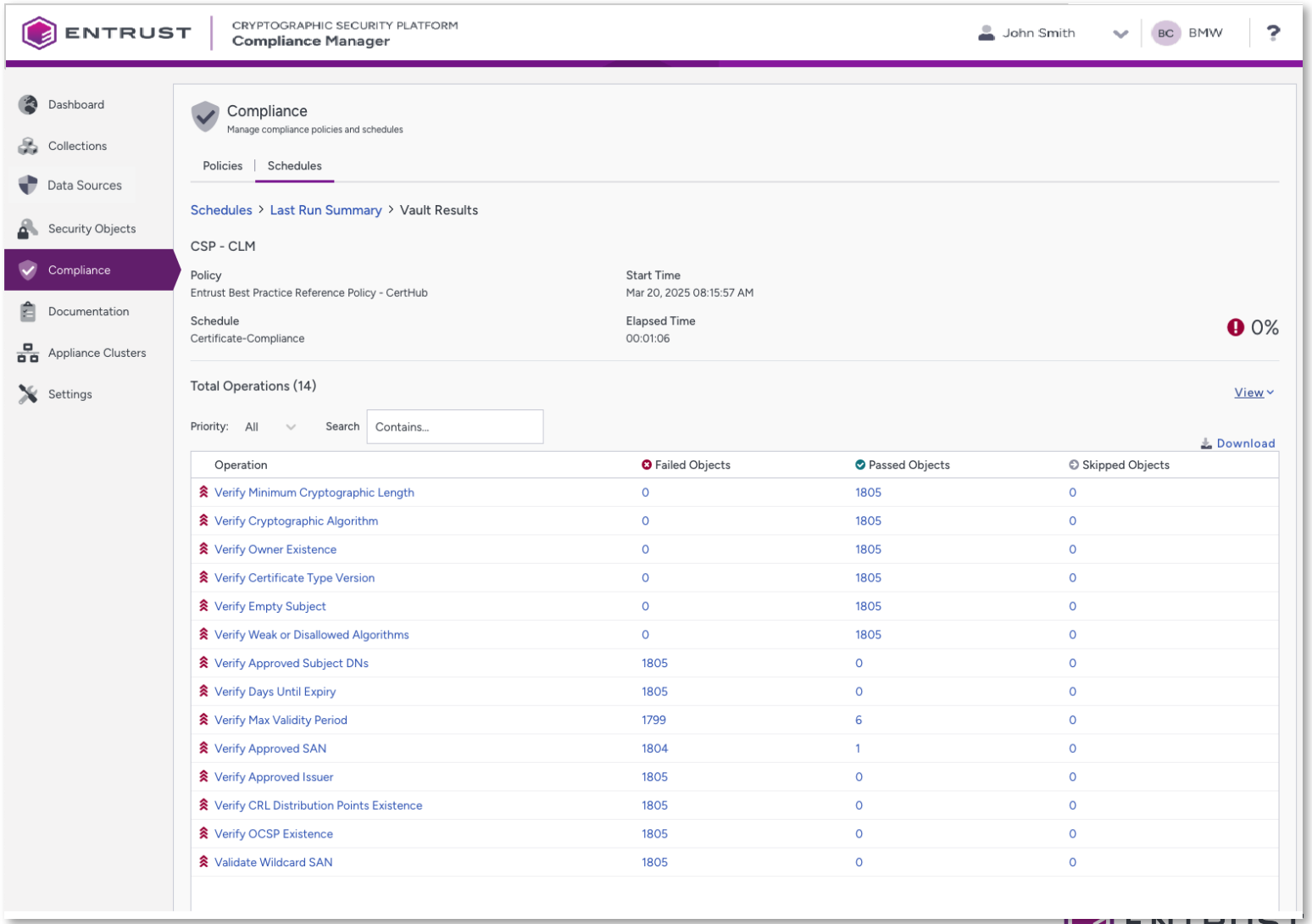
Industry Standards

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

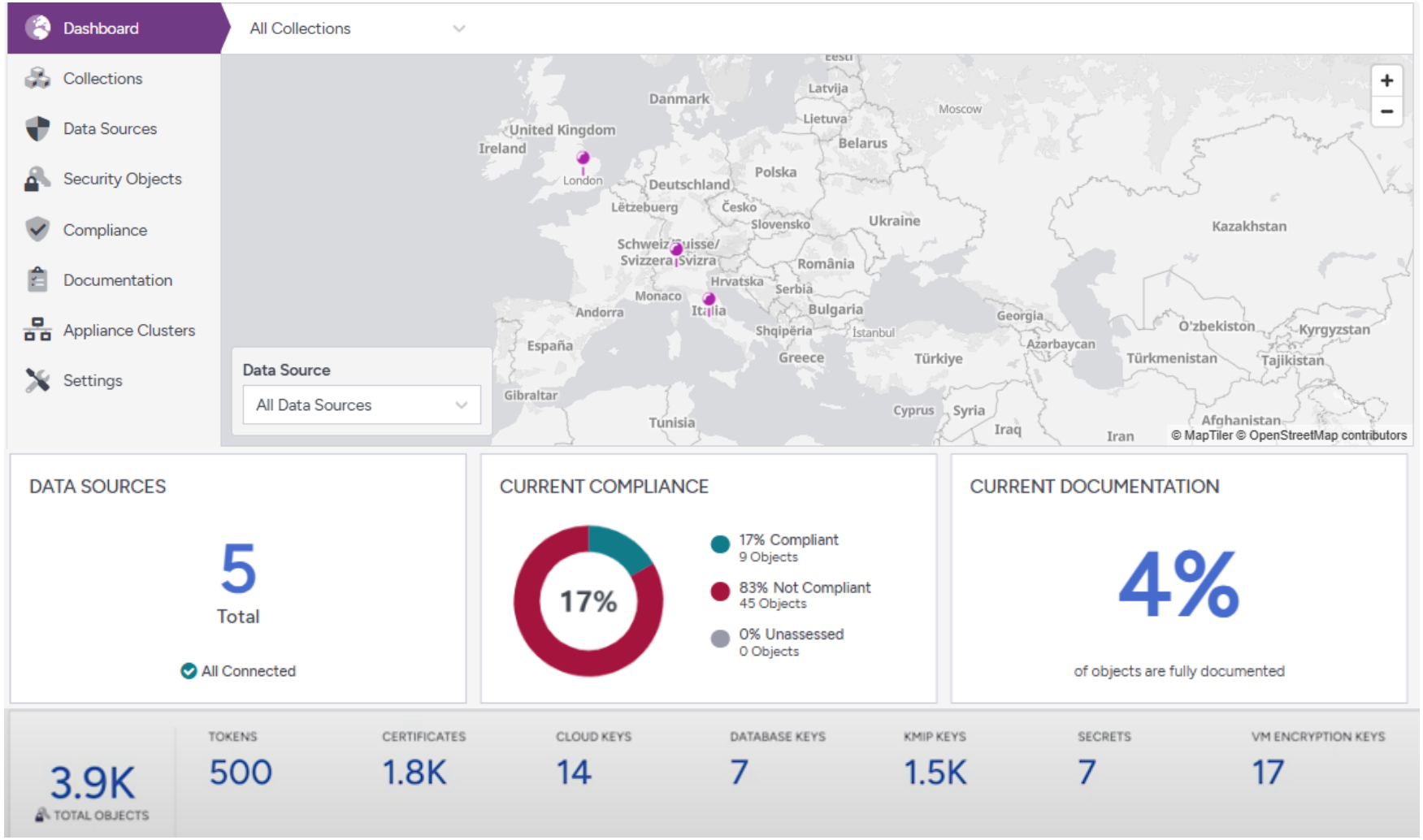
Extensible Operations

Capability to incorporate additional security operations tailored to customer requirements.



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.

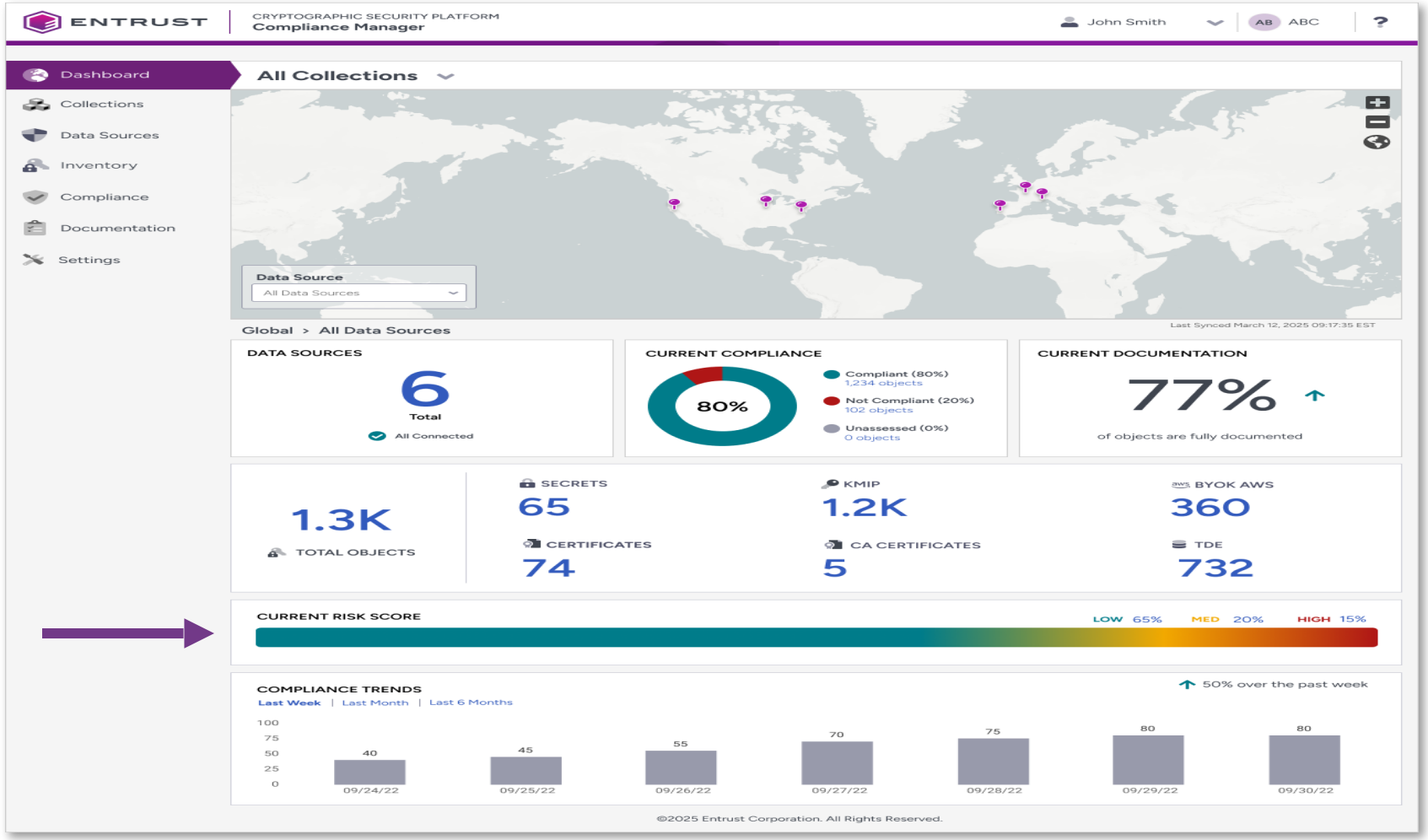


Risk Scoring

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.



ENTRUST

Köszönöm

entrust.com

ENTRUST

SECURING A WORLD IN MOTION