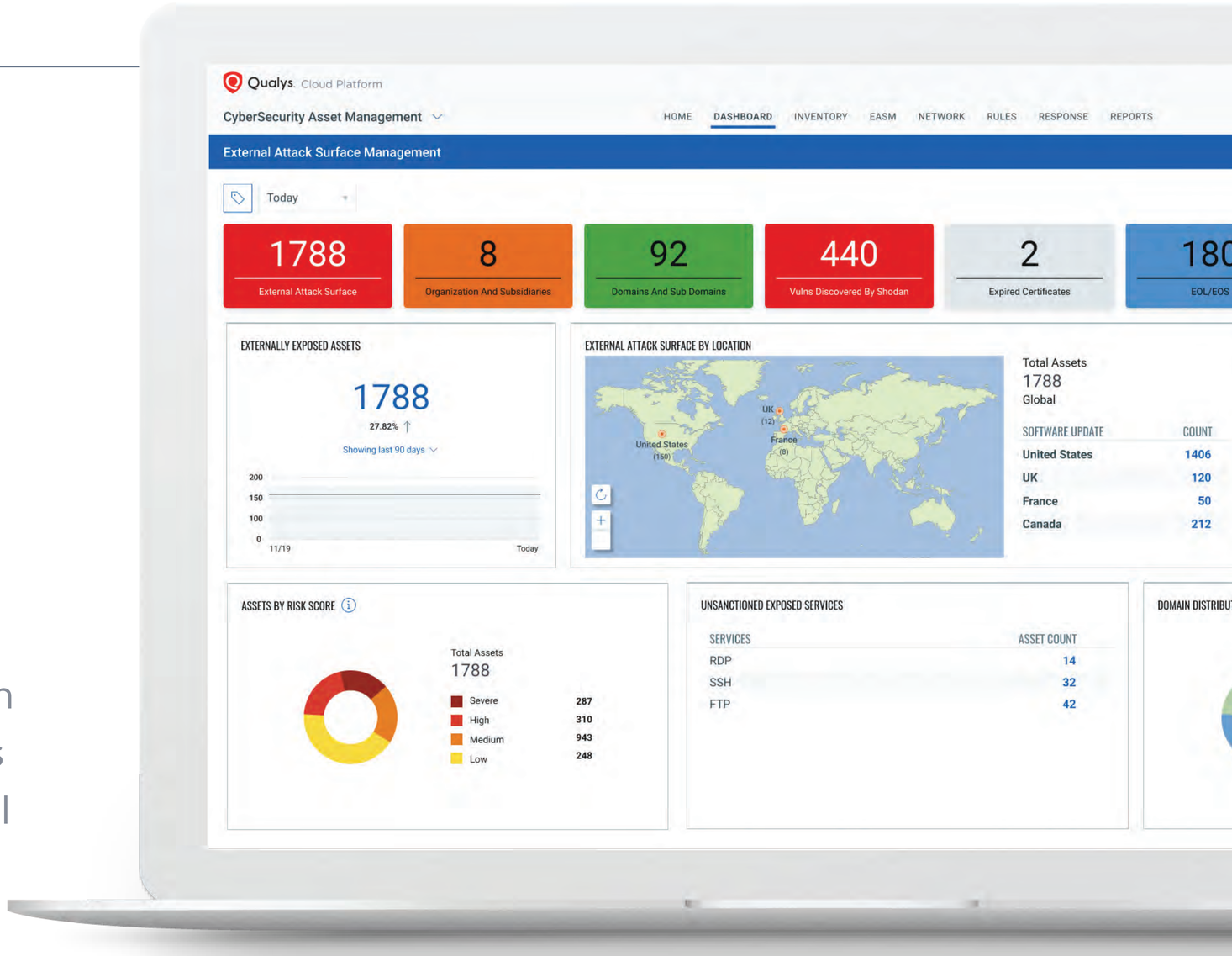
# CyberSecurity Asset Management (CSAM) 2.0

## with External Attack Surface Management




# See your attack surface like an attacker would.

The attack surface is expanding at an exponential rate, providing attackers with new targets. More than 30% of all on-premises and cloud assets and services are not inventoried. It's a huge visibility gap for cybersecurity.

CyberSecurity Asset Management (CSAM) is a cloud service that allows organizations to continuously discover, classify, remediate, and measurably improve their cybersecurity posture for internal and external IT assets before the attackers can — and with the same actionable intelligence that the attackers use. It discovers all known and previously unknown internet-facing assets for 100% visibility and improved cyber risk management.

Qualys CSAM 2.0 includes External Attack Surface Management which adds "defense-in-depth" to update an organization's cybersecurity posture. It provides the ability to continuously discover and classify previously unknown assets with a Red Team-style asset and vulnerability management solution for full 360-degree coverage.

# Key Features

## Asset Management Built for Security, Integrated with IT

### 360-degree inventory of your full IT ecosystem

Get an attacker's view of your ecosystem with continuous discovery of all assets on-premises, OT, IoT, and in the cloud. CyberSecurity Asset Management uses advanced credentialed and non-credential scanning technologies to continuously and quickly discover and classify vulnerabilities for remediation. It automatically finds known and previously unknown assets ranging from instances and containers to repositories and devices as well as domains and subdomains, connected subsidiaries and business partners for full visibility of potential risk vectors.

### Detect and monitor security gaps

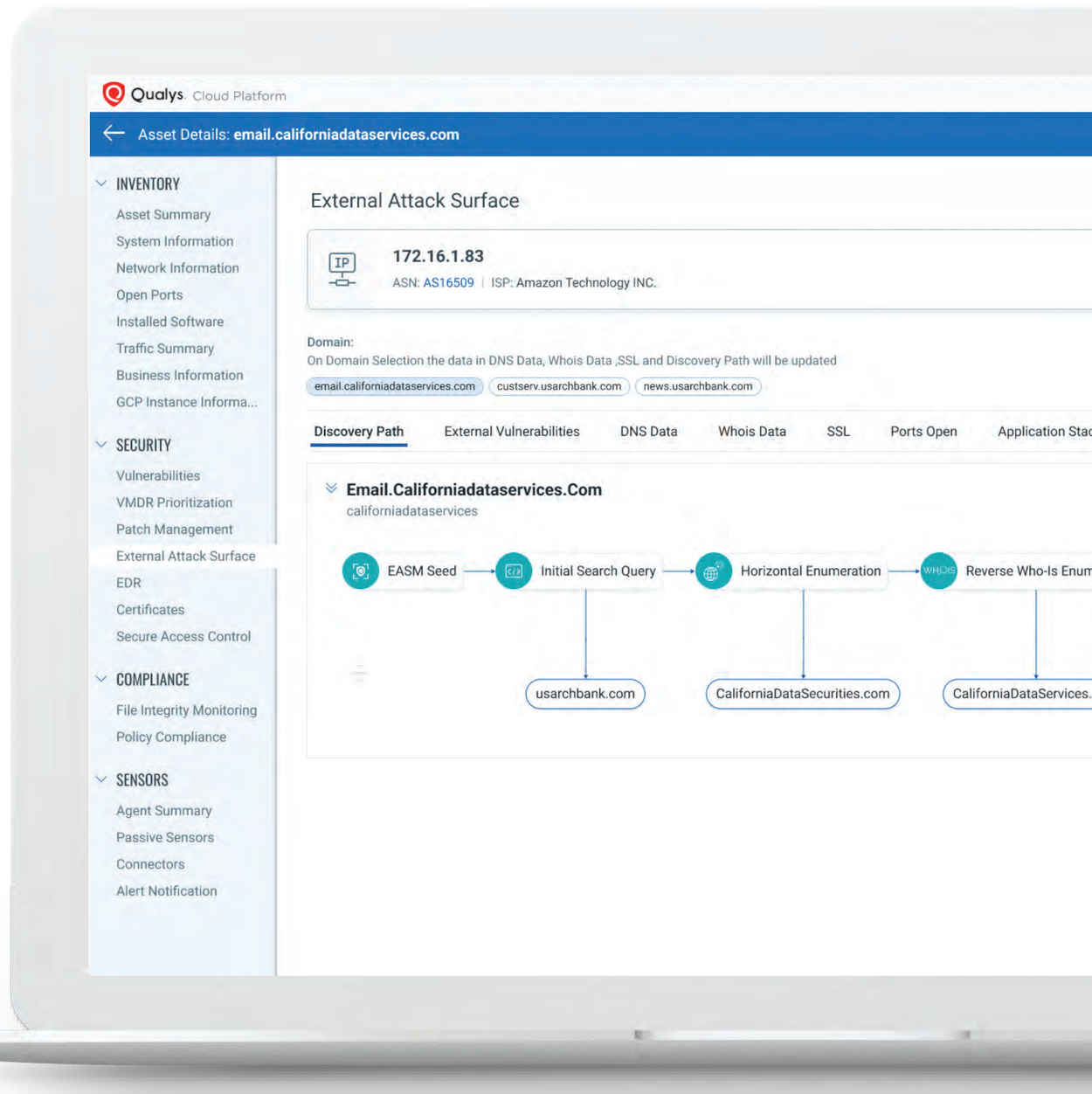
CyberSecurity Asset Management enables easy identification of at-risk assets. It automatically assigns the asset criticality score to a tag and the corresponding asset with organizational in-context enrichment data. This context enables analysis of threats and misconfigurations in real time, with six-sigma accuracy. The service continuously detects remotely exploitable vulnerabilities and critical misconfigurations across your global hybrid environment such as end-of-life/end-of-support and unauthorized or missing titles. CyberSecurity Asset Management also discovers missing required software, and provides real-time alerts on zero-day vulnerabilities, compromised assets, and network irregularities.

### Orchestrate with VMDR 2.0

Automatically deploy the most relevant, correct, and superseding patch to quickly remediate vulnerabilities and threats across any size environment. CyberSecurity Asset Management automatically quarantines suspicious devices until they can be investigated. As part of the Qualys Cloud Platform, the service continuously delivers integrated endpoint detection & response, vulnerability & patch management, and policy compliance.

### Integrate with ServiceNow

CyberSecurity Asset Management provides enriched ServiceNow CMDB bi-directional integration for a continuously updated view on assets. Certified by the Service Graph Connector Program, it enriches Qualys assets with key CMDB business context data such as asset criticality and data owner.



# Benefits

## Get an attacker's view of your full IT ecosystem

- Gain actionable intelligence, visibility, and insight into the entire internal and external attack surface
- Discovers domains, subdomains, and certificates within the enterprise and in subsidiaries and business partners for full visibility of remotely exploitable vulnerabilities — including previously unknown devices via attribution
- Expose "shadow IT" and baseline discrepancies including VMs, containers, functions-as-a-service, and IoT that spin up faster than IT can track with legacy tools
- Get an outside-in view of your internet-facing assets to spot security endpoint blind spots
- Reduce tech debt with CISA-compliant end-of-life and end-of-support software tacking, and Ling software versioning to track OS status and related vulnerabilities

## Find security gaps with quantitative risk management

- Tag assets for easy grouping
- Enable risk management
- Execute like an attacker
- Enable business impact analysis (BIA)

## Receive full context on all assets with ServiceNow integration

- Continuously Sync with ServiceNow
- Add context for security-centric asset visibility
- Add security and business context to asset inventory

## Assign risk profile to assets by business and technical context

- The user optionally selects a criticality score on a tag which is then applied to one or more assets
- An asset attribute is assigned the highest criticality score among allocated asset tags
- If pulling data from CMDB, the asset criticality score is automatically assigned to a tag and the corresponding asset

## Quickly identify blind spots

- Proactively track authorized and unauthorized software
- Automatically manage multiple software lists based on asset type, location, criticality, and usage
- Track detailed asset information for flagging configuration issues, security risks, IT policy violations, and non-compliance

## Orchestrate automatic alert, report, and response with VMDR

- Alert, report & respond to identified security risks
- Auto-document compliance for PCI DSS, FedRAMP, NIST, ISO, and other policies
- Leverage the integrated Qualys Cloud Platform, to extend beyond traditional External Attack Surface Management

# **Powered by the Qualys Cloud Platform —** the revolutionary architecture that powers Qualys IT security and compliance cloud services

## Single-pane-of-glass UI

See the results in one place, in seconds. With AssetView, security and compliance pros and managers get a complete and continuously updated view of all IT assets — from a single dashboard interface. It's fully customizable and lets you see the big picture, drill down into details, and generate reports for teammates and auditors. Intuitive and easy-to-build dynamic dashboards aggregate and correlate all your IT security and compliance data in one place from all the various Qualys Cloud Apps. With its powerful elastic search clusters, you can now search for any asset – on-premises, endpoints and all clouds – with 2-second visibility.

## Centralized & customized

Centralize discovery of host assets for multiple types of assessments. Organize host asset groups to match the structure of your business. Keep security data private with our end-to-end encryption and strong access controls. You can centrally manage users' access to their Qualys accounts through your enterprise's single sign-on (SSO). Qualys supports SAML 2.0-based identity service providers.

## Easy deployment

Deploy from a public or private cloud — fully managed by Qualys. With Qualys, there are no servers to provision, software to install, or databases to maintain. You always have the latest Qualys features available through your browser, without setting up special client software or VPN connections.

## Scalable and extensible

Scale up globally, on demand. Integrate with other systems via extensible XML-based APIs. You can use Qualys with a broad range of security and compliance systems, such as GRC, ticketing systems, SIEM, ERM, and IDS.

---

# **See for yourself.** Try Qualys CSAM 2.0 with External Attack Surface Management.

**Try it free →**

Start your free trial today.
No software to download or install.
Email us or call us at 1 (800) 745-4355.

v2200801