Know Your Assets: Sichtbarkeit herstellen, Sicherheitsniveau bewerten
The 5 New Tenets of Security for enabling the Digital Transformation

Visibility
Accuracy
Scale
Immediacy
Transparent-Orchestration

Building-in - N  T bolting-on
Qualys Cloud Platform
Architecture

Integrated Suite of Applications: CA, AI, VM, CM, TP, FIM, PC, PCI, SAQ, IOC, WAS, WAF

Analytics and Reporting Engines: kafka, ceph, elastic, cassandra, redis, Flink, Microservices

Distributed Sensors: Hardware, Virtual, Cloud, Agent, Passive, API
Qualys Cloud Platform Backend
Scalable, Micro-services, DevOps

Qualys Streaming Data Backbone

Scanner Service

APIs

Cloud Agent Service

VM
PC
WAS
WAF
FIM

Reporting
Analytics
IOC
Indexing Service
Asset Tagging Service
Qualys Cloud Platform

Unified approach to detection, prevention & response across on-premise, cloud and endpoints
## Qualys Sensors

**Scalable, self-updating & centrally managed**

### Physical
- Legacy data centers
- Corporate infrastructure
- Continuous security and compliance scanning

### Virtual
- Private cloud infrastructure
- Virtualized Infrastructure
- Continuous security and compliance scanning

### Cloud/Container
- Commercial IaaS & PaaS clouds
- Pre-certified in marketplace
- Fully automated with API orchestration
- Continuous security and compliance scanning

### Cloud Agents
- Light weight, multi-platform
- On premise, elastic cloud & endpoints
- Real-time data collection
- Continuous evaluation on platform for security and compliance

### Passive
- Passively sniff on network
- Real-time device discovery & identification
- Identification of APT network traffic
- Extract malware files from network for analysis

### API
- Integration with Threat Intel feeds
- CMDB Integration
- Log connectors

**Agentless + Agent Based + Passive**
# Integrated Cloud Apps

## Asset Management
- **Asset Inventory**
  - Maintain full, instant visibility of all your global IT assets

## IT Security
- **Vulnerability Management**
  - Continuously detect and protect against attacks, anytime, anywhere

## Compliance Monitoring
- **Policy Compliance**
  - Assess security configurations of IT systems throughout network

## Web Application Security
- **Web Application Scanning**
  - Secure web applications with end-to-end protection

---

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASSET MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td>AI</td>
<td>Asset Inventory</td>
</tr>
<tr>
<td>SYN</td>
<td>CMDB Sync</td>
</tr>
<tr>
<td>CI</td>
<td>Cloud Inventory</td>
</tr>
<tr>
<td>CRI</td>
<td>Certificate Inventory</td>
</tr>
<tr>
<td>IT SECURITY</td>
<td></td>
</tr>
<tr>
<td>VM</td>
<td>Vulnerability Management</td>
</tr>
<tr>
<td>CM</td>
<td>Continuous Monitoring</td>
</tr>
<tr>
<td>TP</td>
<td>Threat Protection</td>
</tr>
<tr>
<td>IOC</td>
<td>Indication of Compromise</td>
</tr>
<tr>
<td>TP</td>
<td>Threat Protection</td>
</tr>
<tr>
<td>CM</td>
<td>Continuous Monitoring</td>
</tr>
<tr>
<td>CS</td>
<td>Container Security</td>
</tr>
<tr>
<td>PM</td>
<td>Patch Management (Beta in Sept)</td>
</tr>
<tr>
<td>PC</td>
<td>Policy Compliance</td>
</tr>
<tr>
<td>SCA</td>
<td>Security Configuration Assessment</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>WAS</td>
<td>Web Application Scanning</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>PCI</td>
<td>PCI Compliance</td>
</tr>
<tr>
<td>SAG</td>
<td>Security Assessment Questionnaire</td>
</tr>
<tr>
<td>FIM</td>
<td>File Integrity Monitoring</td>
</tr>
<tr>
<td>CSA</td>
<td>Cloud Security Assessment</td>
</tr>
<tr>
<td>AI</td>
<td>Certificate Inventory</td>
</tr>
<tr>
<td>CMDB Sync</td>
<td>Synchronize asset information from Qualys into ServiceNow CMDB</td>
</tr>
<tr>
<td>Cloud Inventory</td>
<td>Inventory of all your cloud assets across AWS, Azure, GCP and others</td>
</tr>
<tr>
<td>Certificate Inventory</td>
<td>Inventory of TLS/SSL digital certificates on a global scale</td>
</tr>
<tr>
<td>Threat Protection</td>
<td>Pinpoint your most critical threats and prioritize patching</td>
</tr>
<tr>
<td>Indication of Compromise</td>
<td>Continuously monitor endpoints to detect suspicious activity</td>
</tr>
<tr>
<td>Container Security</td>
<td>Discover, track, and continuously protect containers</td>
</tr>
<tr>
<td>Patch Management</td>
<td>Select, manage, and deploy patches to remediate vulnerabilities</td>
</tr>
<tr>
<td>Policy Compliance</td>
<td>Automate, simplify and attain PCI compliance quickly</td>
</tr>
<tr>
<td>Security Configuration Assessment</td>
<td>Automate configuration assessment of global IT assets</td>
</tr>
<tr>
<td>Security Assessment Questionnaire</td>
<td>Minimize the risk of doing business with vendors and other third parties</td>
</tr>
<tr>
<td>File Integrity Monitoring</td>
<td>Log and track file changes across global IT systems</td>
</tr>
<tr>
<td>Cloud Security Assessment</td>
<td>Get full visibility and control across all public cloud instances</td>
</tr>
<tr>
<td>Certificate Assessment</td>
<td>Assess all your digital certificates for TLS/SSL vulnerabilities</td>
</tr>
</tbody>
</table>

---

---

Qualys Inc.
Introducing

Qualys Asset Inventory

Source of truth for IT and Security teams managing assets in hybrid environments.

Complete, continuous, structured and enriched asset inventory, that enables better business decisions.
# Use Cases

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visibility</td>
<td>You can’t manage nor protect what you don’t know</td>
</tr>
<tr>
<td>Compliance</td>
<td>Internal and external audits (what</td>
</tr>
<tr>
<td>Security</td>
<td>Identify and track unauthorized software. Ensure software is up-to-date.</td>
</tr>
<tr>
<td>Software Asset</td>
<td>Owned vs. Deployed vs. Used</td>
</tr>
<tr>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>Enterprise</td>
<td>End-of-life application or component</td>
</tr>
<tr>
<td>Architecture</td>
<td></td>
</tr>
</tbody>
</table>
Qualys Asset Inventory

Discovers all assets in global, hybrid infrastructure.

Asset information is normalized and categorized for hardware and software.

Enriched with metadata and indexed for 2-second visibility.

Two-way CMDB synchronization (clean and categorized asset data)
Passive Network Sensor
in Beta
Discovery & Profiling

Eliminate blind spots. Identify and profile devices as soon as they connect to the network.

Continuously enrich existing inventory with additional details in real time.

Extends discovery, for sensitive systems that may not be suited for active probing or agent.
1. Deploy a Passive Sensor (physical or virtual)

1. Mirror traffic

1. Continuously discover and profile every device with network activity
DEMO

Qualys sensors for complete, detailed asset telemetry

Structuring your Hardware and Software (normalization and taxonomy)

Enriching your inventory (e.g. lifecycle)

Blind spots? (showcase passive discovery)
Qualys Cloud Inventory and Security Assessments

Unparalleled Visibility and Continuous Security Monitoring across public cloud infrastructure
Qualys Cloud Inventory and Security Assessment
Key Capability

Visibility into your public clouds
Get topographic view of your cloud inventory (AWS, Azure, GCP)

Continuous security monitoring
Monitor against security standards. Identify threats from misconfigurations (AWS, Azure)

Actionable Insight & threat prioritization
Prioritize by understanding association with exposures linked to vulnerable instances, network placement.
What is my public cloud usage?
What is my security posture?
Do I have any publicly accessible security accounts?
Are my security groups opening unauthorized access to internet?
Qualys Container Security

Container Images

- Build
  - Software Composition
  - Vulnerability Analysis
  - OSS License Analysis
  - Integration with CI Pipelines
  - Bug Tracking Integration

Container Registry

- Ship
  - Registry Scanning
  - Compliance Controls
  - Vulnerability, Package and License-based Rules
  - Real-time Vulnerability Impact Notifications

Container Instances Infrastructure

- Run
  - Host Protection
  - Container Engine Benchmarking
  - Container Orchestration Benchmarking
  - Deep Runtime Visibility
  - Runtime Protection
Containers

Real game changer
Hypervisor disappearing, bare metal is back
Kubernetes Infrastructure-as-code
Container-as-a-Service AWS Fargate
AWS Lambda function-as-a-service, serverless!
Kubefed?
“Priceline” for Containers?
Qualys Container Security

- Host Protection
- CIS Benchmarks
- Protection for container infrastructure stack
- Scanning & Compliance
- Accurate insight and control of container images
- Visibility & Protection
- Automated analysis and enforcement of container behavior
Qualys Mobile Security Platform

1Mobility Acquisition

Cloud Agents on iOS, Android & Windows Mobile
EMM (Enterprise Mobility Management)
Realtime Asset Inventory
AV, VM, PC & Threat detection
Policy enforcement
Beta Q4 2018
Cloud Agent Platform

Lightweight agent (3 MB) for on premise servers, dynamic cloud environments and mobile endpoints

Secure scalable architecture for millions of devices Centrally managed, self updating

Architecture for IoT device security and compliance with SDK

7.3 Million Cloud Agents purchased over last 12 months (Mar 2017 – Mar 2018)
Single Pane of Glass

Dynamic and customizable dashboards
Centrally managed, self-updating, integrated Cloud Apps

1+ trillion
Security Events

3+ billion
IP Scans/Audits a Year

250+ billion
Data Points Indexed on Elasticsearch Clusters

99.9996%
Six Sigma Scanning Accuracy
End-to-end Security Architecture
Automated Continuous Monitoring & Response

Discovery
- On-Prem
- Cloud
- Mobile Devices
- OT/ICS
- IoT
- CMDB
- Inventory

Prevention
- Security Hygiene
- Vulnerability Assessment
- Threat Prioritization
- Patch Management
- Configuration Assessment

Detection
- Endpoint Activity
- Cloud Infra Monitoring
- Network Activity

Response
- Security Orchestration
- Incident Response
- Quarantine
- NAC
Qualys Private Cloud Platform
Data Sovereignty/MOD

Deployed within customer or partner datacenters to maintain data sovereignty

Same codebase as shared platform

Hardware, virtualized or AWS versions

Fully or Partially managed by Qualys

FedRAMP Certified

Qualys Gov Cloud
Qualys Cloud Platform Operations

Global Infrastructure
3+ Billion Scans Annually*

6 Public Clouds online in US, EU and IN

Private Clouds as a Platform Appliance or a Virtual Data Center (65 plus)

Raleigh, NC
Redwood Shores, CA
France, EU
Pune, India

Private Clouds
Public Clouds

Operation, Administration and Maintenance
Signature Updates
Software Updates

Qualys Cloud Platform Operations
### Cloud Platform Capacity

<table>
<thead>
<tr>
<th>Region</th>
<th>POD</th>
<th>Status</th>
<th>Cores</th>
<th>Memory</th>
<th>Storage</th>
<th>Capacity (IPs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>POD1</td>
<td>Live</td>
<td>2500</td>
<td>68 TB</td>
<td>3274 TB</td>
<td>10 mil</td>
</tr>
<tr>
<td>US</td>
<td>POD2</td>
<td>Live</td>
<td>1144</td>
<td>25 TB</td>
<td>675 TB</td>
<td>5 mil</td>
</tr>
<tr>
<td>US</td>
<td>POD3</td>
<td>Live</td>
<td>556</td>
<td>9 TB</td>
<td>277 TB</td>
<td>3 mil</td>
</tr>
<tr>
<td>EU</td>
<td>POD1</td>
<td>Live</td>
<td>632</td>
<td>19 TB</td>
<td>1941 TB</td>
<td>3 mil</td>
</tr>
<tr>
<td>EU</td>
<td>POD2</td>
<td>Live</td>
<td>432</td>
<td>9 TB</td>
<td>277 TB</td>
<td>3 mil</td>
</tr>
<tr>
<td>IN</td>
<td>POD1</td>
<td>Live</td>
<td>504</td>
<td>9 TB</td>
<td>277 TB</td>
<td>3 mil</td>
</tr>
</tbody>
</table>

**Vertical and Horizontal Scalability**

All new product deployments fully DevOps automated
World-Class, Global Customer Support

24x7x365 SUPPORT
Collaborative Approach Involvement of Support, Ops and Engineering

HIGHLY RESPONSIVE
80 TSE Globally working in multiple shifts

WELL ESTABLISHED QUALYS COMMUNITY
12,000+ Members Online Community for Best Practices, Third Party Support, Knowledge Base, and Training Videos

Redwood City, CA
Raleigh, NC
Pune, India
Japan

Free Product Training
Telephone Support
Online Support

Telephone Support
Online Support

Redwood City, CA
Raleigh, NC
Pune, India
Japan

Qualys Cloud Platform
A new unified approach to prevention and response

- 2-second visibility across all of your global IT assets (on premise, endpoints and cloud assets)
- Continuous assessment of your global security & compliance posture
- Identify compromise-able and compromised assets
- Consolidate all your security and compliance stacks
- Secure your digital transformation
- Drastically reduce your spend
Thank You
twendt@qualys.com