QUALYS SECURITY CONFERENCE 2018

Qualys CertView

Managing Digital Certificates

Asif Karel
Director, Product Management, Qualys, Inc.

Agenda

Introduction

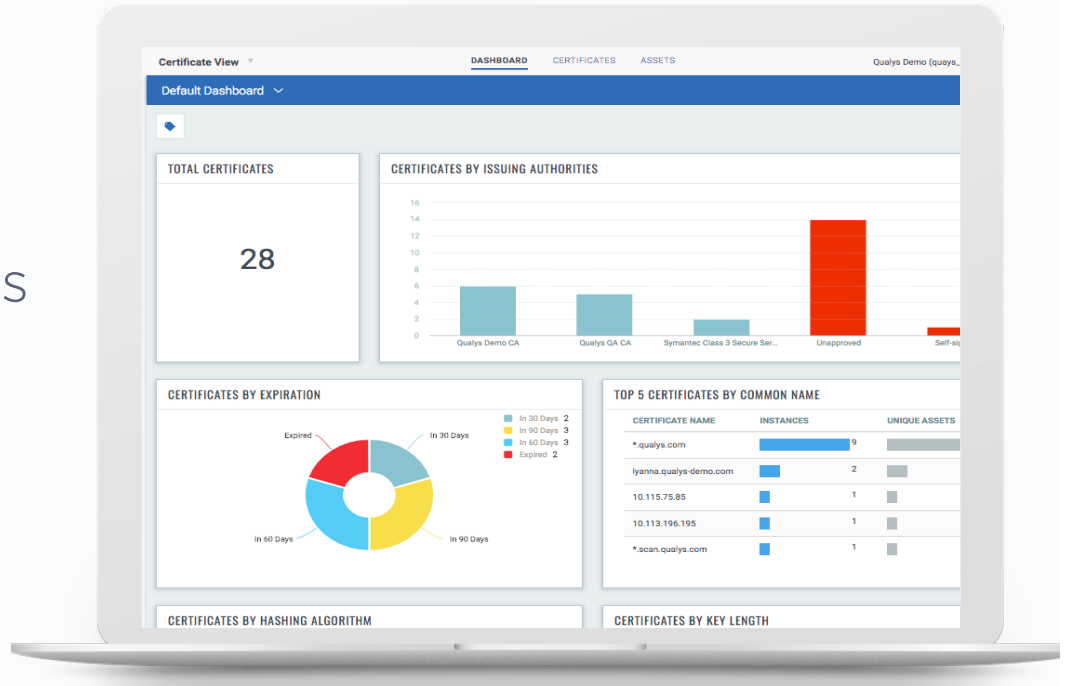
Evolving browser markers

Introducing CertView

Key Use Cases and Capabilities

Demo

Q&A



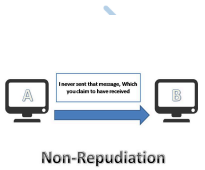
Qualys.

Refresher: What does SSL give you?

Confidentiality

Authentication

Message Integrity



Non-repudiation

Certificates are Everywhere

Evolving security indicators

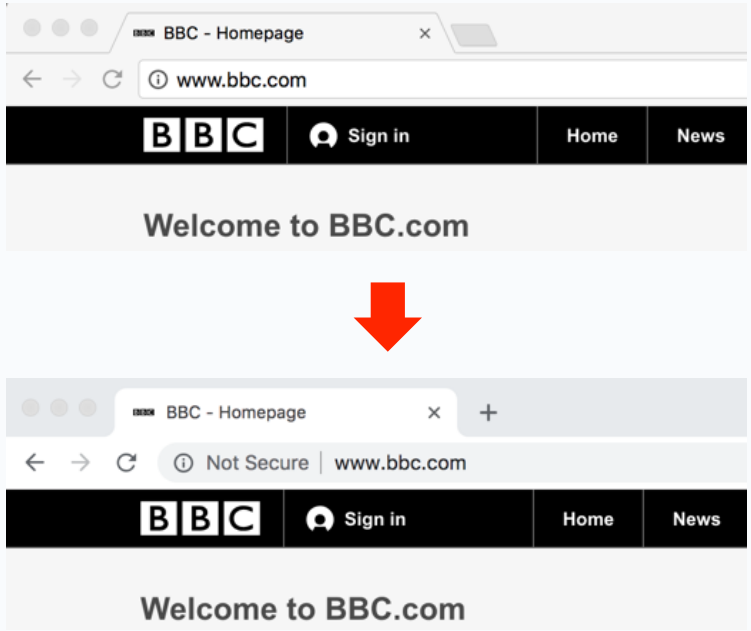
Users should expect that the web is safe by default, and they'll be warned when there's an issue[1].

\- Security Team
Google

[1]https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html

Timeline of Chrome's Evolution

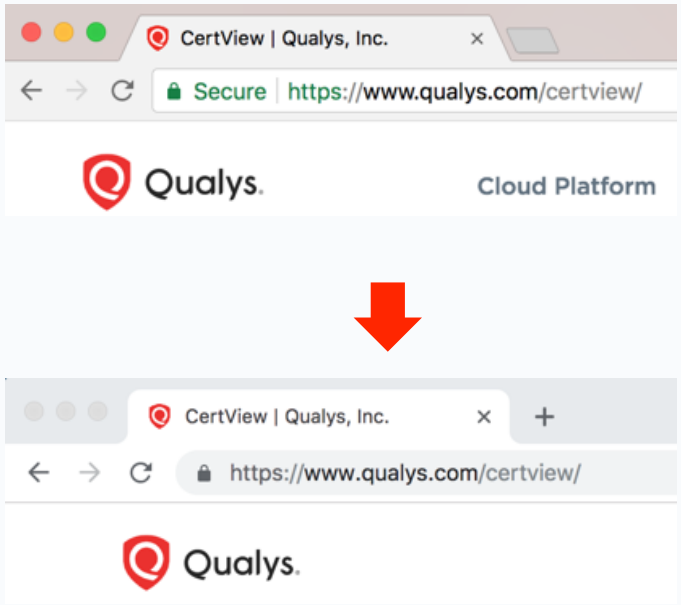
July 2018 (Chrome 68) – All HTTP sites marked
Not Secure



Qualys.

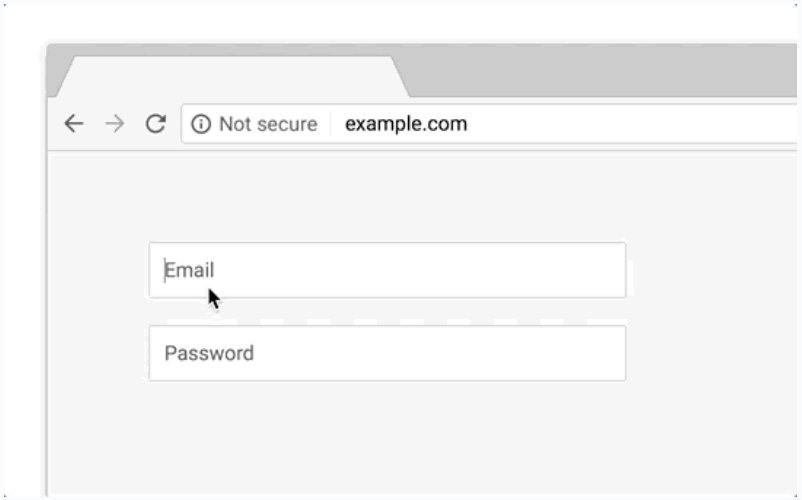
Timeline of Chrome's Evolution

Sept 2018 (Chrome 69) – Secure sites marked neutral instead of the green Secure



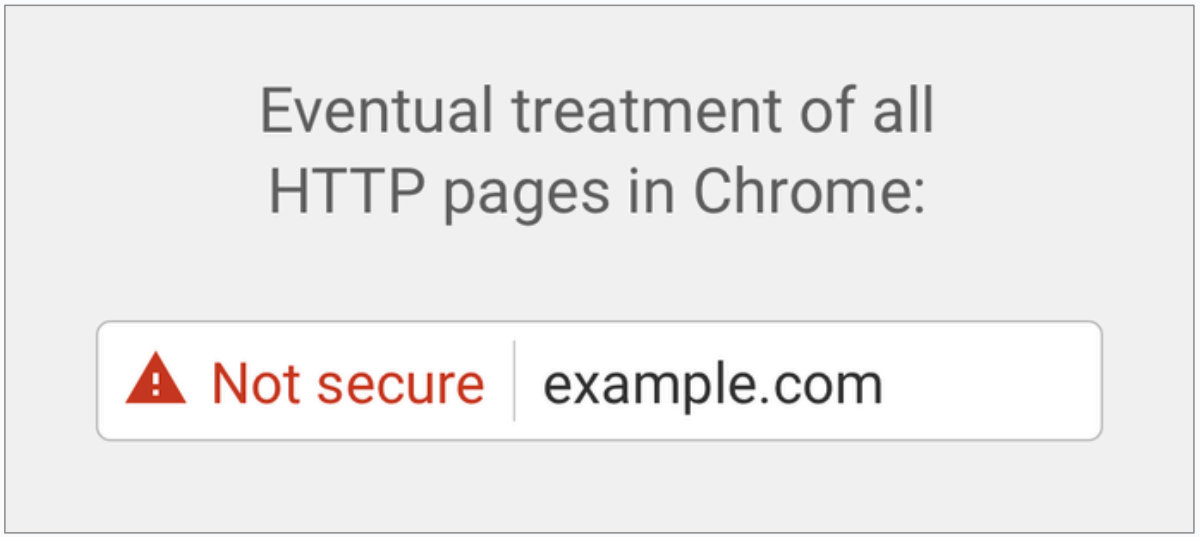
Timeline of Chrome's Evolution

Oct 2018 (Chrome 70) – RED "Not Secure" marker if user interacts with any input field



Qualys.

Timeline of Chrome's Evolution



https://www.chromium.org/Home/chromium-security/marking-http-as-non-secure

Schedule to disable TLS 1.0 / 1.1

- Chrome: Jan 2020
- Firefox/Safari: March 2020
- IE: First half of 2020

TLS 1.3 is faster and removes support for insecure features and ciphers

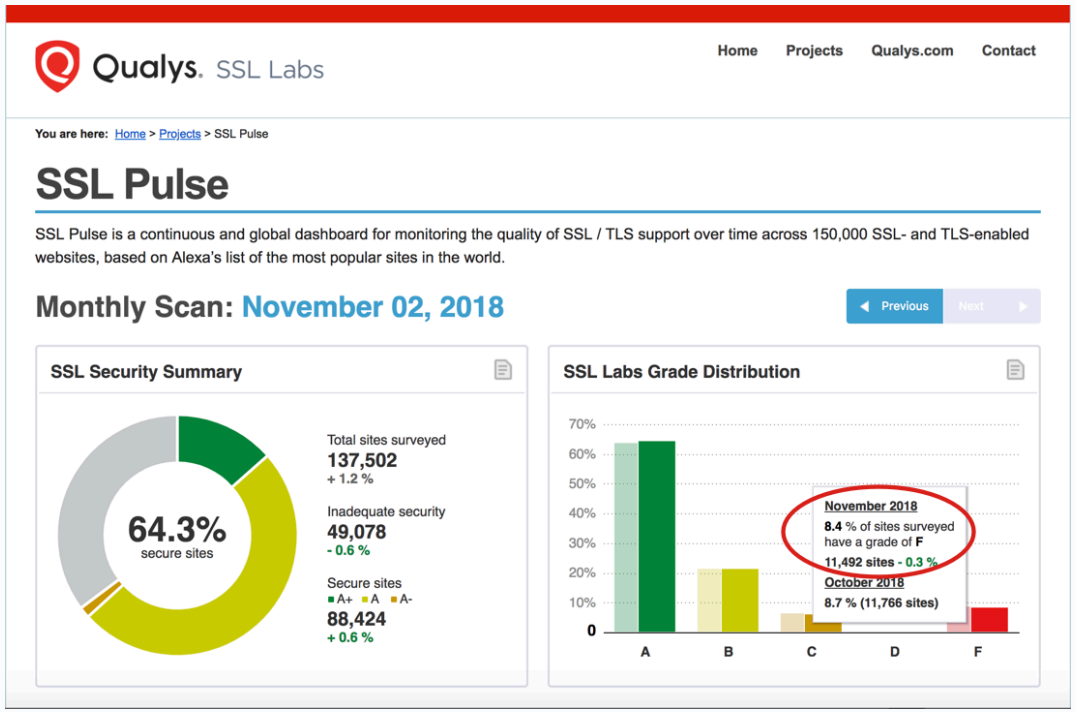
SSL Pulse

The Good

- No SHA1 or 1024 bit keys

The Bad (~35% inadequate)

- Expired certificates: ~5,200
- Expiring in the next 2 weeks: ~4,500
- Weak/Insecure cipher suites: ~4,200
- SSLv2/SSLv3: ~15,000
- TLSv1.0: ~99,000 (72%)
- RC4 enabled: ~22,000 (16%)



Qualys.

Security Solution w/o a Certificate Management System

High-end Security Solution w/o a Certificate Management System

Tinkering with Security Solutions w/o a Certificate Management System

Dangers of Incomplete Security Solutions

Hiding Malicious Actions	• Malware • Ransomware	• Virus • Trojan	• Botnet
Hiding the Initial Infection	Before the call back to a C&C		
Hiding Data Exfiltration	Bypass other controls such as DLP		

Security Solutions w/o a Certificate Management system

Qualys.

Current State of Most Organizations

Limited Visibility

95% of organizations don't know where certs are in their networks

Limited ownership information

The unknown is difficult to manage

Expirations Missed

Unplanned outages

Many more "near misses"

Compliance

Certificates from unapproved CAs

Responding to audits are manually intensive exercises

Reliance on Manual Processes

Spreadsheets are error prone and out-of-date

Expensive, not scalable as certificates increase

Troubleshooting issues is challenging

The average Global **5,000** company spends about **$15 million** to recover from the loss of business due to a certificate outage[1]

[1]http://www.csoonline.com/article/2987186/browser-security/expired-certificates-cost-businesses-15-million-per-outage.html

Challenges of Existing Solutions

Lack of..

Visibility

Point tools, increasing effort and ownership costs

Scalability

Operational silos

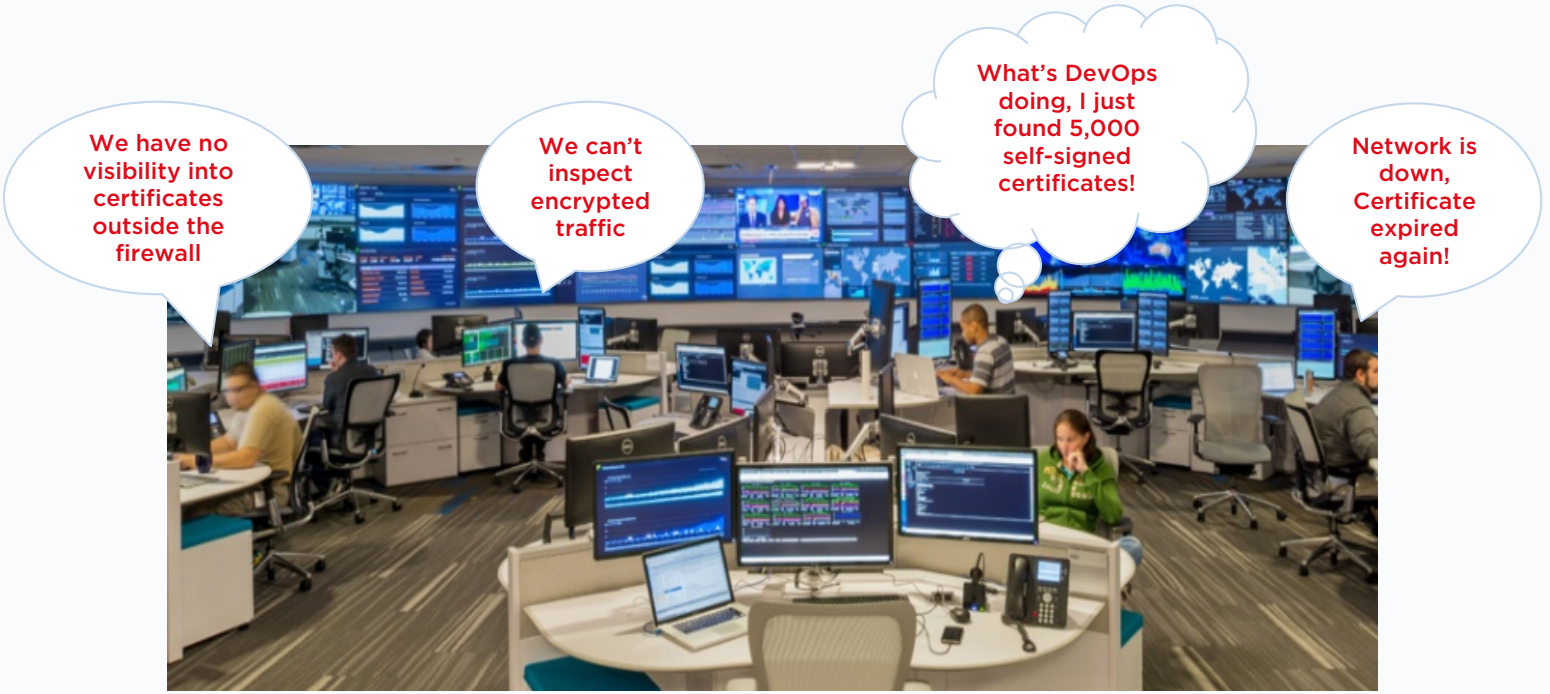
Work in on-premises or cloud-only mode

Require multiple or complex deployments to cover large environments

Maturity

Most solutions are off-the-shelf vulnerability-only or certificate-only “tools”

Single Pane of Glass



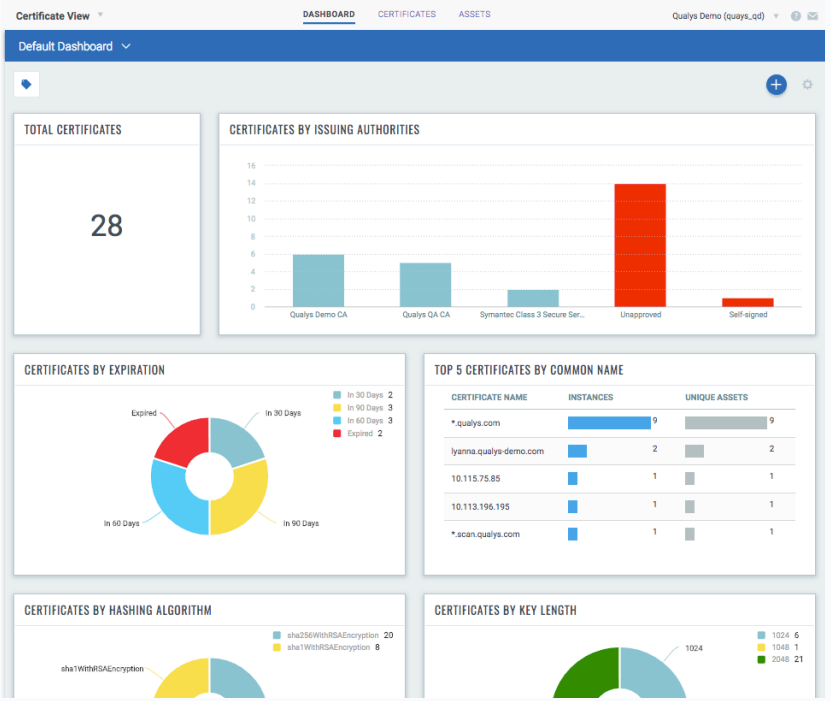
Introducing Qualys CertView

Discover, inventory, monitor certificates

Discover, inventory, monitor host configurations & vulnerabilities

Coverage across both on-premises and cloud environments

Renew certificates from the same platform

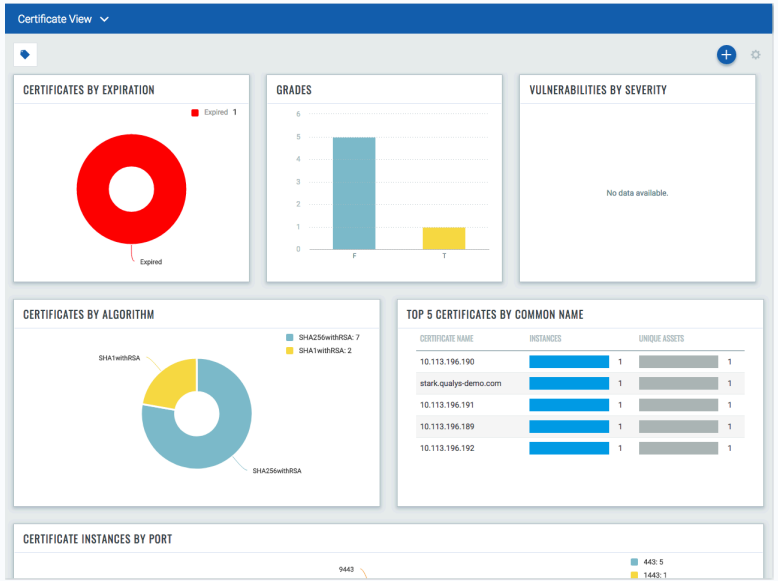


Qualys.

Use Cases

Outage Remediation	Stop expired certificates from interrupting business
Certificate Grades	Find out if your TLS configurations are following best practices
Baseline Normal Usage/ Full Visibility	Establish a baseline to be able to detect anomalies
Audits and Compliance	Achieve audit success and fast remediation
Certificate Renewal	Renew expiring certificates

Key Advantages of Qualys CertView



Uses the same Qualys scanners already deployed for Vulnerability Management or Policy Compliance

Qualys CertView meets much of the common use cases in version 1.0 – and we're working on closing gaps quickly

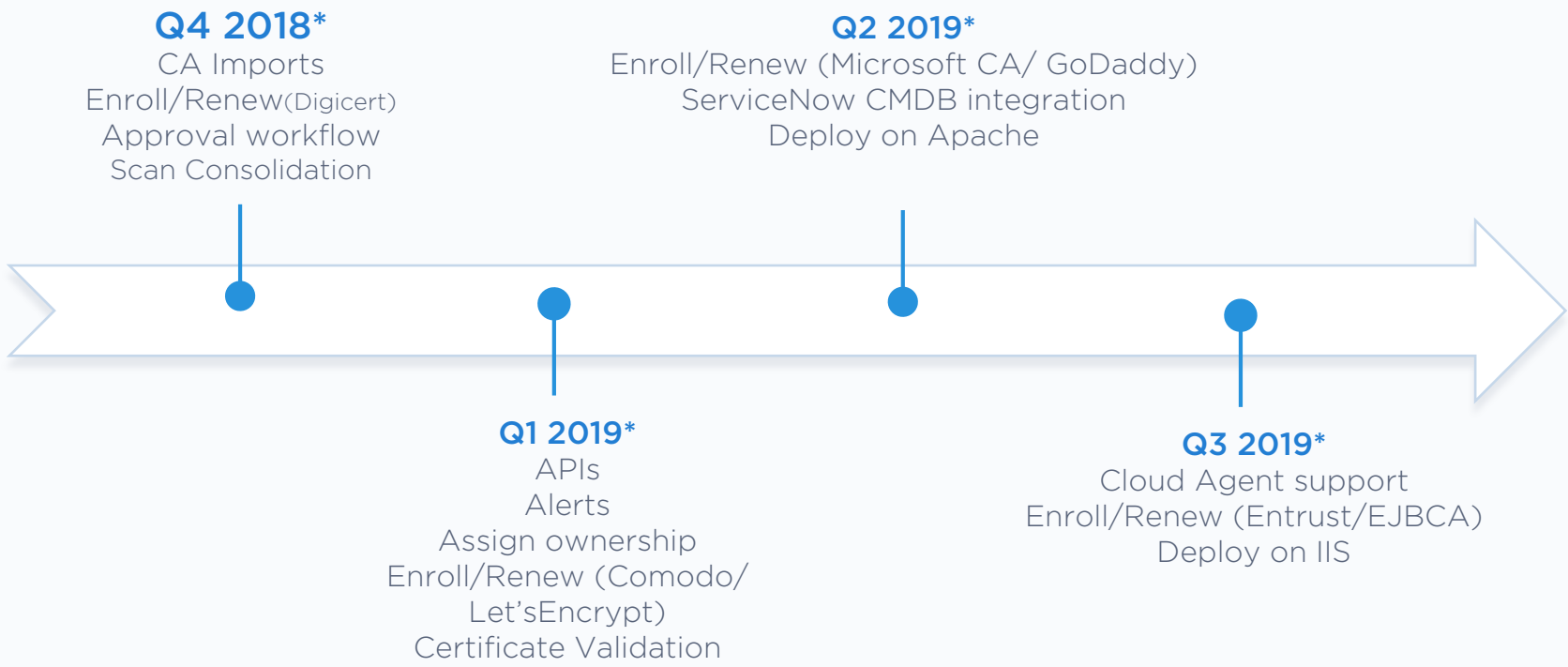
Certificate Enrollment/Renewal Releasing next month

Simplified delivery through Qualys Cloud Platform – easy for existing VM/PC customers to trial and deploy

Attractive Pricing

Qualys.

CertView Releases and Roadmap



* Roadmap items are future looking; timing and specifications may change

Qualys.

CertView is free, it's how you use it (or not) that will cost you!

-Anonymous


Certificates
Monitored
Archived
Search for Certificates
9
Total Certificates
ALGORITHM
SHA256withRSA 7
SHA1withRSA 2
UNIQUE KEY SIZE
2048 8
1024 1
CERTIFICATE AUTHORITY
Unapproved 5
Qualys QA CA 2
COMODO RSA Ex... 1
Self-Signed 1
Actions (0)
1 - 9 of 9
NAME/ORGANIZATION
ISSUER
EXPIRATION
ALGORITHM
KEY SIZE
LAST FOUND
INSTANCES
ASSETS
lyanna.qualys-demo...
Qualys, Inc.
Qualys Demo CA
Qualys, Inc.
Aug 22, 2017
7 months ago
SHA256withRSA 2048 Mar 27, 2018
stark.qualys-demo.c...
House Stark
Qualys QA CA
Qualys, Inc.
Jul 15, 2018
SHA256withRSA 2048 Mar 27, 2018
baratheon.qualys-de...
House Baratheon
Qualys QA CA
Jul 15, 2018
SHA1withRSA 1024 Mar 27, 2018
khal.qualys-demo.c...
Dothraki
COMODO RSA Extended
COMODO CA Limited
Oct 14, 2018
SHA256withRSA 2048 Mar 27, 2018
10.113.196.189
ssllabs
Qualys Security Tec...
May 02, 2027
SHA256withRSA 2048 Mar 6, 2018
10.113.196.191
ssllabs
Qualys Security Tec...
May 02, 2027
SHA256withRSA 2048 Mar 6, 2018
10.113.196.190
ssllabs
Qualys Security Tec...
May 02, 2027
SHA1withRSA 2048 Mar 6, 2018
10.113.196.192
ssllabs
Qualys Security Tec...
May 07, 2027
SHA256withRSA 2048 Mar 6, 2018
DEMO
CERT
Certificate View

Q&A

Qualys.

Thank You

Asif Karel
akarel@qualys.com