



QUALYS SECURITY CONFERENCE 2019

The Evolution of the Qualys Platform

Unveiling Latest Updates and Next-Gen Initiatives

Sumedh Thakar

President & Chief Product Officer, Qualys, Inc.

T T R

Time To Remediate



True Measure of Effectiveness of Security Program

Digital Transformation is accelerating

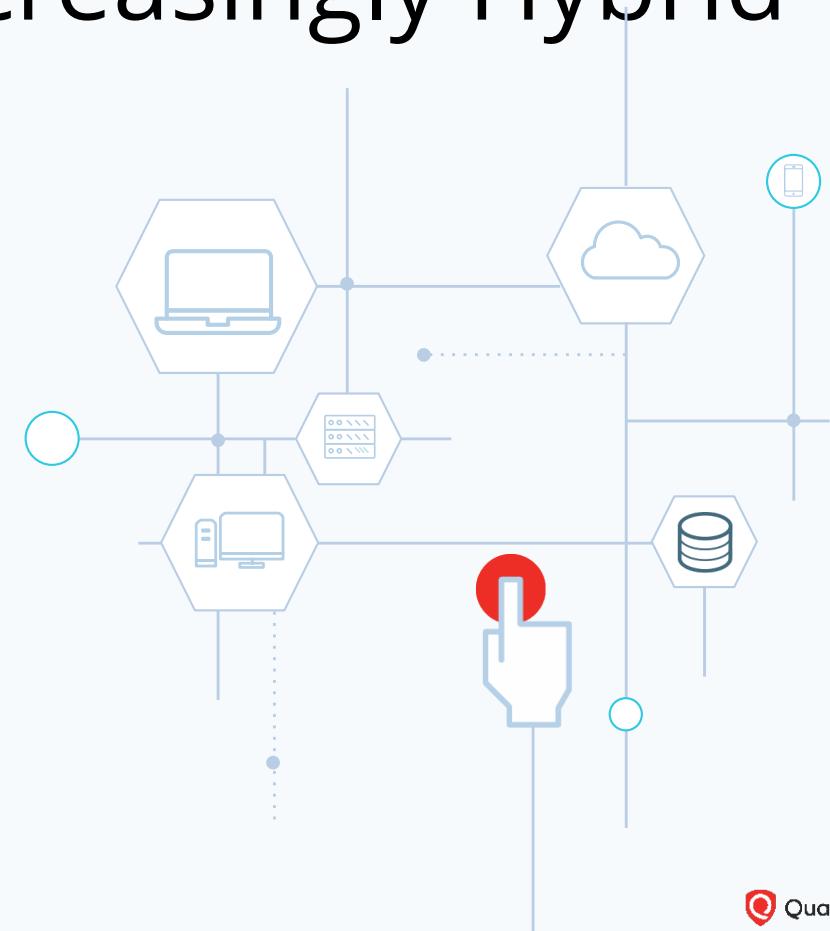


Rapid Adoption of New Processes and Technologies



Infrastructure is Increasingly Hybrid

Cloud, bare-metal,
Containers, Endpoints,
Mobility, OT, IoT, APIs,
etc.

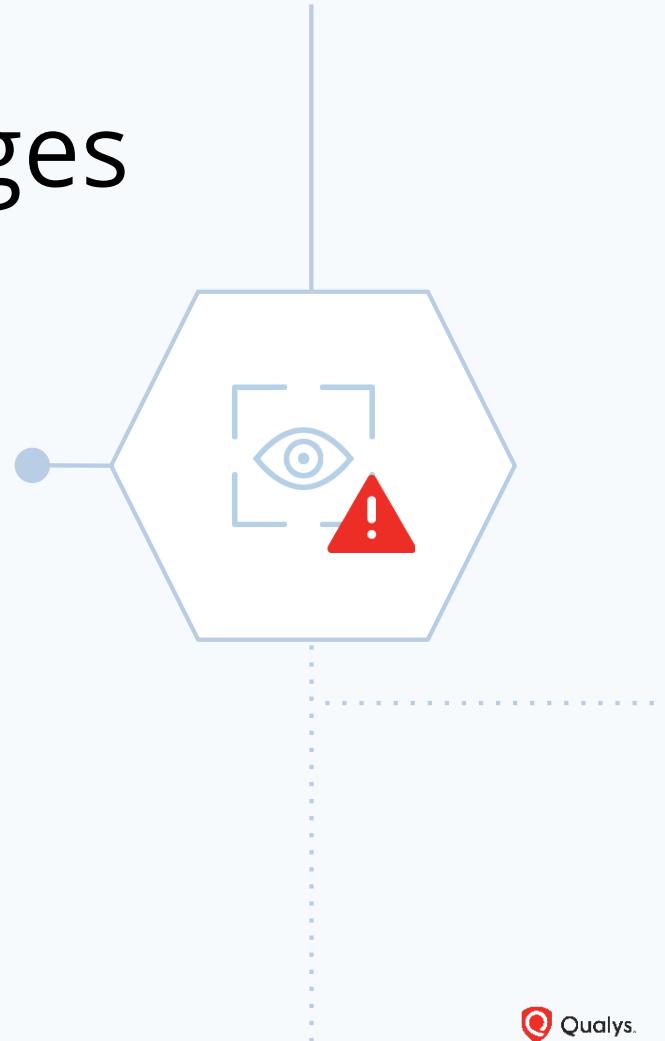


Security Challenges

Increasing surface area

Decreasing visibility

Increasing TTR



Silos!

People

Process

Tools

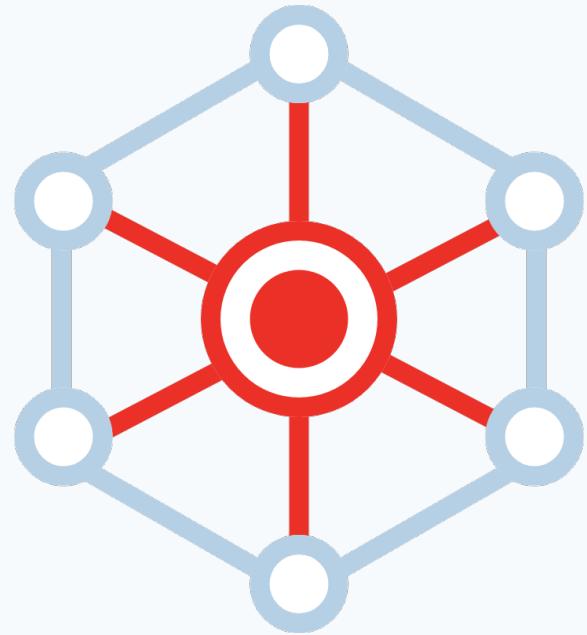
Reduce TTR

Real-time context with continuous data collection

Powerful analytics platform to correlate multiple datapoints and detect issues

Real-time response capabilities

Powerful decision engine to transparently orchestrate the response



Home Security Solutions

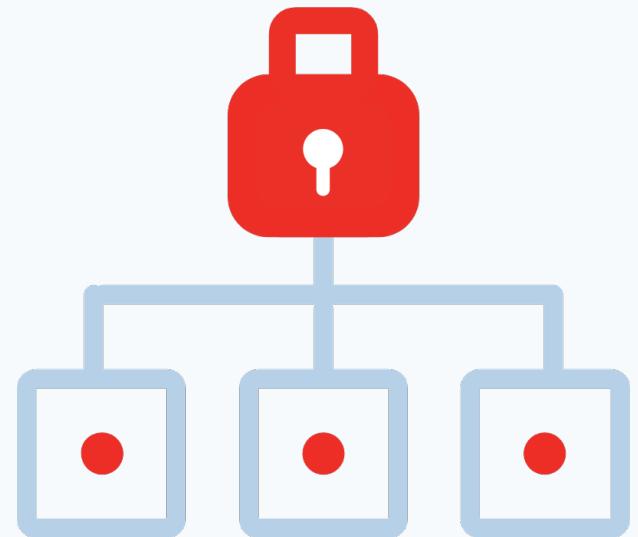
Nest Home Security Sensors

Nest Aware Subscription



Enterprise Security Tools Today

Point solutions
Multiple agents
Multiple consoles

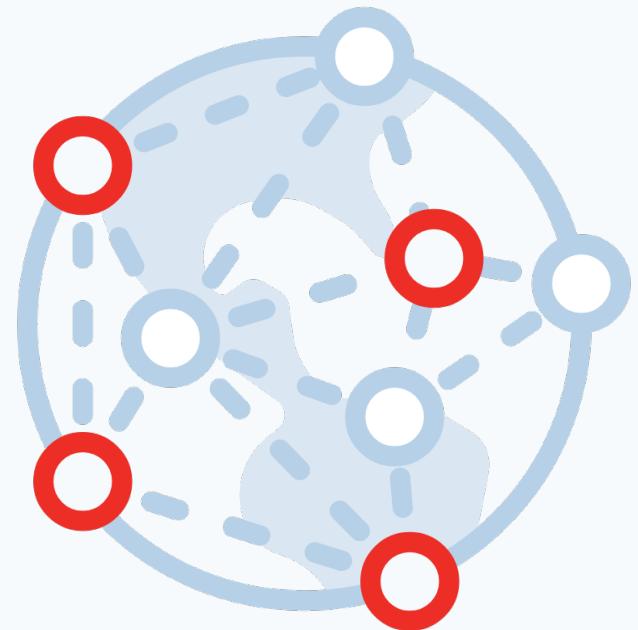


Integrations?

Integrate point solutions

But then too many point to point integrations

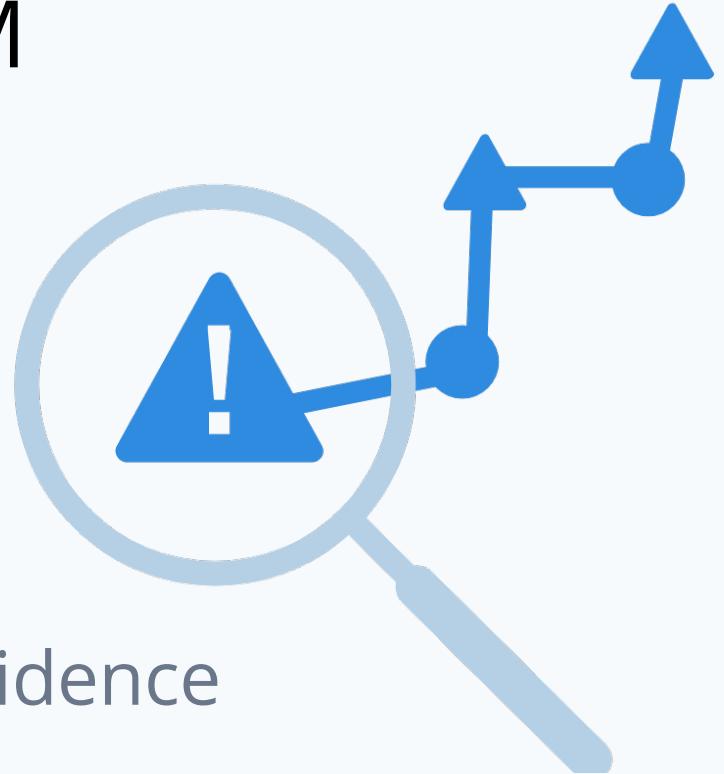
Doesn't provide full context



The Rise of the SIEM

Tie together point solutions
But still point solutions!
+ UEBA + ML/AI

Detection? Sort of with low confidence

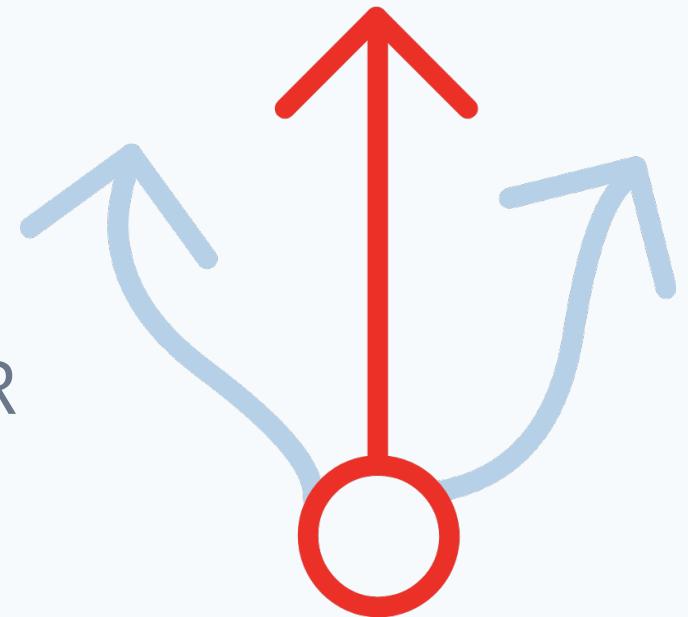


What About Response?

Additional point solutions to respond to

Well now we need new app - SOAR

Ties point solutions together – again!



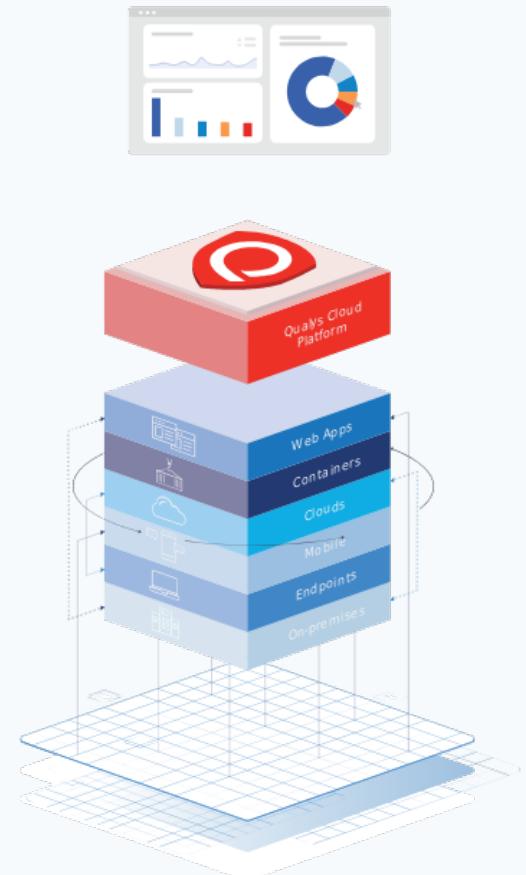
Evolution of the Qualys Cloud Platform



Remember those 19+ Apps?

Evolution of the Qualys Cloud Platform

Unifying IT, Security & Compliance
Consolidating the Stack: reducing point solutions, their agents and consoles



Reduce TTR

0

Best TTR ever?

Cloud & Container Leading the Way

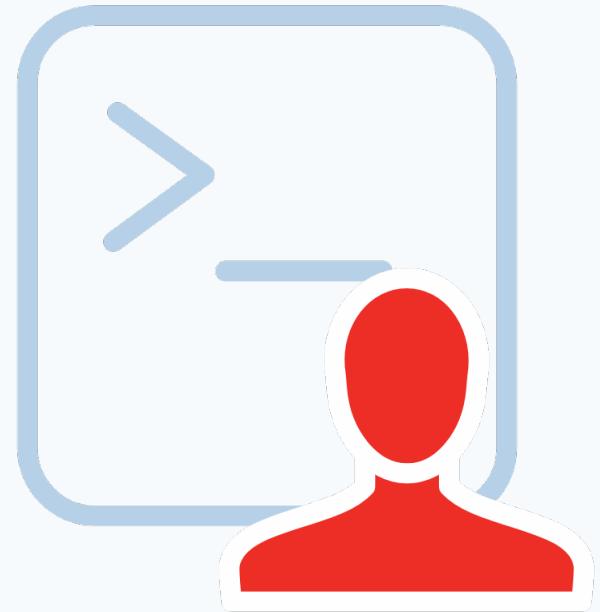
DevOps in CI/CD



Azure built-in security

Evolution of the Qualys Cloud Platform

Cloud-based platform build into
your DevOps



Qualys Next-Gen Initiatives



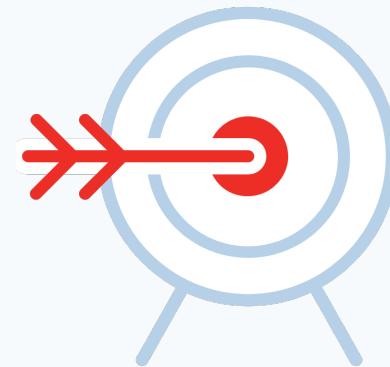
Next-Gen Initiatives 2020

Now introducing Qualys
Respond

Adding Security Analytics &
Orchestration



Comprehensive Response Capabilities



Covering servers, endpoints, mobile, network,
web applications, cloud & containers

Security Analytics, Correlation & Data Lake

Qualys built-in!

Plug-n-play analytics

Powerful cloud-based
correlation and analytics of
known & unknown threats

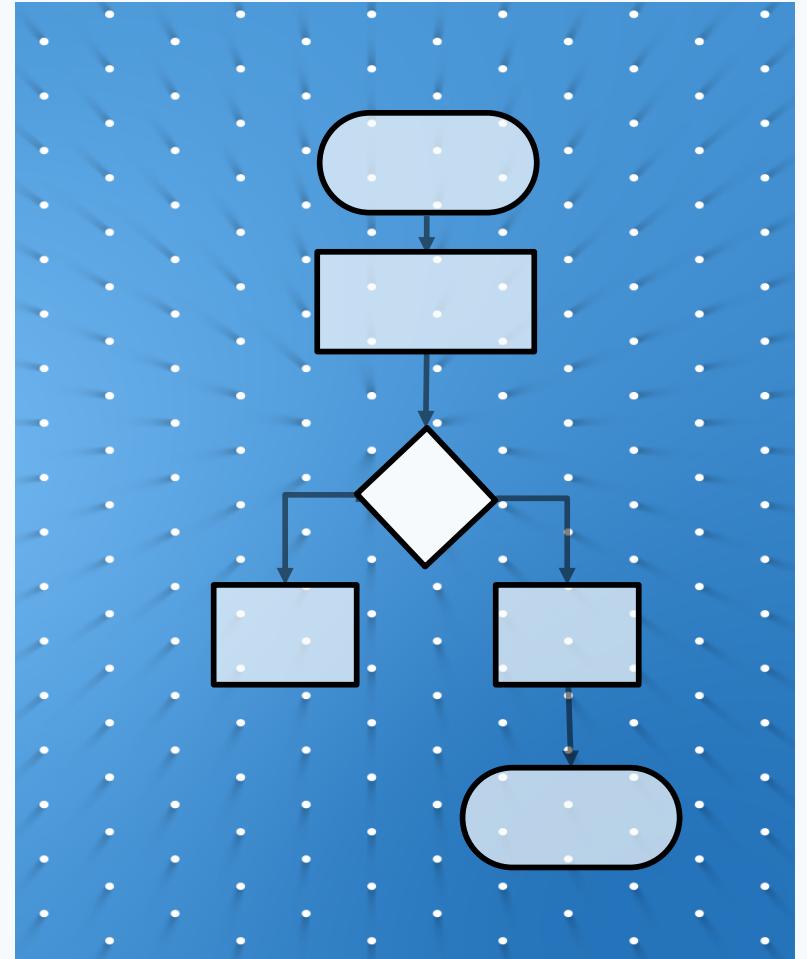


SOAR

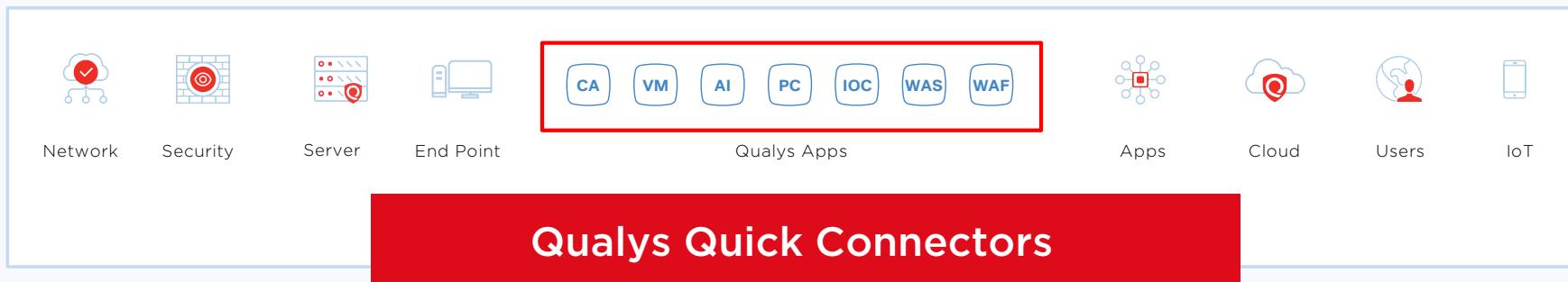
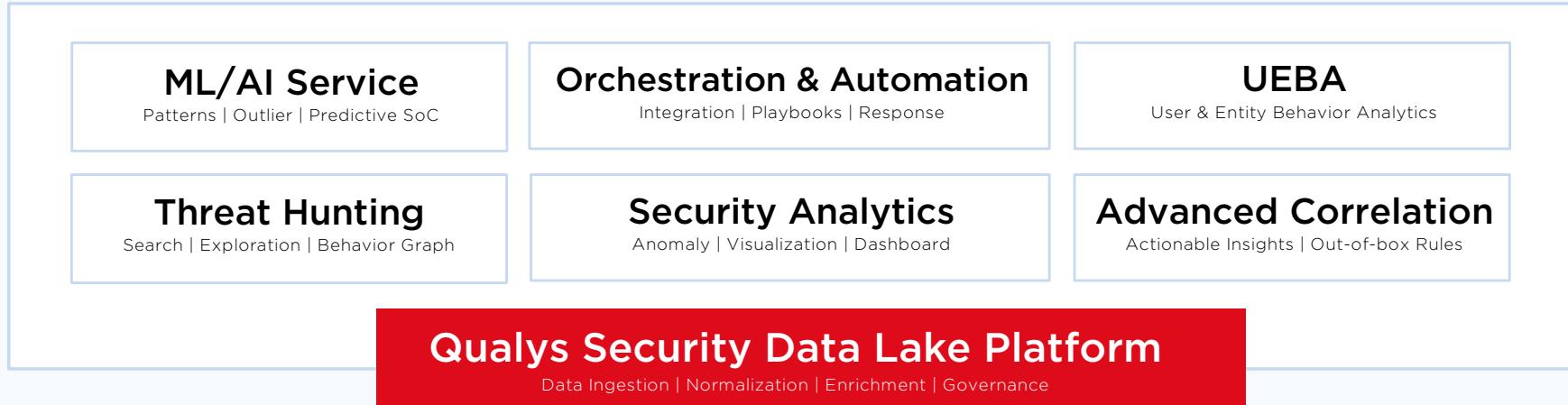
Qualys built-in!

Granular flexible playbooks

Quickly respond with complex actions



Advanced Correlation & Analytics



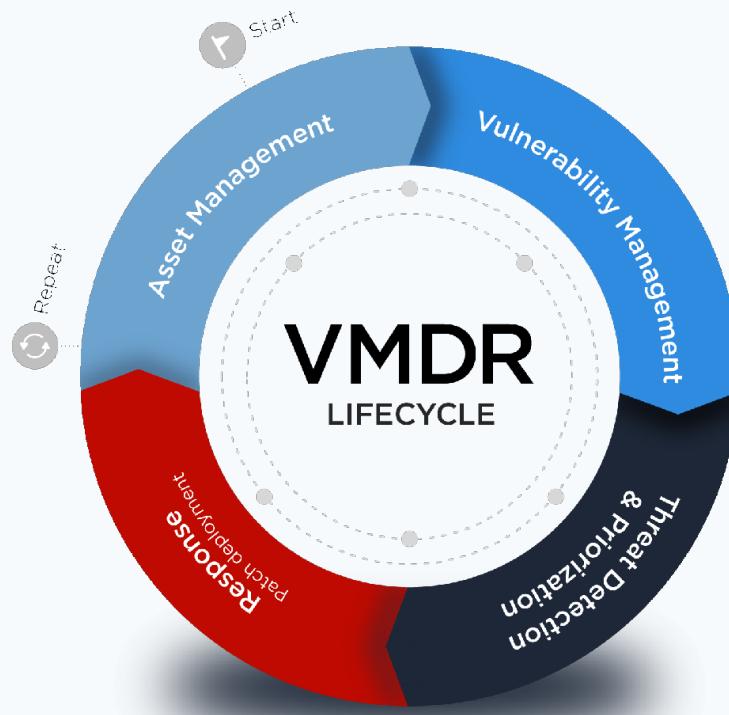
Evolving Qualys Cloud Platform to the Next Level



Single platform for detection & response with built-in orchestration



One solution to discover, assess, prioritize and patch critical vulnerabilities



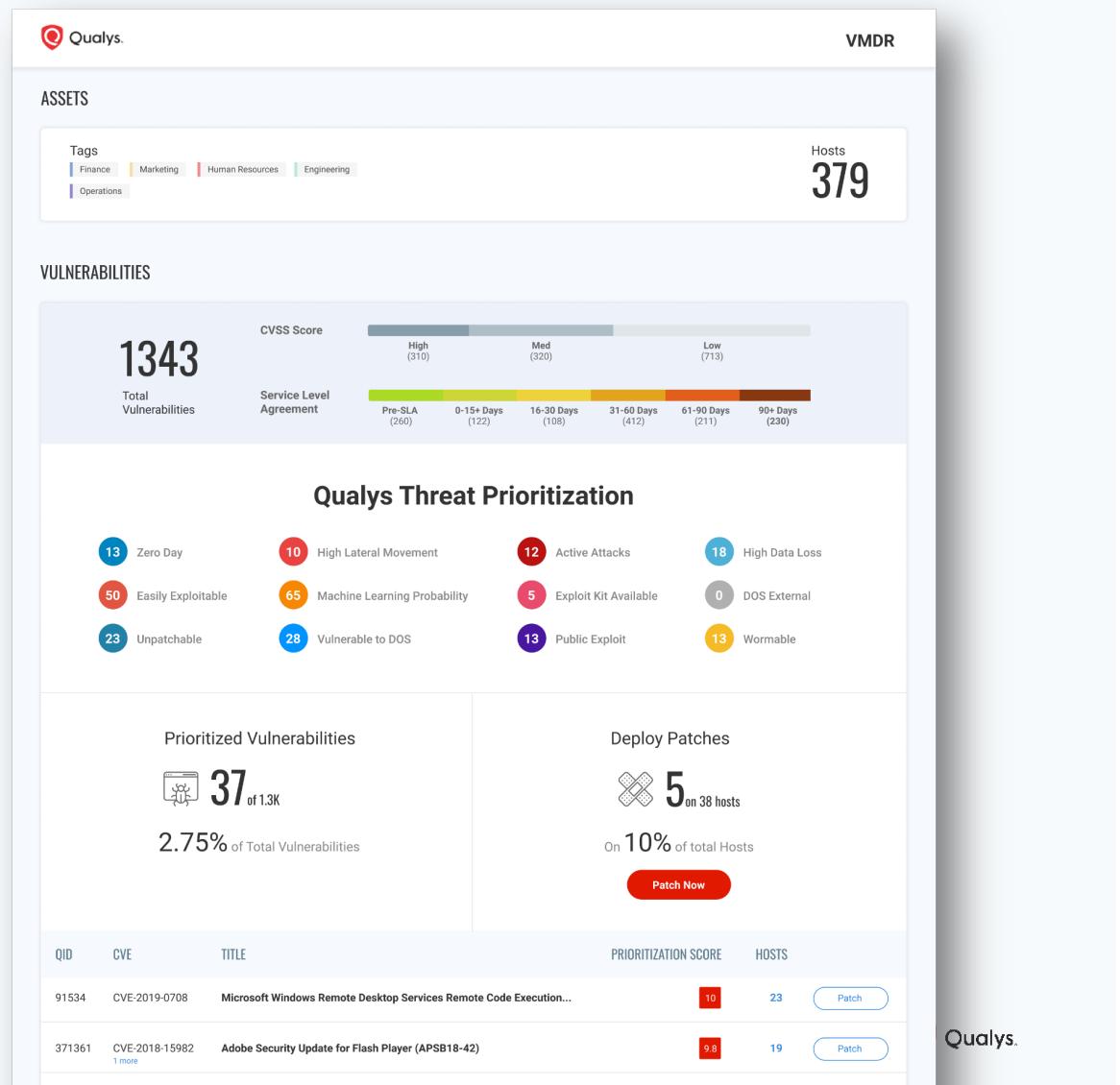
VMDR with Built-in Orchestration

New prioritization engine

Combining real-time threat intelligence, asset context and machine learning

Accurately pinpoint patches for most lethal vulnerabilities instantly

End-to-end workflows & real-time, interactive dashboards

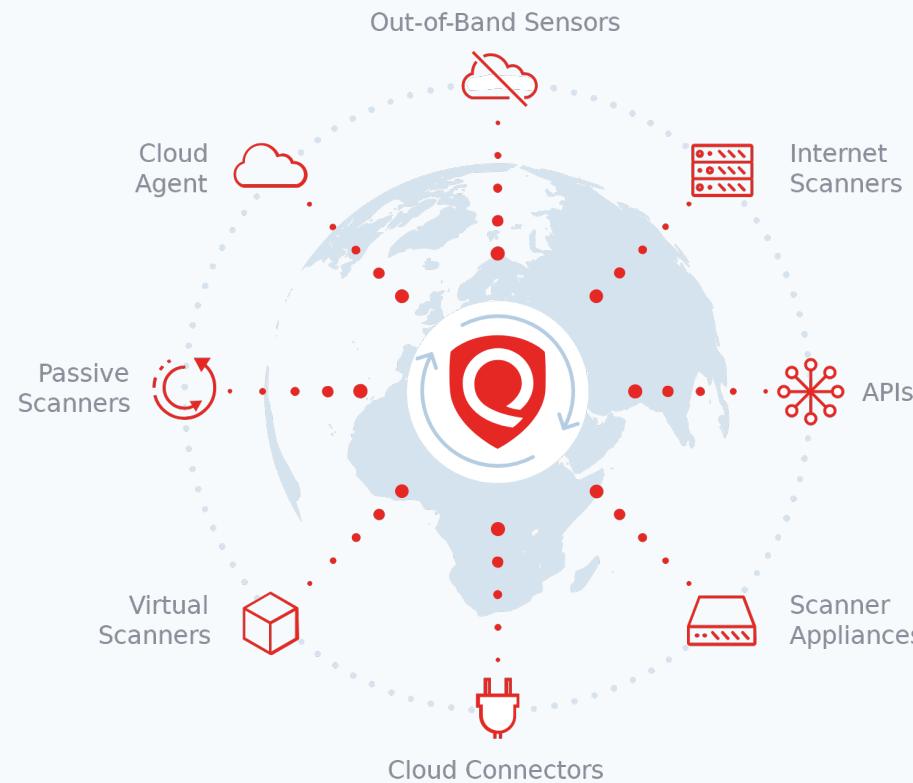


Qualys VMDR

Fastest platform to go from discovering new assets to patching it's most critical vulnerabilities with contextual prioritization

PERIOD!

Cloud Platform Architecture



Qualys Sensor Platform

Scalable, self-updating & centrally managed

Physical	Virtual	Cloud/Container	Cloud Agents	Passive	API
					
Legacy data centers Corporate infrastructure Continuous security and compliance scanning	Private cloud infrastructure Virtualized Infrastructure Continuous security and compliance scanning	Commercial IaaS & PaaS clouds Pre-certified in market place Fully automated with API orchestration Continuous security and compliance scanning	Light weight, multi-platform On premise, elastic cloud & endpoints Real-time data collection Continuous evaluation on platform for security and compliance	Passively sniff on network Real-time device discovery & identification Identification of APT network traffic Extract malware files from network for analysis	Integration with Threat Intel feeds CMDB Integration Log connectors

Qualys Cloud Platform

18+ products providing comprehensive suite of security solutions

12,200+ customers

8 shared cloud platforms across North America, Europe & Asia

85+ private clouds platforms deployed globally... on-prem, AWS, Azure, GCP

19+ PB storage and 27000 cores



Qualys Cloud Platform

3+ billion IP scans/Audits per year

50,000+ Scanner Appliances

28 million Cloud Agents

2+ trillion security events annually

5+ billion messages daily across Kafka clusters

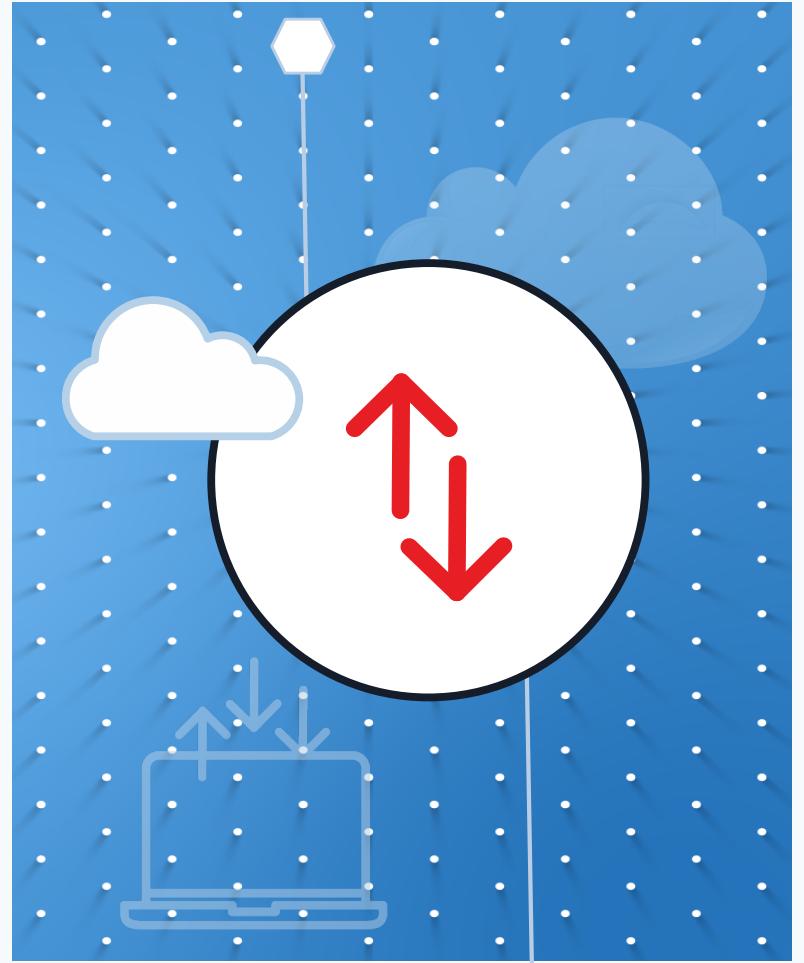
3.2+ trillion data points indexed in our Elasticsearch clusters



Continued Platform Expansion

ICS OT environments

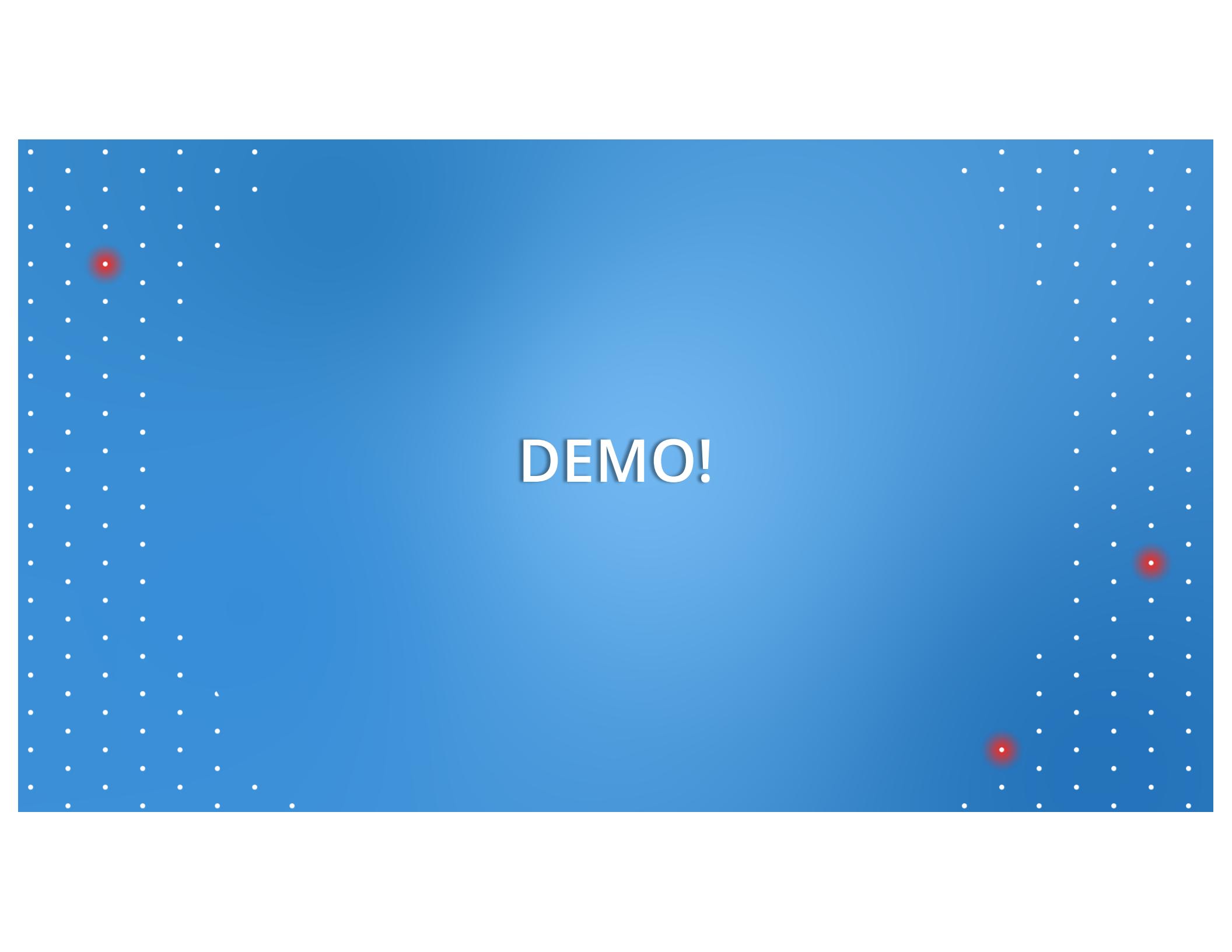
SaaS security & compliance



More DRs Coming Soon

Endpoint Detection & Response
Cloud Detection & Response
Container Detection & Response
Mobile Device Detection & Response
SaaS Security Detection & Response

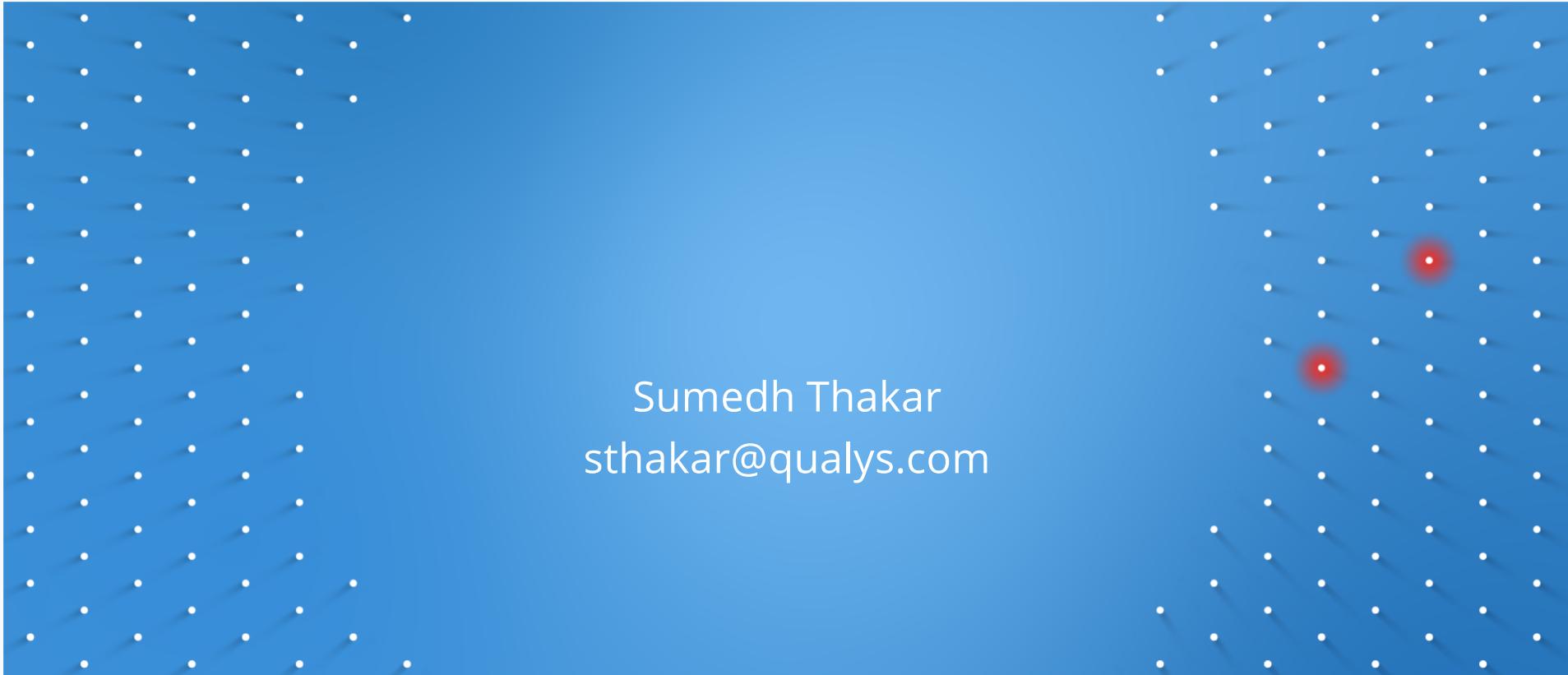




DEMO!



QUALYS SECURITY CONFERENCE 2019



A large blue rectangular area serves as the background for the speaker information. It features a subtle pattern of white dots arranged in a grid-like fashion, with two distinct red glowing circular highlights appearing on the right side of the pattern.

Sumedh Thakar
sthakar@qualys.com