Extending the Power of the Qualys Platform for Protecting Your Endpoints: The Last Line of Defense in Your Cyber Risk Program

Utpal "U.J." Desai,
Andrew Morrisett
Qualys Product Management

Agenda

01 Our Approach

02 Product Capabitlies Overview

03 Product Demonstration

04 Case Study

Qualys.

Qualys®

Enterprise TruRisk™ Platform

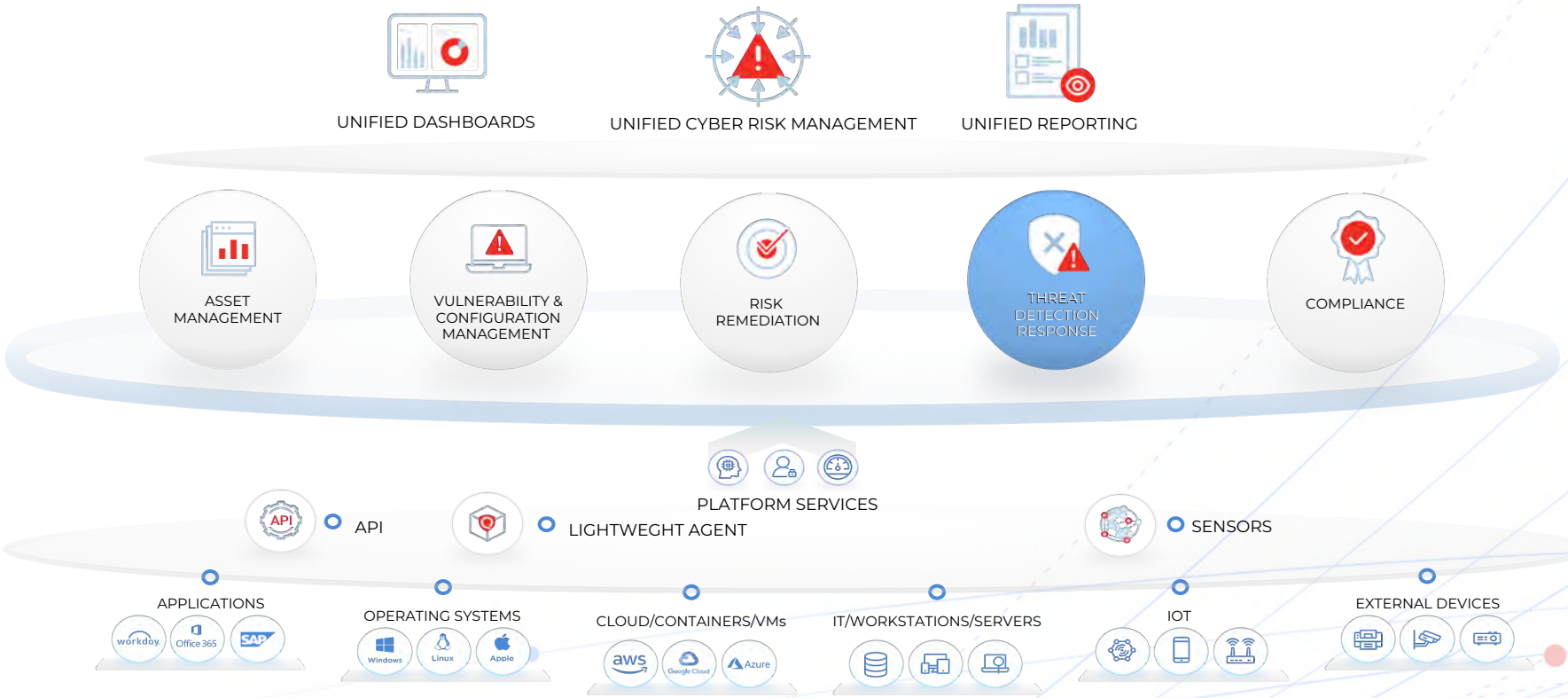
Measure, communicate, and eliminate cyber risk.

De-risk your business.

The Qualys Enterprise TruRisk Platform

Measure, Communicate and Eliminate the Cyber Risk

Qualys TruRisk™



Qualys.

Challenges with Endpoint Security Today

Qualys.

Too Many EDR Alerts

How do you Measure risk? Which alerts should I prioritize?

30% Alerts go unnoticed or without investigation

2 days Time to vuln weaponization

34 days Average time to patch a vulnerability

Hours Time to inflict harm

277 days Average time to identify and contain a threat

Qualys.

Organizations Lack Visibility

How do you communicate risk??

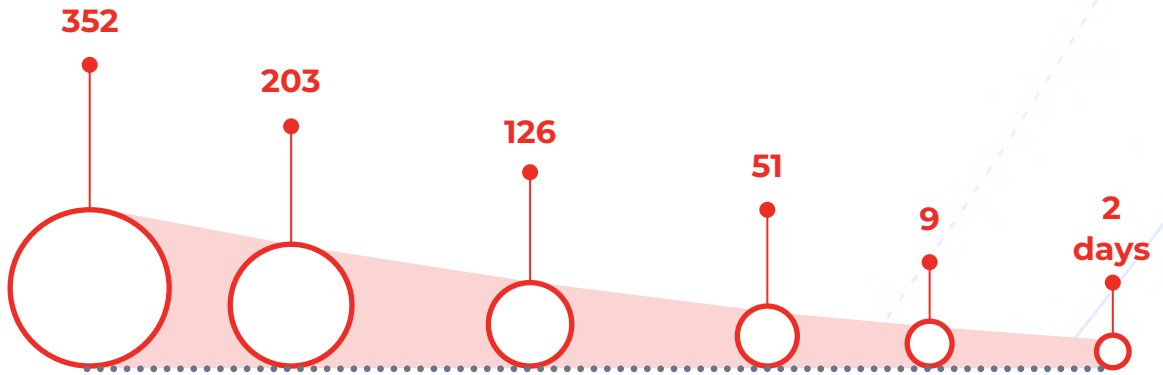
What is the root cause of the malware incidents?

Which vulnerabilities or misconfiguration are exploited by the threat actors in my environment?

Which assets are likely to be exploited?

Qualys.

of Days after NVD Publication that Exploit Weaponized Occurred



- 2018: Exploit weaponization took 352 days
- **2022: Time to weaponize exploit down to 9 days**
- **Mass exploitation of Log4Shell occurred in 48 hours**

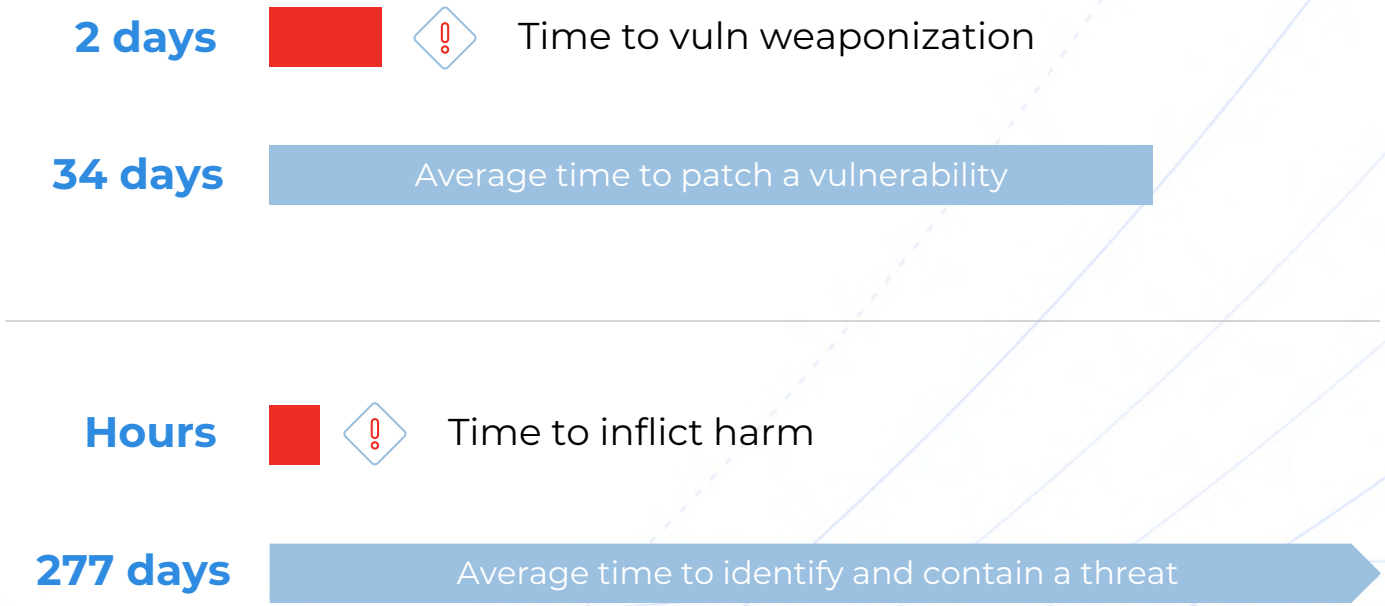
Malware	CVE & Patch Count	Misconfigs Count
Conti	24	61
DarkSide	4	54
Netwalker	8	3
Petya	10	6
REvil	24	27

Too Many EDR Alerts

How do you Eliminate risk?

50%

Of businesses worldwide have experienced recurring attacks from the same hackers



Qualys.

Security Silos Limit on Defender's Efficiency

How do you communicate Cyber Risk?

Asset Management

Discovery
Asset Inventory
Business context

Vulnerability Management

Vulnerability Scans
Config assessment
Compliance

Patch Management

Patch Management
Config Management

Best opportunity to stop threats and reduce risk

BARRIER

Threat Prevention

Anti-malware
Behavioral
ML/AI

Threat Detection

Endpoint
Cloud

Threat Response

Triage
Investigation
Containment
Recovery

Best insights into threat landscape

Qualys.

Updated: 10/03/2023

The Solution

Qualys.

Risk-based Approach for Endpoint Security

Breaking down Organization and Product Silos

Deep context to help prioritize, speed investigations

Asset Management
Discovery
Asset Inventory
Business context

Vulnerability Management
Vulnerability Scans
Config assessment
Compliance

Patch Management
Patch Management
Config Management

Prioritized patching reduces security alerts

Powerful next-gen AV with multi-layered prevention

Threat Prevention
Anti-malware
Behavioral
ML/AI

Threat Detection
Endpoint
Cloud

Threat Response
Triage
Investigation
Containment
Recovery

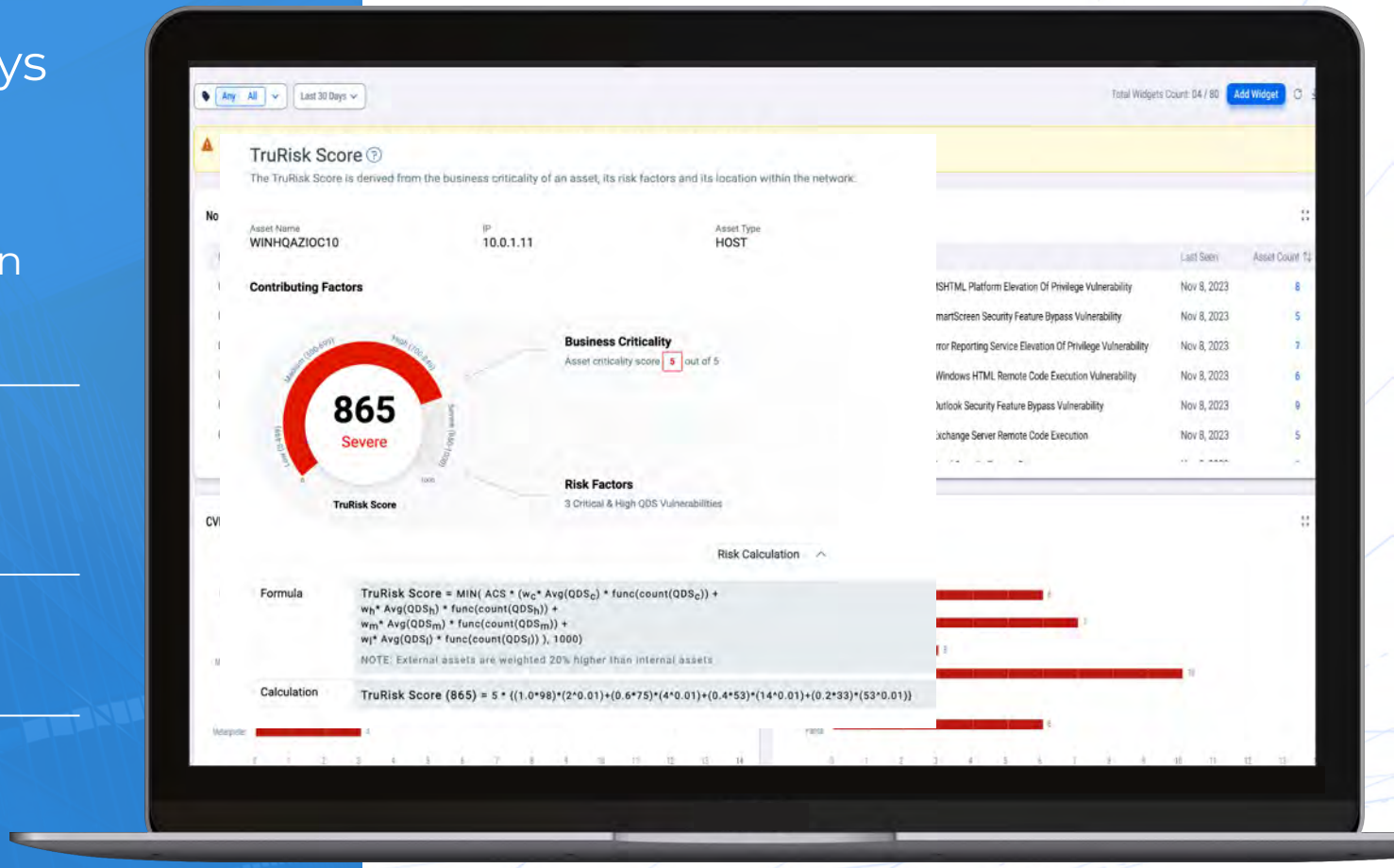
Threat and vulnerability insights to help optimize defenses

Qualys.

Risk-based Approach for Endpoint Security

Measure Risk of attacks with Qualys Endpoint Protection

- Automatic alert prioritization based on asset business context and threat intelligence
- Asset Protection Blind Spot
- TruRisk Score Trends

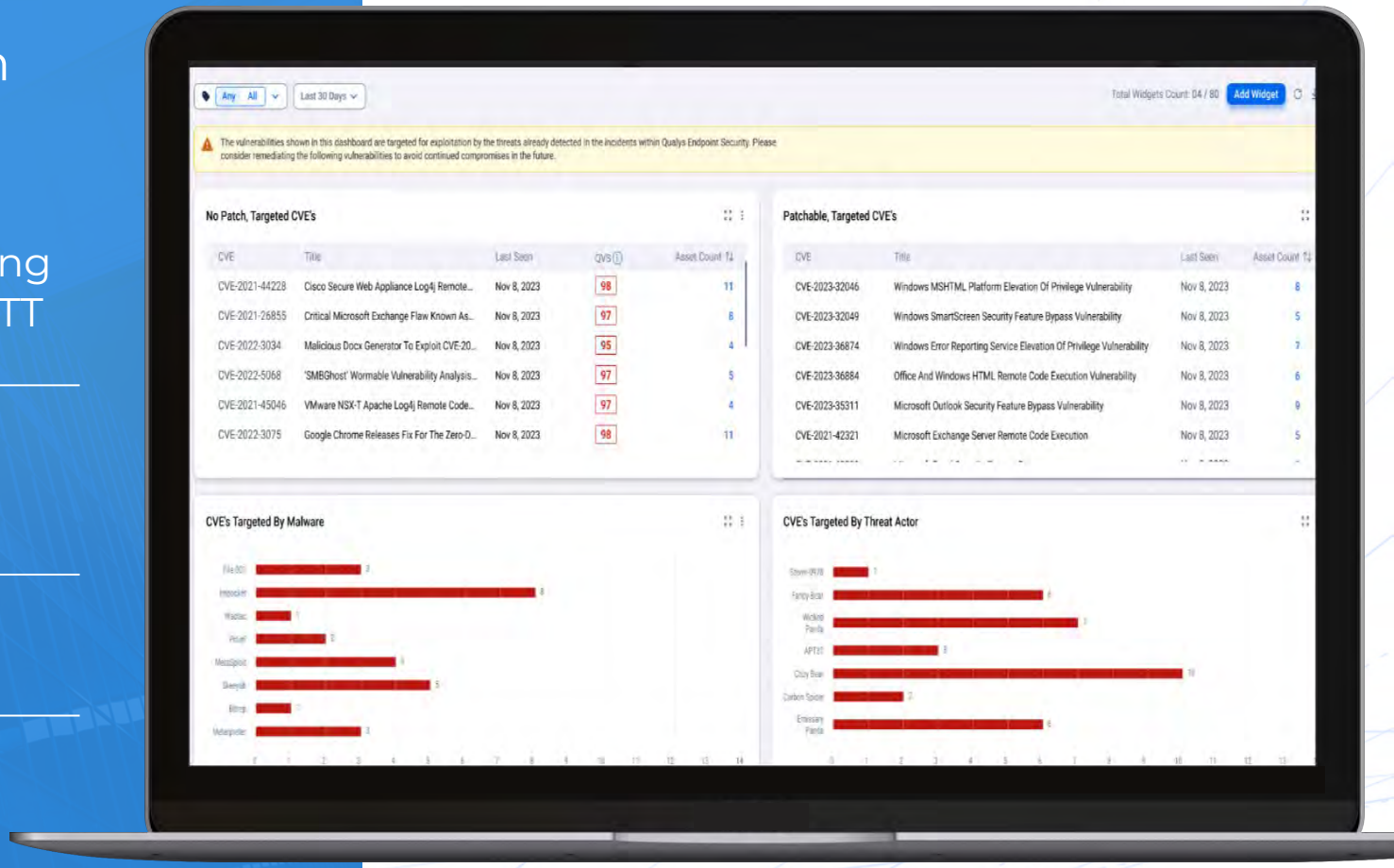


Qualys.

Risk-based Approach for Endpoint Security

Communicate Risk of attacks with Qualys Endpoint Protection

- Type of threats and threat actors detected in your environment including CVEs, Misconfigurations and MITRE ATT & CK mapping
- Identify risky users and assets for remediation and automatic response
- A Single Pane of Glass visibility



Qualys.

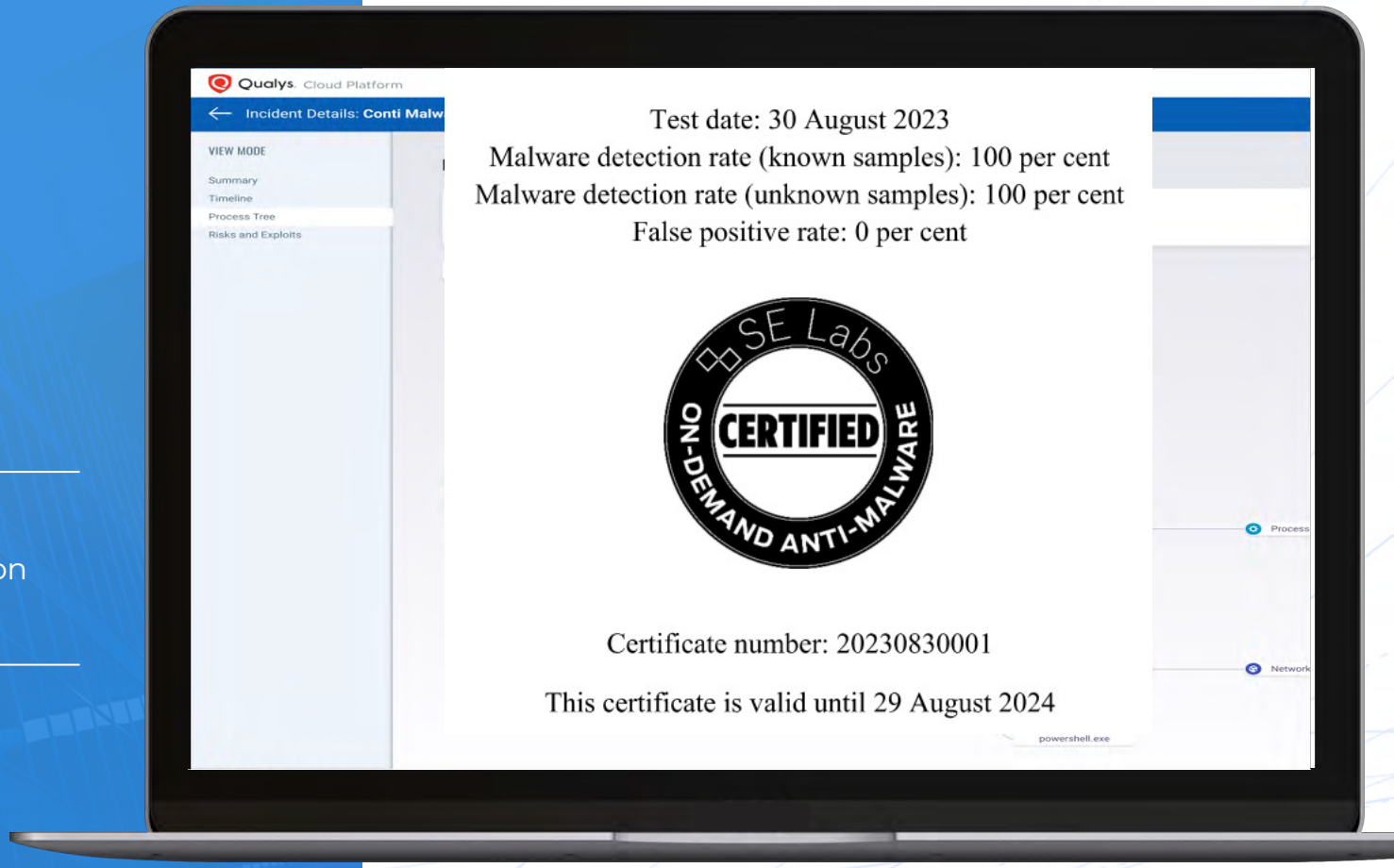
Risk-based Approach for Endpoint Security

Eliminate Risk of known and unknown attacks with Qualys Endpoint Protection

- Multiple layers of mature behavior and ML-based protection technologies effective in blocking zero-days including ransomware, fileless attacks and credential-theft

- Automatic Incident Prioritization based on asset context allowing security administrators to focus on the most important activities

- Out of the box automation options to define your risk thresholds and response
  - Isolate host based on vulnerabilities
  - Automatically kill the process when a malicious hash is detected



Qualys.

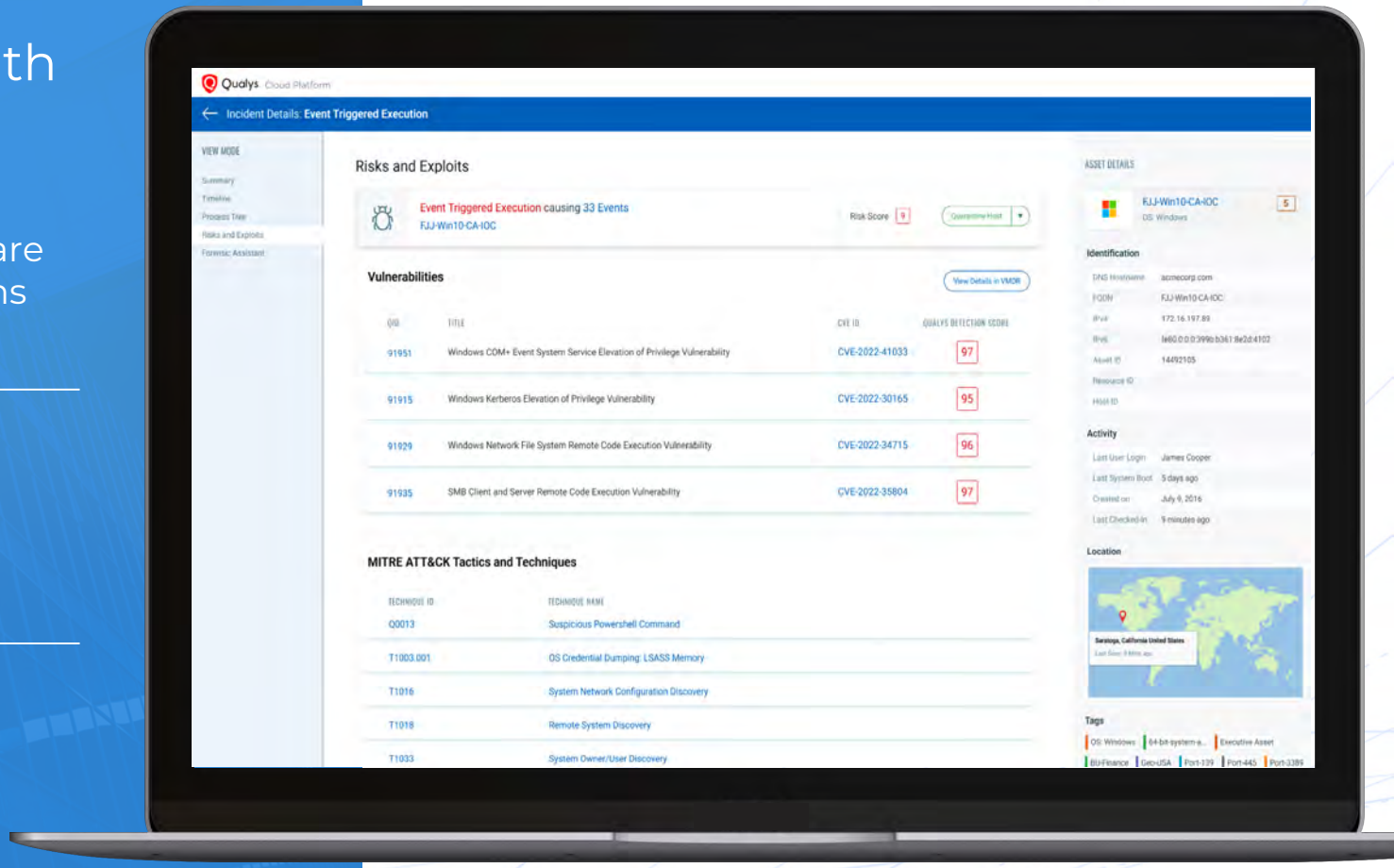
Risk-based Approach for Endpoint Security

Eliminate Risk of future attacks with Qualys Endpoint Protection

01 Ability to automatically correlate malware detection to CVEs and Misconfigurations

02 Ability to automatically identify other assets in your environment that could be at risk

03 Ability to remediate CVEs and misconfigurations associated with malware detected and autotune protection to prevent future attacks



Qualys.

Risk-based Approach for Endpoint Security

Eliminate Risk of future attacks with Qualys Endpoint Protection

Stratejm

nuspire

kellerschroeder
APPLICATIONS SOLUTIONS GROUP

MDR Services

Qualys

Falkirk Council

Enhanced protection and team productivity with a single pane of glass visibility

Consolidated 5 different security tools with Qualys

Migration in Four Weeks

40% Cost Savings

Teams are more productive

Qualys.

Falkirk Council

Product Demo

Qualys.

Risk-based Approach for Endpoint Security

Measure, Communicate and Eliminate Risk with Qualys Endpoint Protection

01 Reduce risk of business disruption and breaches by preventing more attacks automatically

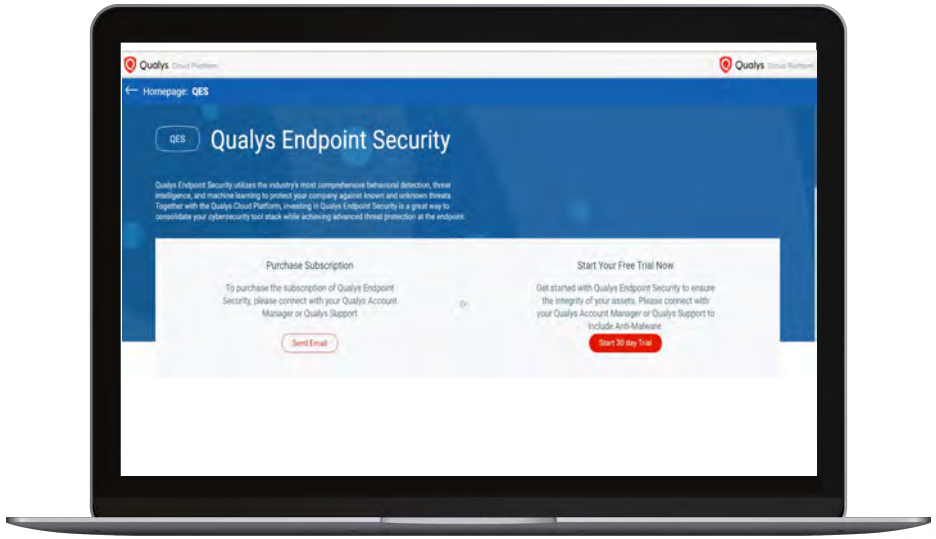
02 Reduce alert fatigue and eliminate the risk of future attacks by close loop response

03 Speed up incident response by breaking down organization and product silos

Qualys.

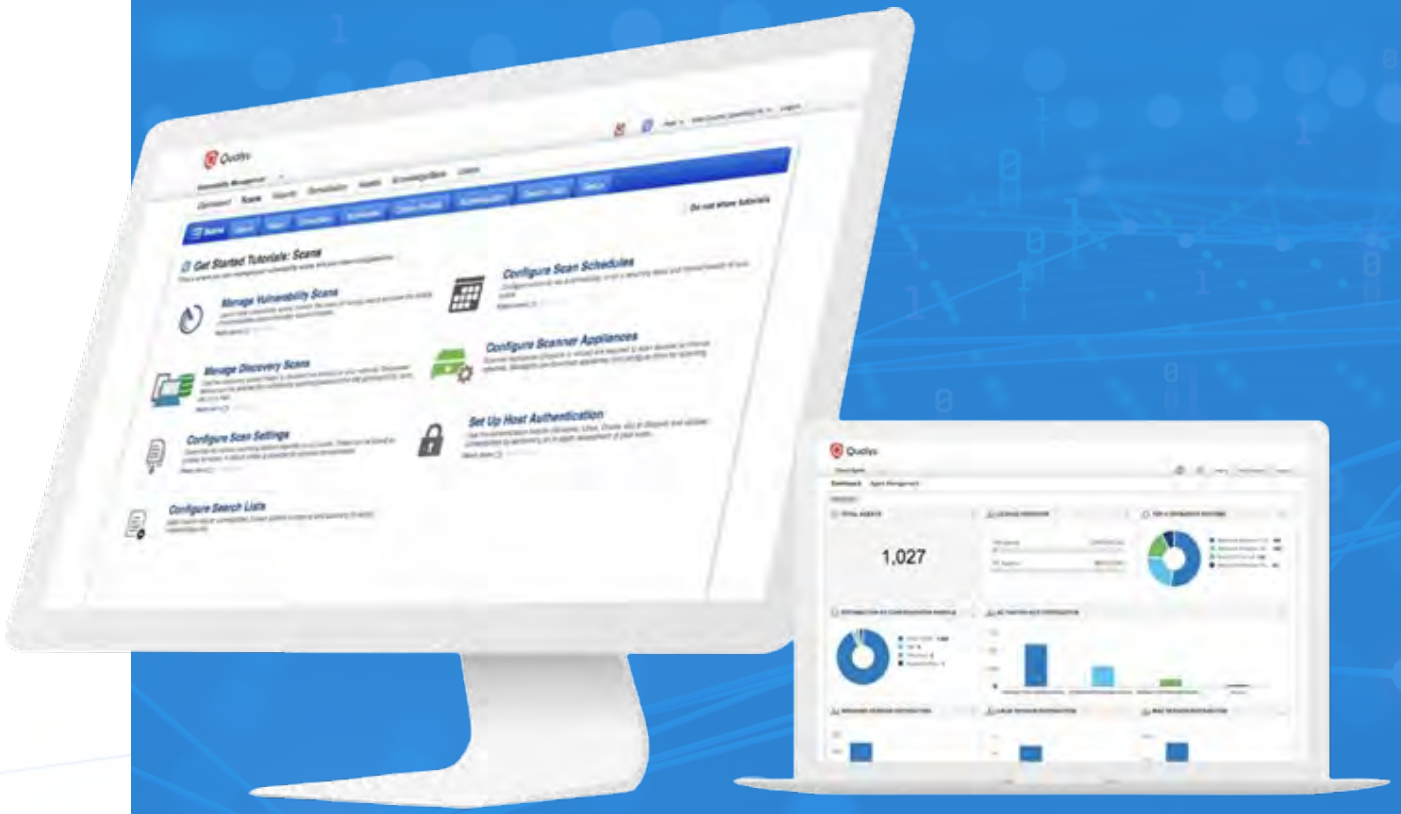
Try it today

Existing Qualys Customer?



New to Qualys?

https://www.qualys.com/free-trial/



Qualys.

Qualys®