Controlware Security Day 2022

Eine einheitliche Sicht über Ihre IT-Sicherheit

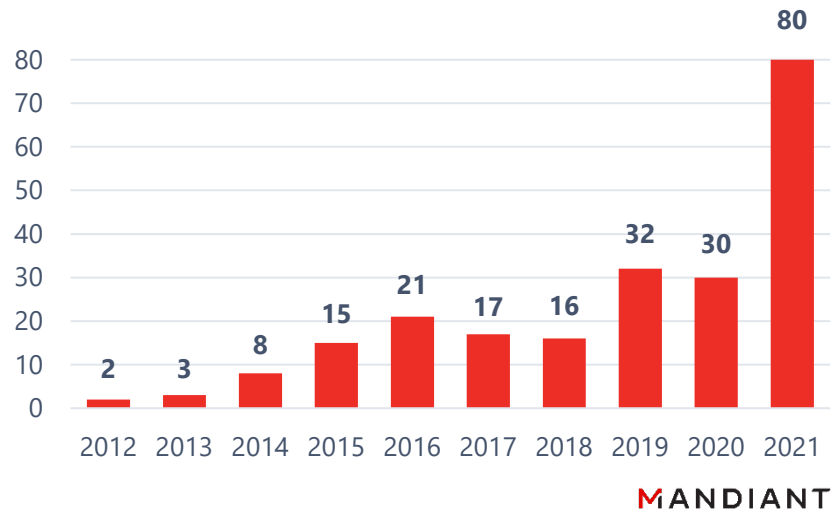
Mit der Technologie der Qualys Cloud liefern wir Ihnen eine einheitliche Sicht auf Ihren IT-Security Status

controlware

GET MORE SECURITY. Qualys.

Mehr Exploits

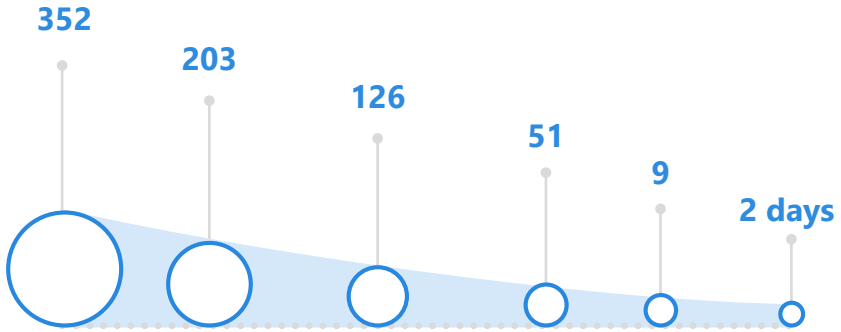
Die Zero-Day-Exploitation erreichte 2021 ein Hoch und haben sich seit 2020 mehr als verdoppelt



Zero-day exploits have grown by 250% in one year according to recent Mandiant Threat Intelligence

Faster Weaponization

Weaponization von Exploits hat sich **beschleunigt** – mit höherer Geschwindigkeit und größerer Menge



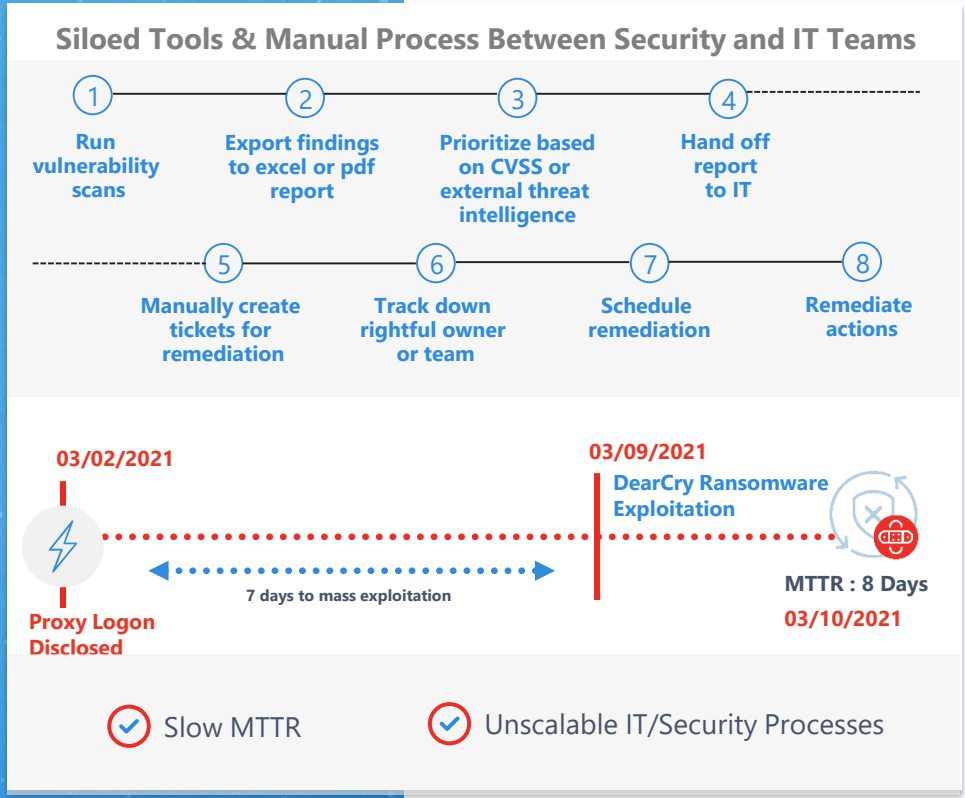
2018: Exploit weaponization took 352 days

2022: Time to weaponize exploit down to 9 days

Mass exploitation of Log4Shell occurred in 48 hours

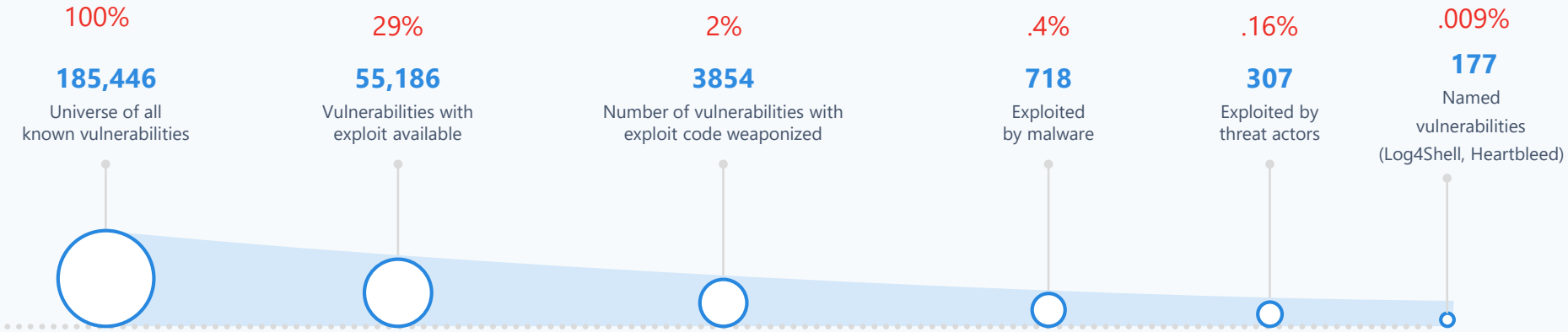
Slow Remediation Times

Eine langsame Reaktion kann den Unterschied zwischen einem **laufenden Unternehmen und einem Unternehmen ausmachen, dass tagelang offline ist**



Weniger über Schwachstellen → Mehr zu Risiko

Number of Vulnerabilities



Weniger als 2 % der Schwachstellen verursachen das größte Risiko!

Source: Qualys Inc.

controlware

GET MORE SECURITY. Qualys.

Gleiche Interessen – unterschiedliche Herausforderungen

Security Leaders

- Welche **geschäftlichen Auswirkungen** hat mein Risiko und wo ist es angesiedelt?
- Welche Schwachstellen, Assets oder Asset-Gruppen stellen das **höchste Risiko** dar?
- Welche Schwachstellen werden wahrscheinlich **in meiner Umgebung** ausgenutzt?

IT Leaders

- Wie können wir die Lücke zwischen **IT & Security schließen**?
- Wie können wir automatisieren, um die MTTR zu reduzieren?
- Wie können wir das Risiko von **Ausfallzeiten** reduzieren?

Wie können wir die Wirksamkeit unserer Cybersicherheitsprogramme veranschaulichen?

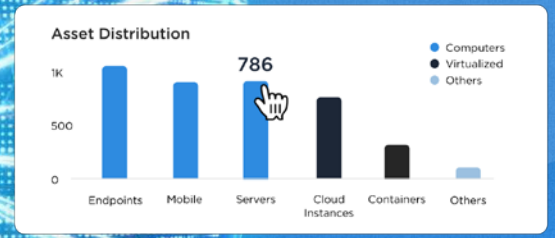
Beheben wir die richtigen Dinge, um Risiken zu reduzieren?

Cloud Agent,
Mobile Device
Agent,

Passive Sensor

Network Scanner

Cloud Connectors &
Container Sensors



VMDR 2.0 Path of Innovation

Asset and Vulnerability Management, Threat Prioritization and Patching

Asset Inventory & Management

Hybrid environment across IT,OT, IoT, Mobile, Containers and more

Vulnerability & Configuration Assessment

Near real-time scanning for latest vulnerabilities

Threat Prioritization

Prioritize based on threat, asset, & vulnerability context

Patch Management

Precise patch identification and remediation

2-second visibility

Across a hybrid infrastructure

69K+ CVE's

<24-hour response for critical CVE's

4-hour MTTD

15+ RTI's

Ransomware, active attacks, CISA known exploited & more

Multiple attack surface options

60% Faster

Remediation for critical vulnerabilities

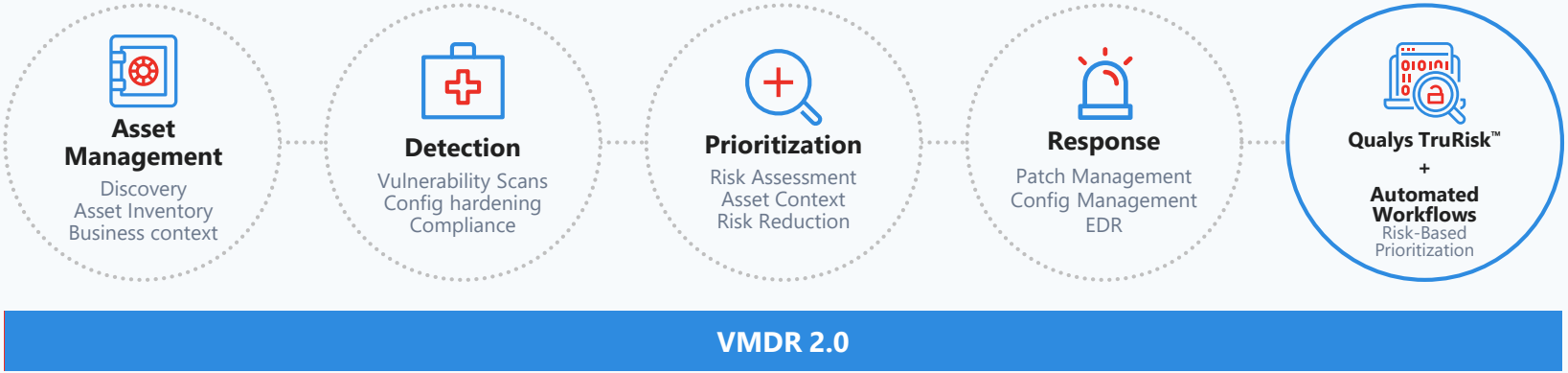
controlware

GET MORE SECURITY. Qualys.

Bringing Risk Insights into Intelligent Response

Wo IT- und Sicherheitsteams früher gezwungen waren, zahlreiche Einzellösungen zu verwenden, bot Qualys VMDR 1.0 eine ganzheitliche, integrierte Einzellösung.

Jetzt fügt VMDR 2.0 mit Qualys TruRisk eine beispiellose Cyber-Risikoquantifizierung, Visualisierung, automatisierte Workflows mit ITSM- und QFlow-Integrationen in einer einzigen einheitlichen Lösung hinzu.



controlware

GET MORE SECURITY. Qualys.

VMDR 2.0 Key Capabilities

Bringing **Prioritization** and **Automated Workflow** to Vulnerability Management Detection and Response, with:

- **Understand and Manage Cybersecurity Risk:** Quantifizieren Sie das Risiko über Schwachstellen, Assets und Asset-Gruppen hinweg, um Organisationen dabei zu helfen, Risiken proaktiv zu reduzieren und die Risikominderung im Laufe der Zeit mit Qualys TruRisk ™ zu verfolgen

- **Close the IT-Security Gap:** Vereinheitlichen Sie Sicherheits- und IT-Bedrohungsreaktionspfade für eine schnellere Behebung mit nahtloser Integration zwischen ITSM-Tools wie ServiceNow und Patch-Management-Lösungen

- **Automate remediation with no-code workflows:** Sparen Sie wertvolle Zeit, indem Sie betriebliche Aufgaben mit Qualys QFlow automatisieren und orchestrieren

- **Receive Preemptive Attack Alerts :** Nutzen Sie Erkenntnisse aus über 180.000 Schwachstellen aus über 25 Bedrohungsquellen, um mit der Qualys Threat DB präventive Warnungen zu potenziellen Angriffen zu erhalten

controlware

GET MORE SECURITY. Qualys.

VMDR 2.0 with TruRisk

A Fresh Approach to Reduce Cyber Risk

VMDR 2.0 with Qualys TruRisk™ offers

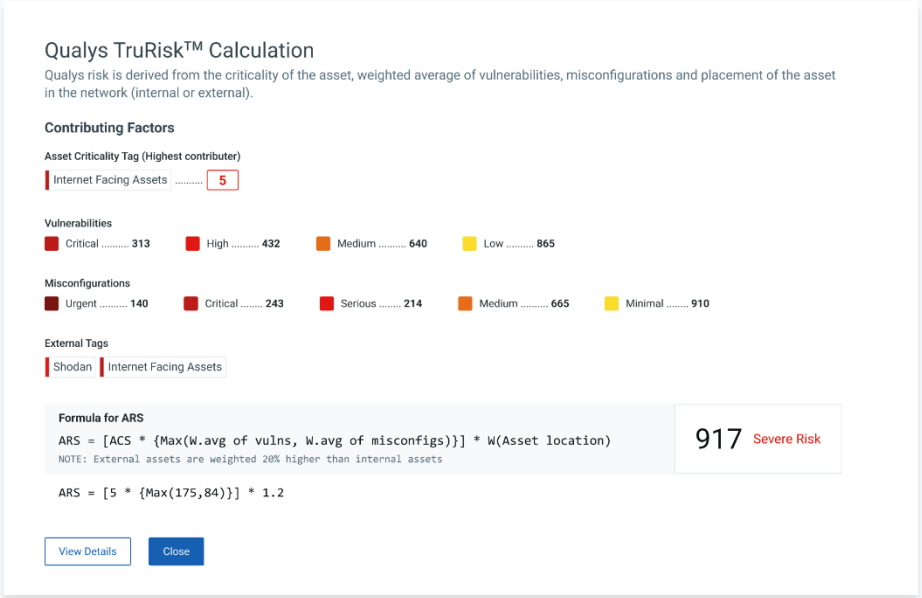
Better Cybersecurity Risk Intelligence:
mit detailliertem und transparentem Risiko-Scoring

Faster Remediation:
mit automatisierten No-Code-Workflows

Qualys TruRisk

Transparent Cyber Risk Measurement and Visualization

- **Asset Risk Score**
  Basierend auf der Kritikalität von Assets, die direkt aus Ihrer CMDB stammt oder definieren Sie regelbasierte Kritikalität + QDS + Minderung
- **Qualys Detection Score (QDS)**
  Severity of the vulnerability, misconfiguration + environmental factors + attack surface + threat indicators + active malware mapped to vulnerabilities
- **Mitigation Factors**
  Kompensierende Konfigurationskontrollen, Sicherheitstools, die die Ausnutzung blockieren
- **Asset Group Risk**
  Bewerten Sie das Risiko von Assetgroups, identifizieren Sie Risiken, verfolgen Sie die Risikominderung und messen Sie die Wirksamkeit des Cybersicherheitsprogramms



controlware

GET MORE SECURITY. Qualys.

Qualys TruRisk

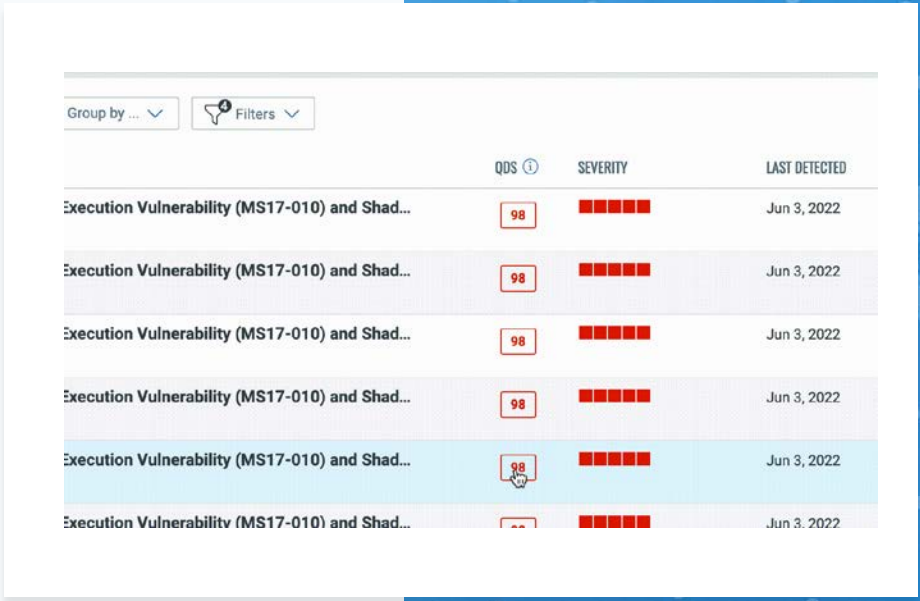
Transparent Cyber Risk Measurement and Visualization

Asset Risk Score
Basierend auf der Kritikalität von Assets, die direkt aus Ihrer CMDB stammt oder definieren Sie regelbasierte Kritikalität + QDS + Minderung

Qualys Detection Score (QDS)
Severity of the vulnerability, misconfiguration + environmental factors + attack surface + threat indicators + active malware mapped to vulnerabilities

Mitigation Factors
Kompensierende Konfigurationskontrollen, Sicherheitstools, die die Ausnutzung blockieren

Asset Group Risk
Bewerten Sie das Risiko von Assetgroups, identifizieren Sie Risiken, verfolgen Sie die Risikominderung und messen Sie die Wirksamkeit des Cybersicherheitsprogramms



controlware

Qualys TruRisk

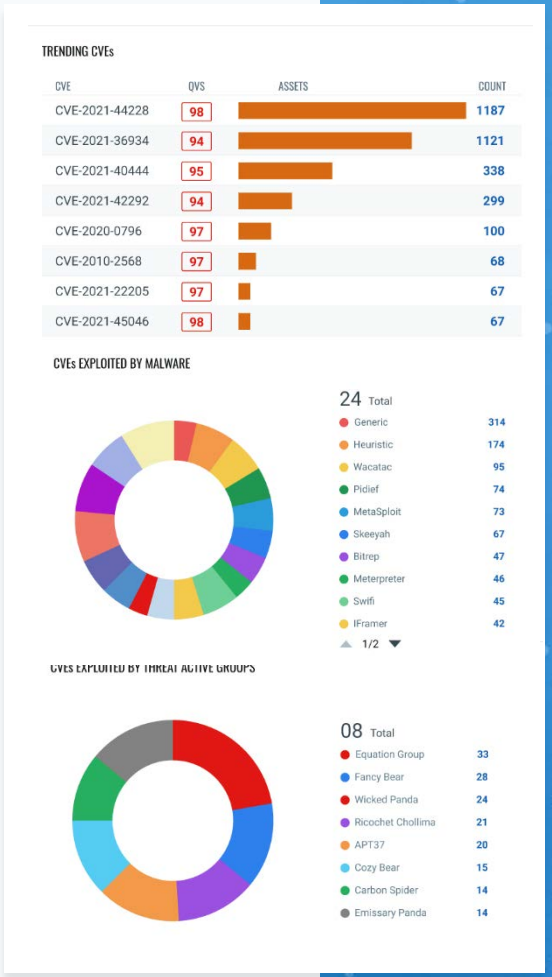
Transparent Cyber Risk Measurement and Visualization

- **Asset Risk Score**
  Basierend auf der Kritikalität von Assets, die direkt aus Ihrer CMDB stammt oder definieren Sie regelbasierte Kritikalität + QDS + Minderung
- **Qualys Detection Score (QDS)**
  Severity of the vulnerability, misconfiguration + environmental factors + attack surface + threat indicators + active malware mapped to vulnerabilities
- **Mitigation Factors**
  Kompensierende Konfigurationskontrollen, Sicherheitstools, die die Ausnutzung blockieren
- **Asset Group Risk**
  Bewerten Sie das Risiko von Assetgroups, identifizieren Sie Risiken, verfolgen Sie die Risikominderung und messen Sie die Wirksamkeit des Cybersicherheitsprogramms

controlware

Comprehensive Exploit and Threat Intelligence

- CVE Intelligenz für über 180K CVE's
- Threat and exploit Intelligenz aus 25+ Quellen
- Konzentrieren Sie sich auf das wahre Risiko, das durch CVEs dargestellt wird, die in freier Wildbahn ausgenutzt werden, ausgenutzt werden von Malware, Ransomware-Gruppen und active threat actors

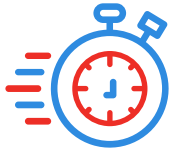


controlware

VMDR 2.0: Driving Value for Security and IT

Better Understand and Manage Cybersecurity Risk

Machen Sie sich mit den geschäftlichen Auswirkungen von Cyberrisiken vertraut und schließen Sie die Cybersicherheits- und IT-Lücke für optimierte Compliance, Berichterstattung und skalierbare Unternehmensführung.



Faster Threat Response

Priorisierung und automatisierter Workflow für Vulnerability Management, Detection and Response.

More Accurate Threat Response

Nutzen Sie eine kontinuierlich verbesserte Bedrohungsdatenbank und die Qualys Cloud-Plattform für detaillierte Bedrohungsinformationen und fundierte Reaktionsmaßnahmen.

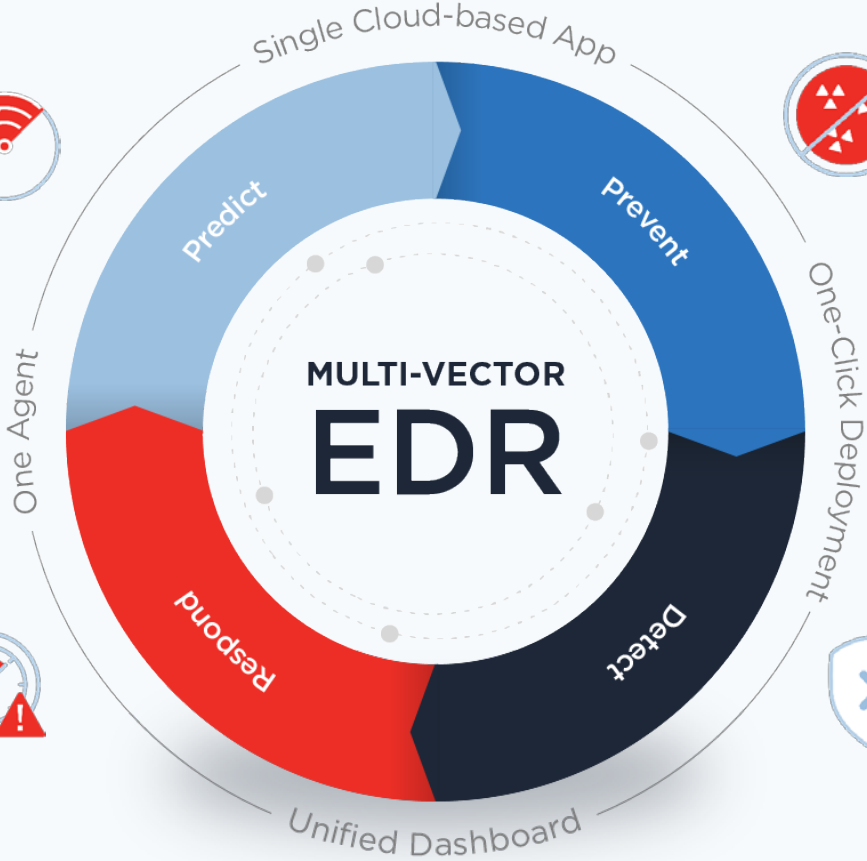
controlware

GET MORE SECURITY. Qualys.

Qualys Multi-Vector EDR

Vorhersagen

- Vulnerabilities
- Baselines
- Asset Inventory



Schützen

- Hardening
- Isolation
- Attack surface

Reagieren

- Investigate
- Remediate
- Design Change

Erkennen

- Detect
- Contain
- Prioritize

controlware

GET MORE SECURITY. Qualys.

Benefits of Multi-Vector EDR

EDR

Vorhersagen

Identify Critical Unprotected Assets

Malware-to-Vulnerability Correlation

Malware-to-Misconfiguration Correlation

Schützen

Proactive Malware Blocking

Memory Protection

Behavioral Protection

Phishing Protection

Network Protection

Erkennen

Endpoint Telemetry

Threat Intelligence

MITRE ATT&CK

Advanced Correlation Rules

Timeline & Process Tree View

Threat Hunt

Origins of Malware or Breach

Reagieren

Automated Action

Kill Process

Quarantine File or Host

Prevent Future Attacks:
Patch related vulnerabilities
Fix misconfigurations

controlware

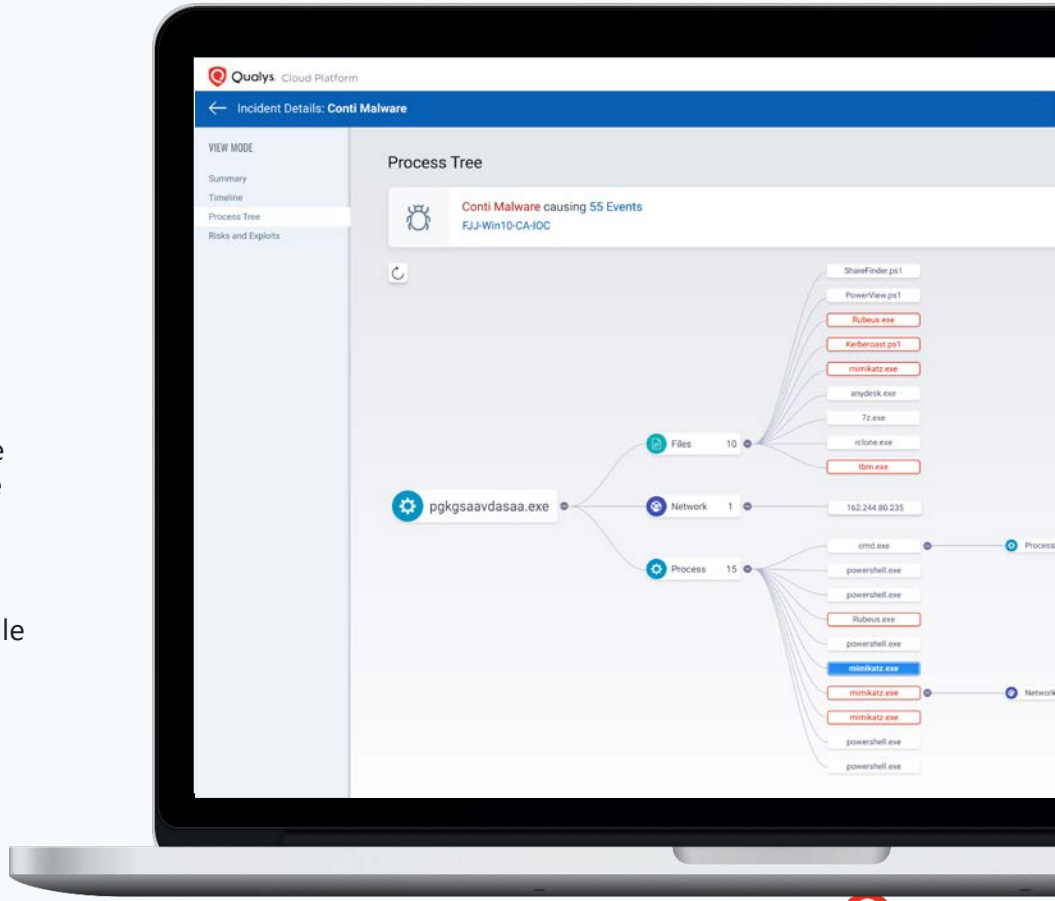
GET MORE SECURITY. Qualys.

EDR

Multi-Vector EDR

Endpoint Security with Complete Context

- One Agent, one platform, one place to execute
- Vorhersagen und schützen sowie erkennen und reagieren
- Priorisieren Sie die Reaktion auf Vorfälle, indem Sie korrelierte Risikobewertungen nutzen, um kritische Ressourcen zu priorisieren
- Verbinden Sie Erkenntnisse aus Bedrohungen, Schwachstellen und Fehlkonfigurationen für schnelle Reaktions- und Patching-Funktionen



controlware

GET MORE SECURITY. Qualys.

Q&A

Vielen Dank

Holger Schellein
Post-Sales Account Manager DACH
hschellein@qualys.com

controlware

Qualys.
Continuous Security