Qualys ROCon 26
The Risk Operations Conference
EMEA

How to Eliminate Risk Most Efficiently





Eran Livne

Senior Director,
Product Management,
Endpoint Remediation

Qualys ROCon 26
The Risk Operations Conference
EMEA

Manual Remediation Is Dead

30+ Days

Human Speed

Average Window of Exposure before manual patching completes.

The Mythos Avalanche



-7 Days

Machine Speed

Attacker exploitation window using AI-generated tooling.

If Vuln & Patch count increases 2x or 3x, you cannot outrun an AI-driven pace of detection & exploitation with human speed.

Remediation must become autonomous. But we must address the three systemic fears:

Trust. Confidence. Backup Plan.

National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

Qualys ROCon 26
The Risk Operations Conference
EMEA

Cyber Essentials: Requirements for IT Infrastructure v3.3

Requirements

You must make sure that all software in scope is kept up to date. All software on in-scope devices must:

- Be licensed and supported
- Be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to or from the internet
- Have automatic updates enabled where possible
- Be updated, including vulnerability fixes, **within 14 days*** of release, where:
    - The update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'
    - The update addresses vulnerabilities with a CVSS v3 base score of 7 or above
    - There are no details of the level of vulnerabilities that the update fixes provided by the vendor

Please note: For optimum security we strongly recommend (but it's not mandatory) that all released updates are applied within 14 days of release.

Why Is Remediation Still This Slow?

Qualys ROCon 26 The Risk Operations Conference EMEA

Every hour a vulnerability stays open is an hour your adversary doesn't have to work for

01

Too Many Patches

Too many findings to address

02

Trust & Confidence

Will the patch break the app?

03

Patch is Not Enough

What to do if a patch cannot be deployed

04

Validation is Slow

& Rollback Is Hard

Qualys ROCon 26
The Risk Operations Conference
EMEA



The New Pact

Security commits to Noise Reduction.
IT commits to Velocity.

Qualys ROCon 26
The Risk Operations Conference
EMEA

Build Trust

AI Based Patch Reliability.

AI-Powered Patch Reliability Score – Building Trust

Qualys ROCon 26 The Risk Operations Conference EMEA



Predict Patch Reliability Before You Deploy

Internet-wide signals - forums, blogs, official sites etc. combined with rollback data from millions of agents



Reliability Powered Automation

Patch reliability can be embedded in your automations



Strategic Gap Mitigation

Mitigate risk until “risky” assets can be patched

Qualys ROCon 26
The Risk Operations Conference
EMEA

Mitigations

When the Patch is Too Risky DON’T wait Mitigate!

Mitigate Risk Before a Patch can Be Deployed

Qualys ROCon 26
The Risk Operations Conference
EMEA

Mitigate Vulnerabilities When Patching Isn’t Fast Enough

- Deploy mitigations and compensating controls
- Quickly contain zero-day vulnerabilities without waiting for an official patch.
- Risk reduction reflected in VM reports
- Mitigations options mapped to risk

Qualys ROCon 26
The Risk Operations Conference
EMEA

Don’t Hand IT the Problem

Hand them the Solution!

Every Vuln. Every Fix. Zero Guesswork.

Qualys ROCon 26
The Risk Operations Conference
EMEA

Vuln → Patch

Every vulnerability is mapped directly to the right patch. No back-and-forth between Security and IT.

Eliminates manual matching across teams

No patch? Script fix

When vendors lack a patch, remediation script is needed - IT is never left researching an open problem.

Ready-made fix, even without vendor support

AI detects gaps

Patch deployed but vuln still open? No patch when there should be? AI detects the problem and recommends a solution.

Scans Say Vulnerable. IT Says Patched.
AI Finds the Truth.

Validate

& Rollback when needed

Post Patch Health Validation

Qualys ROCon 26 The Risk Operations Conference EMEA



Agent Validates Assets Health

Compare before and after patching to identify issues



Rollbacks Options

In case of a failure, rollback the patch or re-install when needed.

Qualys ROCon 26
The Risk Operations Conference
EMEA

Meet Agent Sara

Your Autonomous Remediation Agent

Agent Sara Doesn't Wait. Neither Should You.

Qualys ROCon 26 The Risk Operations Conference EMEA



Wave-Based Patching Built Around Your Business

Workstations move fast; production servers move in staged cycles with validation gates. When a critical vuln can't wait Agent Sara applies temporary mitigations.



Reliability Score drives every test cycle

Agent Sara routes low-confidence assets into separate testing automatically. Confidence is built before production is ever touched.



Always ready for Patch Tuesday

Agent Sara maps every new vulnerability to its patch and has deployment jobs configured before your team has finished their coffee

Qualys ROCon 26
The Risk Operations Conference
EMEA

TruRisk Eliminate

Helps make the
SecOps – IT bond a reality

Qualys ROCon 26
The Risk Operations Conference
EMEA



150M

Patches Deployed In The Past Year



~40M

Patches Deployed with Zero Touch Automation

(<0.1% rollbacks)



~1M

Mitigations, Fixes, Isolations

TruRisk Eliminate

Qualys ROCon 26 The Risk Operations Conference EMEA

AI Based Recommendation Engine

Map vulns to remediation & mitigation actions

Patch

- Windows
- MacOS
- Linux
- 3rd party apps
- Zero-Touch Patch Automation

Fix

- Remediate vulnerabilities even when no patch exists

Mitigate

- Reduce exposure when patching carries too much operational risk

Custom

- Pre-built scripts for cases that stump both IT and security.
- Create your own for what's unique to your environment

AI Helpers

- AI embedded throughout Eliminate

Isolate

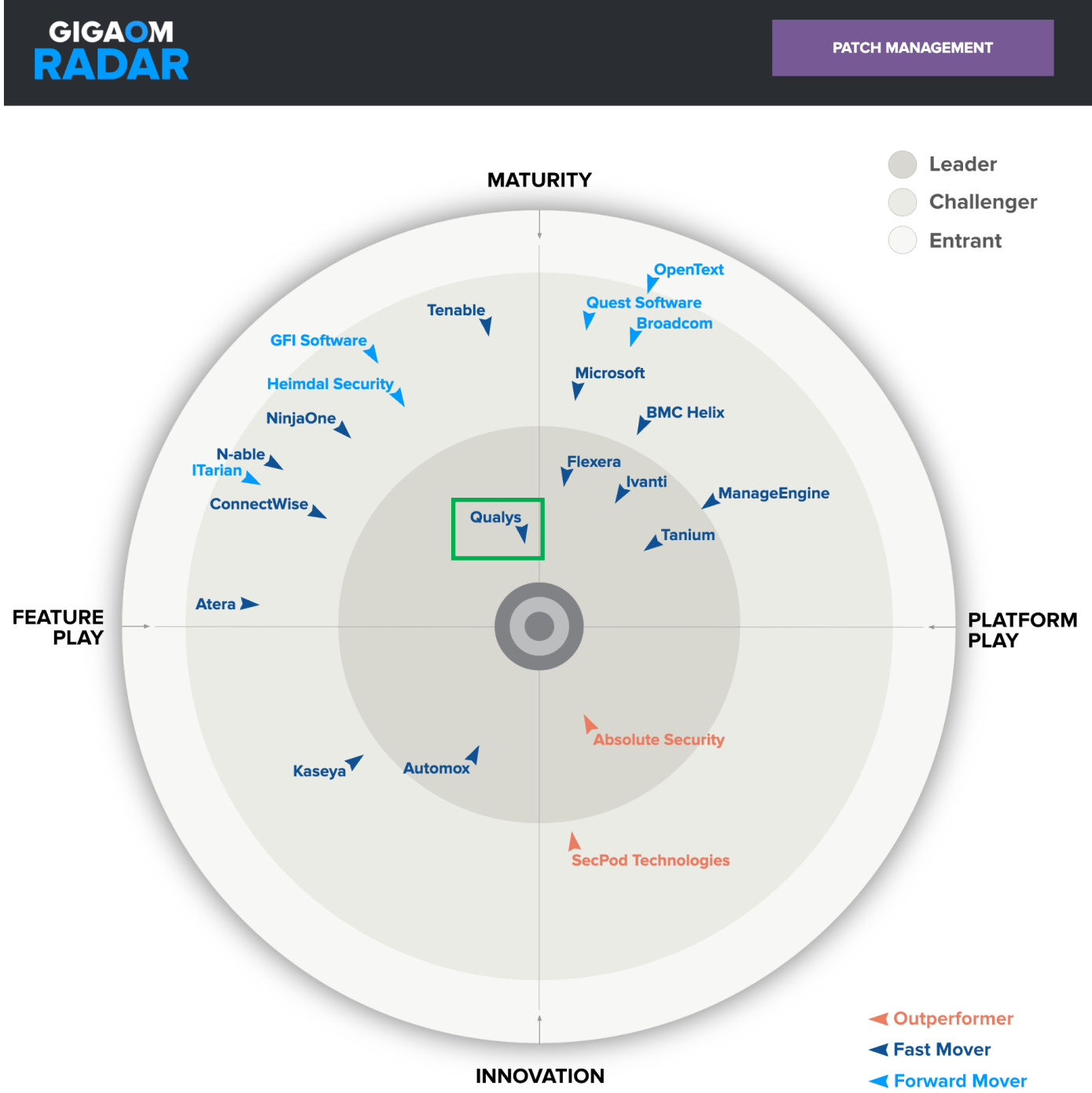
- Last resort containment
- Contain high-risk devices from the network while patching them remotely

Sep 2, 2025

GIGAOM RADAR for Patch Management Solution v4

TruRisk Eliminate

The Leader!



Not Just a Patch

92K

Uninstall: Instances of Zoom removed from user space and securely migrated to admin-controlled environments

27K

Script Fix: WinVerifyTrust vulnerabilities remediated within just **3 days**

40K

Uninstall: NET end-of-life vulnerabilities resolved in **16 days**

10K

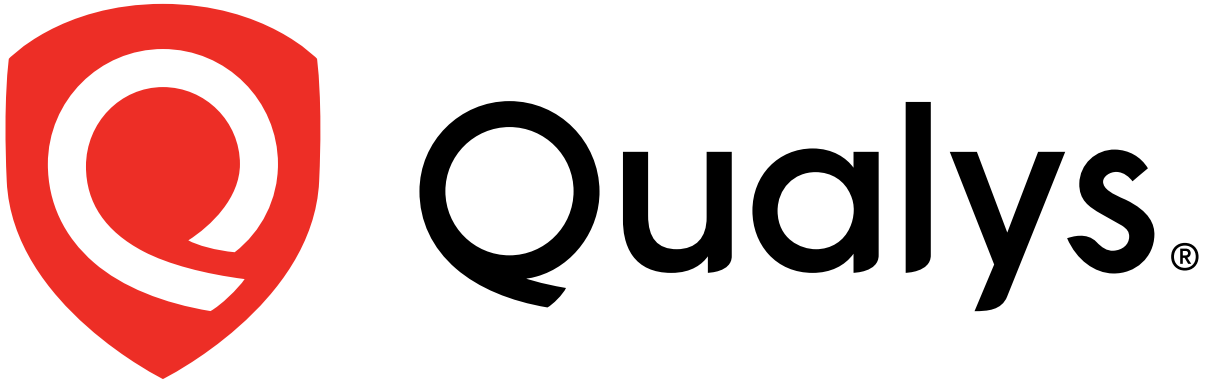
Script Fix : Birthday attack vulnerabilities fixed in **6 days**

Demo

Qualys ROCon 26
The Risk Operations Conference
EMEA

Thank You!




Qualys®

Qualys

ROCon 26

The Risk Operations Conference

EMEA

IT TEAM



Lack Of Collaboration

Misaligned Goals

SECURITY TEAM



Qualys ROCon 26
The Risk Operations Conference
EMEA



The New Pact

Security commits to Noise Reduction.
IT commits to Velocity.

Security Role

Minimize Noise

Send only prioritized and validated vulns	TruRisk, TruConfirm…
Don't hand IT a problem	Hand them the solution: patch/fix/mitigate
Don't add to the queue what's already in it	Anticipate what IT is already planning to patch
Detect when a closed patch leaves the door still open	Surface the mismatch and prescribes the right fix

IT Role

What IT Needs to Reduce MTTR

Automate Smarter, Not Harder	Automated patching that acts on risk, not just schedules
Predict patch reliability before deployment	AI-based reliability score
Flag the systems most likely to break under a new patch	AI predicts which assets won't survive the patch
When the patch is too risky, don't wait — mitigate	Recommend a non-intrusive mitigation

Qualys ROCon 26
The Risk Operations Conference
EMEA

The Strategic Alliance

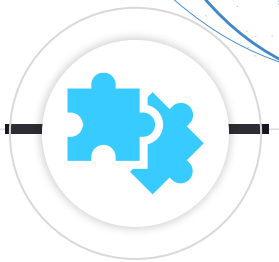
A Mutual Commitment Between IT and Security Teams to Transform Vulnerabilities Remediation



Predict Patch Reliability Before Deploying It



Reliability Based Automation



Strategic Gap Mitigation

Mitigate Risk Before a Patch can Be Deployed

Qualys ROCon 26
The Risk Operations Conference
EMEA

Mitigate Vulnerabilities When Patching Isn’t Fast Enough

- Deploy mitigations and compensating controls
- Quickly contain zero-day vulnerabilities without waiting for an official patch.
- Risk reduction reflected in VM reports
- Mitigations options mapped to risk