

MOVING TO RISK-BASED CYBERSECURITY

The old way of measuring cybersecurity success isn't working.

CIOs and CISOs at enterprises large and small struggle with similar challenges:

The potential attack surface is widened by problems like unregistered public IPs.

"Our teams have limited visibility." "We're swamped by tools & data."

The average enterprise has 16+ security tools. 12% of organizations have 46+ tools

"Manual processes can't keep up."

A lack of cybersecurity automation compounds the IT Security skills gap.

Cyber Risk is Now a Board-level Concern

Cybersecurity risk is now a regular topic in the boardroom. Security leaders should simplify how they discuss cyber risk with executives by defining it in terms of bottom-line business risk.



agendas include the CISO

Average cost of a data breach, 2021

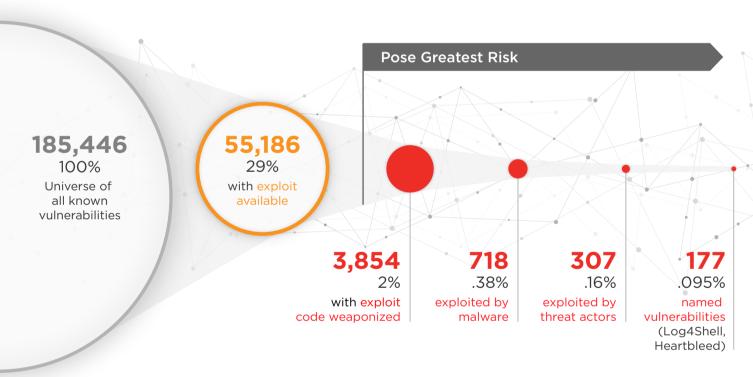


Avg. mentions of cybersecurity in quarterly earnings reports



Don't Count Vulnerabilities, Count Risks!

The old way of counting vulnerabilities to measure cyber risk is ineffective. While the total number of vulnerabilities is soaring, just a small subset pose material risk.



Follow this 3-Step Cyber Risk Process...

Qualys suggests a three-step cyber risk management cycle that continuously monitors the threat landscape, enables quick response, and measures the metrics that company leadership cares about.



Assess Risk

Gain visibility & control over all IT assets in your environment. Understand your organization's total attack surface

- ☑ Inventory all assets for baseline threat assessment
- ☑ Use a security platform that can quantify business risk



Reduce Risk

Consolidate your security stack into a unified platform.

- ☑ Simplify the number of cybersecurity tools used by your teams ✓ Use automation capabilities for risk monitoring, detection,
- and remediation
- Assign actions to reduce risk across Security, IT, and Compliance



Report on Risk

Adopt automated dashboards with clear, risk-defined metrics. ☑ Measure risk against industry standards, peer benchmarks, and

- best practices
- ☑ Report on risk by need: Business metrics for executives: Technical metrics for security practitioners

☑ A comprehensive cybersecurity platform will automatically do both