Executives Believe Their IT Is More Secure Than It Really Is

Tuesday 5 May, 2026

Related Sectors:

Computing & Telecoms ::

Related Keywords:

IT :: Cyber Security :: Study ::

Scan Me:

New study reveals a structural cyber security problem in organisations, with a widening gap between assumed security and proven resilience

Report "The State of Assumed Security 2026" available to download: https://horizon3.ai/downloads/research/the-state-of-assumed-security/

Organisations are investing heavily in cyber security, yet many are still judging success by the wrong measures. That is the central finding of a new global survey from cybersecurity company Horizon3.ai. The report is based on a survey of 750 IT security professionals across Europe and the United States, including both senior security leaders and frontline practitioners. It was commissioned to examine the gap between executive confidence and operational reality.

The findings suggest many organisations continue to treat busy security programmes as evidence of security. Assets are scanned, alerts are generated, patches are deployed and dashboards are updated. Yet these activities do not always confirm whether exploitable weaknesses have been removed or whether defences would withstand real-world attacker behaviour.

The report can be downloaded free of charge here:
https://horizon3.ai/downloads/research/the-state-of-assumed-security/

High Confidence at Leadership Level, Limited Validation in Practice

Confidence in existing controls is high among senior decision-makers. According to the survey, 93% of CISOs say they could demonstrate that their organisation had taken reasonable, validated steps to prevent a breach. Meanwhile, 97% are confident their endpoint protection would detect lateral movement or privilege escalation, while 96% believe their Security Operations Centre (SOC) could identify an attacker operating inside the environment.

However, day-to-day operational practice tells a different story. Only 30% of CISOs say their organisations patch vulnerabilities and then test to confirm that risk has been properly remediated. Nearly half patch systems and simply rerun a vulnerability scanner instead. Just 12% report validating the effectiveness of their Endpoint Detection and Response (EDR) tools within the past three months, while only 26% use red team exercises or penetration testing to assess the detection capability of their SOC. Among frontline practitioners, one third assume scanner findings are accurate without further testing, while 17% do not validate findings at all.

"Security teams don't struggle to find problems. They struggle to prove those problems are actually gone. Most workflows end at patch and rescan, but attackers don't operate in isolation. They chain weaknesses into real attack paths. If you're not validating those paths in your environment, you're not measuring risk," said Dan Bird, Field CTO EMEA, Horizon3.ai.

Delays in Addressing Actively Exploited Vulnerabilities

A similar delay is evident when it comes to known vulnerabilities that are already being actively exploited. Only 11% of respondents say they validate or patch systems within 24 hours of an alert from CISA (Cybersecurity and Infrastructure Security Agency) or ENISA (European Union Agency for Cybersecurity). Many require a week or longer simply to determine if they are exposed.

According to the Horizon3.ai report, the pattern is clear: many security programmes are built around workflow completion — scan, patch, rescan, close. Detection tools are deployed and monitored, and automation helps accelerate speed. What is too often missing, however, is clear validation that these measures are genuinely reducing risk or would stop a real attack.

High Confidence, Limited Verification

One of the most striking findings in the survey is the disconnect between perception and reality. Senior leaders are largely confident in the effectiveness of their security controls. On the operational front line, however, many practitioners continue to see significant levels of risk. This difference in perspective has

tangible consequences. It shapes decisions around budgets, priorities and response times, and can often result in genuine threats being underestimated.

Patching Does Not Equal Security

The report identifies vulnerability management as a core issue. In many organisations, a problem is considered solved once a patch has been applied and a ticket has been closed. Far less common is the follow-up step of confirming whether the underlying weakness can still be exploited. The result is a false sense of security: processes are completed correctly on paper, while potential attack paths may still remain open.

Detection Systems Rarely Tested Under Real-World Conditions

The survey found a similar pattern when it comes to threat detection. Modern security tools are widely deployed and continuously monitored. Yet many organisations still lack systematic testing under realistic conditions. Without targeted exercises, it remains unclear whether attacks would be detected and stopped in time – or only become visible once damage has already been done.

AI Speeds Up Processes, but Does Not Replace Validation

The use of artificial intelligence in cyber security is increasing rapidly. Automated systems are helping organisations prioritise vulnerabilities more quickly, process tickets more efficiently and implement actions at greater speed. However, the report highlights the same underlying issue: speed is not the same as effectiveness. Without independent validation, there is no clear evidence that automated decisions are genuinely reducing risk.

Metrics Measure Pace, Not Impact

Many IT organisations continue to rely on traditional performance indicators such as response times or the number of closed tickets. These figures may show how quickly work is being completed, but not whether an attack could actually be prevented. The more meaningful measure of success – real resilience against attackers – is far less frequently assessed.

A New Priority: Proof Over Assumption

Horizon3.ai says the study points to a wider shift in cybersecurity priorities. In the future, success will be defined less by how many controls or actions are implemented, and more by whether those measures can be shown to work in practice. Organisations now face the challenge of aligning security strategies more closely with realistic attack scenarios and regularly testing whether their systems can withstand them.

As the report concludes: The findings do not point to a lack of effort. Security programs are active, instrumented, and increasingly automated. The gap lies in confirmation. Security maturity depends on how clearly organisations can demonstrate that their actions reduce real exposure. Moving from assumed security to demonstrated resilience requires deliberate shifts in behaviour.

About the survey

Survey data for this report was collected by Censuswide, an independent research firm, from

750 cybersecurity leaders and practitioners across the United States and Europe.

About Horizon3.ai: Horizon3.ai, the AI-native proactive security company, has redefined how organisations validate and strengthen their defences. It is the company behind NodeZero®, the world's most experienced AI hacker, used by 4 of the Fortune 10, global banks, top global pharmaceutical and semiconductor manufacturers, and critical infrastructure operators.

NodeZero enables organisations to proactively hack, fix, verify, and repeat testing on demand across their environment, resulting in stronger defences and measurable improvements in cyber resilience over time. Founded by former U.S. Special Operations members and industry experts, Horizon3.ai is trusted by more than 5,200 customers who have executed over 225,000 production-safe pentests.

Recognised as one of the world's most innovative and fastest-growing cybersecurity companies, Horizon3.ai has been honored by Fast Company, Deloitte, Inc., Fortune, and the Black Unicorn Awards. Founded by former U.S. Special Operations members and industry experts, the company is headquartered in San Francisco.

Further information: Press contact: Stephen Gates - press@horizon3.ai, Web: www.horizon3.ai

PR Agency: euromarcom public relations GmbH, Web: www.euromarcom.de, Email: team@euromarcom.com

Company Contact:

_

news aktuell

E. desk@newsaktuell.de
W. https://www.newsaktuell.de/

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.newsaktuell.pressat.co.uk