Trend Research

TREND MICRO

Key Takeaways for CISOs

The Role of Exposure Management and Detection-Response Capability in Proactive Security

Contents

Published by
Trend Research

Most security programs are built to respond, but fewer are designed to avoid the need. As attacks escalate in speed and complexity, the organizations that withstand them best aren't always the ones with faster alerts, but those with fewer openings to begin with.

Our study shows that risk exposure — and not just response capability — is the strongest predictor of whether an incident leads to real damage. When exposure is well-managed, capabilities like managed detection and response (MDR) become significantly more effective.

This primer unpacks what the data tells us, where the risk lies, and what proactive security looks like when exposure, detection, and response are treated as a unified, holistic ecosystem of cybersecurity capabilities. If your organization hasn't experienced a major incident yet, that period of calm is your window to build resilience, strengthen culture, and invest in proactive security capabilities before the next attempt arrives.

Key numbers behind cyber resilience

Trend Micro analyzed telemetry from mid-sized to large enterprises across multiple regions and industries. The results drew a clear line between exposure levels, MDR usage, and actual cyber damage:

- Organizations with high exposure were 2.6 times more likely to experience damaging incidents.
- MDR alone reduced incident rates (33% vs. 42%), but didn't achieve statistical significance.
- The lowest damage rate (13%) was found in organizations combining MDR with low exposure.
- Organizations without MDR and with high exposure saw damage rates as high as 54%.

Our analysis showed that exposure determines how quickly an attacker can progress. MDR gauges how quickly enterprises can respond, but the best outcomes happen when both are optimized together. The outcomes consistently showed that reducing exposure has the greatest influence on security outcomes and raises the effectiveness of investments in MDR and security operations center (SOC).

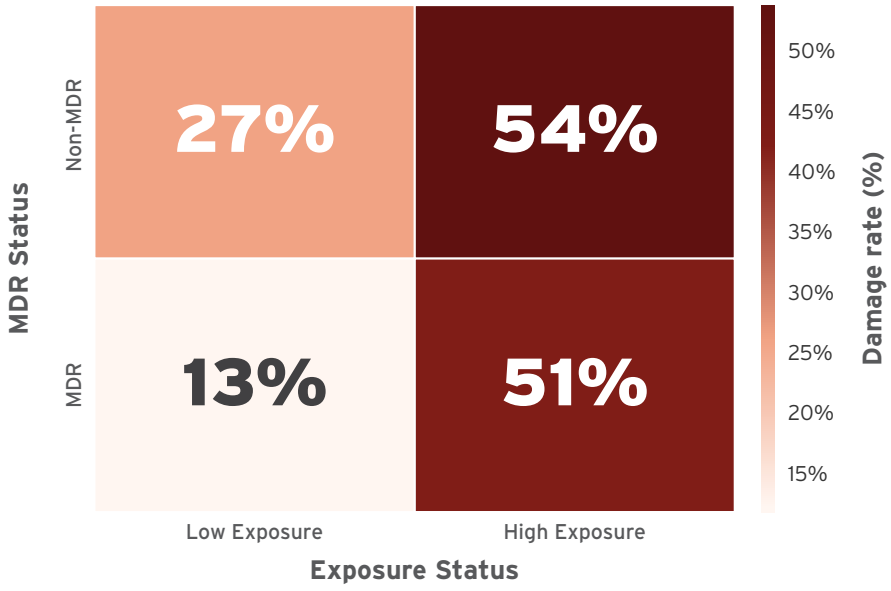

Figure 1. Damage rate by MDR and exposure status

What the data says about the cost of exposure

To understand what drives real-world damage, Trend Micro analyzed telemetry from 190 organizations that used both extended detection response (XDR) capabilities and cyber risk exposure management tools throughout 2024. Each organization met certain criteria, such as consistent use of endpoint, email, and network telemetry, employee size between 500 and 10,000, and continuous deployment of key security controls. This created a balanced dataset for comparing outcomes.

Two factors were also measured:

- **Risk exposure via the Exposure Index:** A composite score built on vulnerabilities, configurations, and external-facing assets
- **Detection and response posture:** Determined by whether the organization used MDR

Damage was not estimated but observed. Using detections mapped to the MITRE ATT&CK framework, organizations were considered "damaged" if they experienced exfiltration (TA0010) or impact on systems and operations (TA0040). Statistical analysis confirmed that the differences between groups were not random. Risk ratios, confidence intervals, and absolute risk reduction were applied to identify which combinations of exposure and response translated into lower risk.

The analysis was a view into how real-world conditions across industries, regions, and maturity levels influenced outcomes. The result is a data-backed model that shows CISOs where to focus their efforts and investments to reduce impact.

Turning exposure into a modifiable control point

Based on the data, organizations that kept their exposure low were significantly less likely to suffer damage regardless of how advanced their detection capabilities were. This reinforces what many security teams already assume: Attackers don't need to be sophisticated if the environment is easy to exploit.

There's also a clear correlation that MDR works best when paired with exposure management. While MDR provided moderate benefits in high-exposure environments, the impact was limited. In contrast, organizations that combined MDR with low exposure saw the steepest reduction in damage.

The implication is strategic: MDR amplifies response capability, but it depends on time. In high-exposure conditions, attacks move faster, and the impact might already be underway by the time detection tools trigger. Exposure management changes this dynamic by reducing the number of paths an attacker can take, slowing down lateral movement, and giving the enterprise's SOC and cybersecurity team more space to respond before the damage is done.

This is where CISOs gain leverage. When reduced intentionally, it creates upstream advantages across the security stack and gives response investments like MDR a clearer return.

Even in low-exposure environments, zero risk is unrealistic. Threats like zero-days, insider threats, abuse of tools, and targeted attacks still require fast, coordinated response. This is where MDR still plays a critical role in limiting damage.

Where and how CISOs can act today

The findings provide a practical framework for reducing exposure, improving incident readiness, and aligning security investments with measurable risk reduction. Below are four areas where CISOs can take immediate action:

Control the surface. The most reliable way to reduce damage is to reduce exposure. Start with visibility. Tools and capabilities, such as Cyber Risk Exposure Management (CREM), offer a structured view of the organization's risk posture, highlighting misconfigurations, unpatched systems, and unnecessarily exposed assets. Move from periodic assessments to continuous measurement. Use exposure scores to track progress and prioritize remediation based on business impact and not just on technical severity.

Prepare for containment, not just detection. MDR is most effective when it has time to act. That time comes from reducing attacker speed, but it also depends on clearly defined incident response flows. CREM plays a key role here by providing visibility into gaps and misconfigurations that, in turn, helps security teams prepare proactively and thus improve response time and accuracy. Additionally, ensure that detection rules reflect the threats most relevant to your environment. Develop playbooks with business unit input. Practice escalation through executive tabletop exercises. The goal is not just a faster alert, but a faster decision.

Build internal alignment around risk. Exposure management cuts across infrastructure, applications, identity, and operations. Successful programs build coordination between teams and use risk scores to support executive conversations. For example, the Exposure Index provides a language the board can understand. Treat it as a metric that aligns security goals with business risk. When CISOs can show improvements in exposure scores tied to fewer incidents, security becomes a strategic function.

Bring in the right external support. Not every organization has the capacity to build these capabilities internally. That's where services like Cyber Risk Advisory Services (CRAS) and managed XDR can help. They can assess the environment, prioritize exposure reduction, and translate technical gaps into executive-level strategy. Combining internal action with outside perspective helps accelerate maturity, especially in environments where attack surfaces are large or legacy complexity is a limiting factor.

When viewed together, these steps form the foundation of a proactive security posture that doesn't just strive to respond better, but also aim to be targeted less often and be affected less severely when it occurs. Indeed, a proactive security posture is not just a set of tools or technologies, but a mindset. Embedding readiness across teams, processes, and leadership is what allows organizations to act swiftly when the unpredictable happens.

Read the full research to learn more.