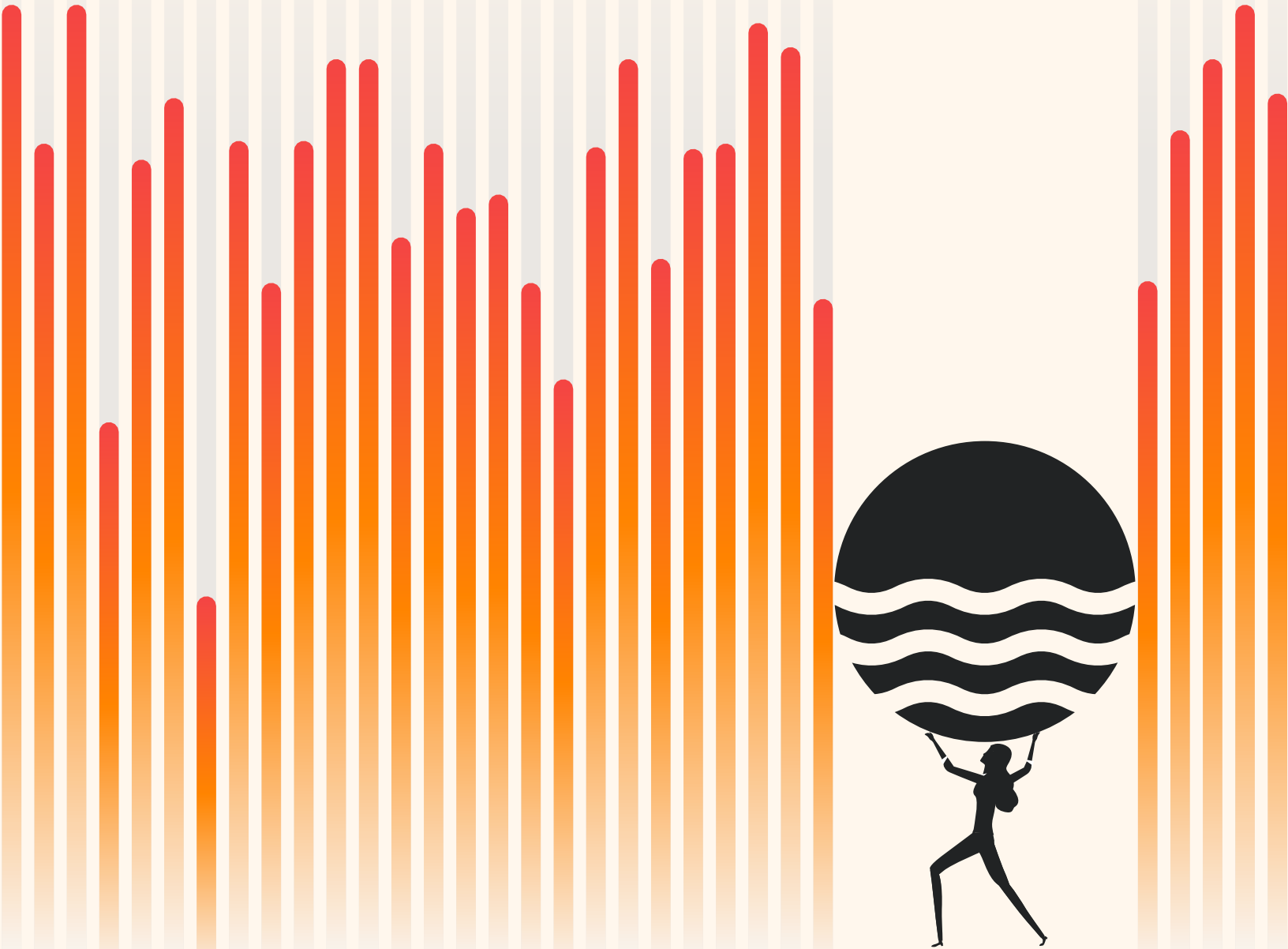
Survey Report

halcyon

2026 SECURITY LEADERSHIP SURVEY RESULTS

The Ransomware Gap in the AI Era



Executive Summary

Security leaders are experienced and ready. Their tools are not. This survey of 100 CISOs and senior security executives reveals a dangerous disconnect between leader confidence and tool effectiveness in the age of AI-powered ransomware.

Key Findings

- **The Confidence Paradox**: 99% of security leaders are confident in their ability to detect attacks. Among organizations that experienced an attack, 49% of victims admit they detected their last attack too late to prevent significant damage.
- **The EDR Trust Collapse**: 98% of organizations use EDR for ransomware defense, but only 25% actually trust it to defend against today's evolving ransomware threats.
- **The AI Asymmetry**: 78% of leaders say AI has made ransomware attacks more effective, while only 6% believe AI has improved their own defenses.
- **The 'Mostly Sufficient' Trap**: 90% of leaders rate their current security solutions as 'sufficient' or 'mostly sufficient', yet almost half of them (49%) experienced moderate to significant disruption from successful ransomware attacks.

Survey Methodology

Halcyon commissioned this research using an online survey prepared by Method Research and distributed by Rep Data. The survey was distributed to 100 Chief Information Security Officers, Heads of Security Operations, SVPs/ VPs of Information Security or Cybersecurity, and other security leadership roles in the United States from January 5 to February 12, 2026.

Respondent Profile	
Role	50% CISOs / 50% CIOs, SVPs
Experience	72% have 6+ years as Head of Security
Tenure	87% have been in current role 3+ years
Company	56%: 500-2,499 employees 44%: 2,500+

THE CONFIDENCE PARADOX

Confident to Detect Attack	Fell Victim to Attack
99%	49%

THE EDR TRUST COLLAPSE

Use EDR Defense	Trust EDR to Defend
98%	25%

THE AI ASYMMETRY

AI Helps Attackers	AI Helps Defenders
78%	6%

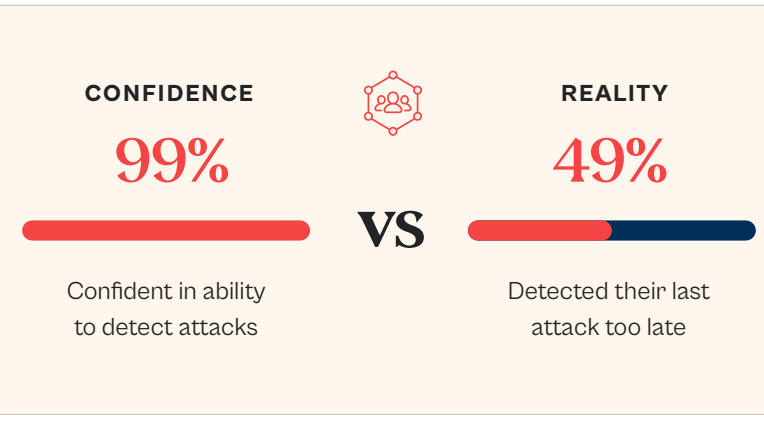
THE 'MOSTLY SUFFICIENT' TRAP

Rate Security Sufficient	Experience Disruption
90%	49%

THE CONFIDENCE GAP

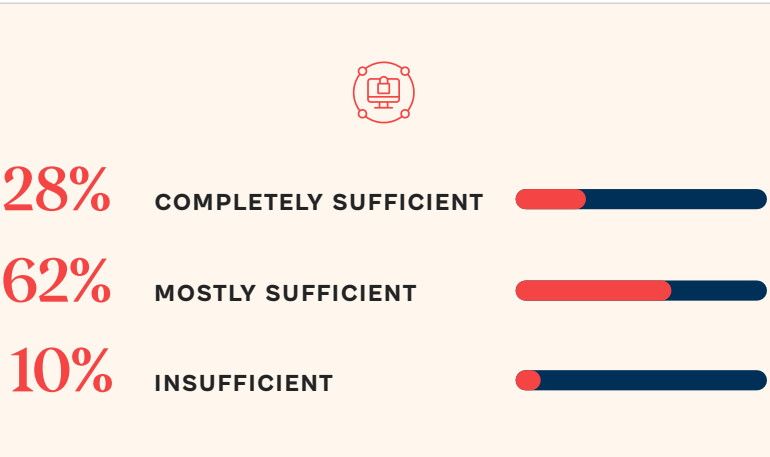
When ‘Mostly Sufficient’ Is Not Good Enough

On the surface, security leaders project high confidence in their ransomware detection and protection capabilities. Nearly all report robust detection (99%) and sufficient prevention tools (94%). Yet this confidence collides with the reality of successful attacks.



The ‘Mostly Sufficient’ Problem

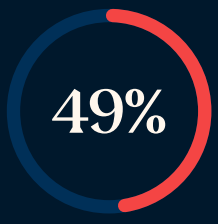
The gap between confidence and reality illustrated above explains why only 28% rate their current security solutions as ‘completely sufficient,’ while 62% rate them as ‘mostly sufficient.’ These are highly experienced leaders. Their confidence stems from expertise, not blind faith in their tools.



When Attacks Succeed, Businesses Suffer

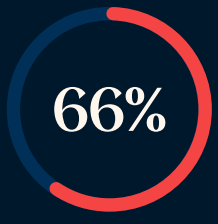
The consequences of ‘mostly sufficient’ tools against ransomware are measurable and significant

experienced some impact on business operations due to ransomware



reported moderate to significant disruption

rank business downtime among their top three concerns



cite data loss or corruption as a top three concern

halcyon

AI as the Threat Multiplier

Security leaders view Artificial Intelligence (AI) as an enabler and threat multiplier for ransomware attacks, not a tool to prevent them. This creates a dangerous asymmetry where attackers benefit far more from AI than defenders.

AI HELPS ATTACKERS

78%

Say AI makes ransomware attacks more effective

AI HELPS DEFENDERS

6%

Believe AI has improved their own defenses

This 13:1 advantage creates a significant vulnerability gap, with 74% of leaders saying their organizations are now more exposed due to AI advancements.

The EDR Trust Collapse

The survey revealed a troubling infrastructure gap: experienced security leaders are forced to fight modern, AI-powered threats using tools that weren't designed for them.

98%

Currently use EDR for ransomware defense

25%

Actually trust their EDR to defend against modern ransomware attacks

This 73-percentage-point trust gap reveals that while EDR remains ubiquitous, it's no longer sufficient for the AI-powered ransomware threat landscape. Leaders know their tools weren't built for today's attacks, yet they're often stuck using them anyway.

AI-Powered Threats Keep Leaders Up at Night

When asked about their biggest anticipated challenges over the next 12-18 months, security leaders cited AI-powered attacks as a primary concern.

AI-POWERED PHISHING

"Realistic emails are easily generated and are very hard to detect and differentiate."
– CISO respondent

CUSTOMER-TARGETED SCAMS

"The growing use of AI in customer-targeted scams is my biggest concern."
– CISO respondent

INTERNAL RISKS

Leaking information into external AI tools.

Ransomware is No Longer Just a CISO Priority

Ransomware has secured its place as the first cybersecurity problem to become a business-wide concern. Unique among cyberattacks, ransomware's impact is not theoretical; it is immediately quantifiable. The overwhelming operational and financial disruption it causes has elevated it to a boardroom priority, with executive leadership directly influencing anti-ransomware investments and demanding answers about preparedness.

CISO Ransomware Concerns

97% Asked by board/execs about their defense strategy

64% Rank it within their top 3 business priorities

35% Rank ransomware as their #1 business priority

What Are Boards Actually Asking?

The conversations reveal specific board concerns:

69% Asked about disaster preparedness plans for ransomware

63% Asked about incident response plans for ransomware attacks

56% Asked about ransomware recovery time objectives

Board Scrutiny Drives Investment Decisions

This executive attention directly influences purchasing behavior.

74%

say board inquiries are significantly influencing anti-ransomware investments

82%

say executive leadership directives significantly influence purchasing decisions

91%

admit recent high-stakes ransomware incidents moderately or significantly influence their buying decisions

Conclusions

This survey reveals three critical gaps that security leaders must address:

1. THE EXPERIENCE-EFFICACY GAP

Teams Are Ready, Their Tools Aren't.

The lack of confidence doesn't stem from inexperience. These are highly seasoned leaders averaging 6+ years as Heads of Security. The gap is driven by a harder truth: the tools they are forced to use were not built for today's evolving ransomware threats.

The EDR Trust Collapse: While 98% of organizations use EDR for ransomware defense, only 25% trust it to defend against today's evolving ransomware threats. This 73-percentage-point trust gap reveals that experienced leaders know their tools weren't purpose-built for ransomware.

2 . THE PREPARATION-REALITY GAP

Confidence Doesn't Prevent Damage.

There's a dangerous disconnect between how prepared leaders feel before an attack and what happens when an attack occurs. Despite universal confidence in their detection capabilities, reality tells a different story.

The Confidence Paradox: 99% of security leaders are confident in their ability to detect attacks, yet 49% of victims admit they detected their last attack too late to prevent significant damage.

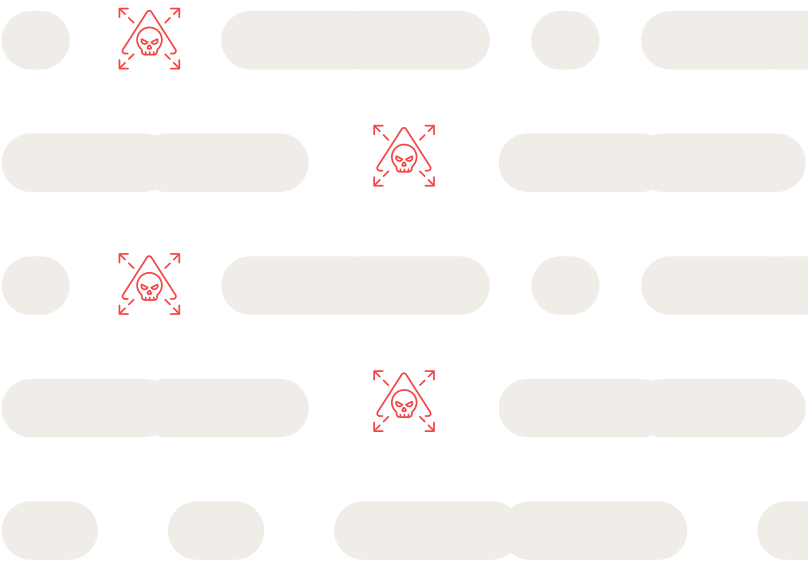
The 'Mostly Sufficient' Trap: 90% of leaders rate their current security solutions as 'sufficient' or 'mostly sufficient,' yet nearly half of them (49%) experienced moderate to significant disruption from successful ransomware attacks. When "mostly sufficient" tools lead to "moderately disruptive" (or worse) outcomes, the gap between preparation and reality becomes painfully clear.

3. THE AI ASYMMETRY GAP

Attackers Are Winning the AI Arms Race.

Security leaders recognize the playing field has fundamentally shifted, creating a dangerous imbalance in how AI impacts attackers versus defenders.

The AI Asymmetry: 78% of leaders say AI has made ransomware attacks more effective, while only 6% believe AI has improved their own defenses. This means attackers have the upper hand in leveraging AI for convincing phishing, reconnaissance, and evasion techniques while organizations struggle to operationalize AI defensively. This asymmetry is evidence that generalist security tools built for yesterday's threats are no longer sufficient for today's AI-powered ransomware landscape.



The Path Forward

The message is clear: Ransomware isn't just another threat. It's a different category of attack. Experienced security leaders need tools that match their readiness. 'Mostly sufficient' security is no longer sufficient when facing AI-powered ransomware. With 91% already exploring ransomware-specific tools following high-stakes incidents and boards demanding answers, the shift from general-purpose security to purpose-built ransomware defense is no longer optional; it's imperative.

halcyon