TechnologyAdvice

July 2025

INDUSTRY TREND REPORT

Building Cyber Resilience:

Aligning Business, Threat Intel, and SecOps

SPONSORED BY

ThreatConnect.
now a part of Dataminr.

TABLE OF CONTENTS

The Exponential Evolution of Threats and Attackers

The security industry has long confronted the asymmetric battle between attackers and defenders. A threat actor needs only to be successful once, while cybersecurity teams, threat hunters, and analysts need to be successful against every attack, every time.

This disparate dynamic is exacerbated by the exponential growth of attack surfaces. In 2023, **63% of SOC analysts** said that the size of their organization's attack surface has significantly increased over the past 3 years. Emerging threats now have to contend with attacks from the cloud, remote work, IoT, and most recently, AI.

This wider attack surface also coincides with increased complexity, as attacks are now stealthier and better equipped to break down traditional defenses. In 2024 alone, we saw a **180% surge** in the exploitation of vulnerabilities as the primary method of initiating a breach and a **68% increase** in incidents involving supply chain attacks. This has enabled threat actors to ramp up extortion and ransomware-based attacks, exposing businesses to both financial and operational damage.

As we approach a tipping point where threat risk will grow exponentially, defenders are left relying on linear resources and tools. In the next section, we explore how this mismatch creates operational challenges and how it affects not only an organization's security posture but also its business and financial impacts.

Challenges Faced by Security Teams Amid a Shifting Threat

This growing, exponential threat risk isn't just a problem for cyberdefense—it has real, material impact on the business. According to IBM, the global average cost of a cyber attack in 2024 was $4.88 million, a 10% increase from previous years and the highest average on record.

Despite the financial consequences, a disconnect persists: cybersecurity and business teams are misaligned. Most organizations still operate without clear alignment between threat intelligence and financial or business risk.

USD 4.9M

Source: IBM

The global average cost of a data breach in 2024: a 10% increase over last year and the highest total ever.

Imagine this scenario:

A lone security analyst, overwhelmed by thousands of alerts, misses a critical high-level threat due to fatigue and burnout. That overlooked threat leads to a breach—one that the CISO now has to deal with and one that impacts the company's bottom line, whether through PR, legal, service downtime, or other issues. Ironically, the CISO was willing to invest in additional resources but lacked the necessary insight into the financial impact of each risk. Without that context, the urgency of the threat wasn't made clear until it was too late.

In essence, security practitioners at large lack the business context needed to know which threats matter most, while business leaders lack relevant insights to allocate resources effectively. The result is a struggle to contextualize, prioritize, and operationalize threats that address the asymmetric growth of attacks and the linear defenses of traditional security teams.

To illustrate the misalignment, here's a breakdown of how roles across a security team experience the same disconnect in distinct ways:

Defender	Challenge Faced
CISOs and Cyber Defense Leaders	• Resource allocation crisis: Difficulty identifying which parts of the security posture demand focus • Insufficient intelligence resources and security insights to help justify budget and spending decisions • Soaring cyber insurance costs that amplify demand for risk-informed decision-making
Cyber Threat Intelligence (CTI) Teams	• Struggle to demonstrate ROI in business terms, with only **36% of teams** measuring CTI program effectiveness • Sidelined from strategic decision-making, as **79% of organizations** say they make decisions without adversary insights
Security Teams	• Alert Overload: **43% of teams** say more than 40% of their alerts are false positives • Linear workflows and brittle prioritization models • Severe burnout and operational fatigue
SOC Analysts	• Analyst Fatigue: **71% of analysts** say they've experienced burnout due to understaffing, increased workload • **55% of teams** say they missed alerts due to ineffective prioritization
Threat Hunters	• Lack of enriched intelligence, hindering understanding of how attack methods map to adversary behavior and business risk • Excessive time spent extracting data instead of hunting threats

As shown, clear overlaps exist between an organization's security efforts and its broader business goals. Inevitably, analyst resources are tied to security budgets, while executive decision-making must rely on insights and data from people on the ground.

With this, it's evident that there must be a strong connection between threat intel, risk management, and operations for all defenders to be set up for success. When this alignment is missing, teams are left operating in silos, leaving them unable to act on the most pressing threats. To close this gap, organizations must shift their approach by aligning their threat intelligence with financial risk to ensure resources are focused where they'll have the greatest impact.

Fortunately, ThreatConnect's risk-informed cyber defense system is purpose-built to solve this problem and more.

How ThreatConnect Helps Bridge the Gap Between Threat Defense and Risk Management

ThreatConnect helps organizations address the misalignment of cyber defense and business teams amid the exponential growth of threats. By offering threat intelligence management, cyber risk quantification, and innovative investigation in a single platform, ThreatConnect allows organizations to contextualize, prioritize, and operationalize their threat response with ease. ThreatConnect delivers value in three specific ways:

Actionable Context

ThreatConnect solves the absence of context by integrating it into every layer —from ATT&CK-based threat modeling to contextual federated search, AI-curated intel requirements, and real-time global feedback loops. Whether it's an analyst triaging an alert or a CISO prioritizing investments, it surfaces the right intel, with the right context, at the right moment.

Risk-based Prioritization

With the overwhelming volume of alerts security teams face daily, ThreatConnect's risk-based prioritization cuts through the noise by quantifying threats by business impact. This empowers analysts to focus on the threats that matter the most—reducing alert fatigue, demonstrating ROI, and helping them feel more fulfilled and valued. It also makes it easier to secure budget, buy-in, and resources.

Accelerated Operationalization

ThreatConnect's automation and workflow capabilities streamline cyber team operations, enabling faster mean-time-to-respond (MTTR) and boosting analyst efficiency. The platform also ensures intelligence is quickly disseminated to all relevant teams at the moment of decision and action, then takes automated response and mitigation measures without interrupting their workflow, keeping the entire organization informed and ready to act on emerging threats.

The combination of the three elements helps organizations build cyber resilience in the face of more advanced cyberattacks and attack vectors.

How Organizations Have Used ThreatConnect To Build Cyber Resilience Amid Exponential Threats

Here's how organizations and businesses across sectors have used ThreatConnect to operationalize business-aligned cyber defense and build long-lasting security resilience.

Medical Insurance Provider Quantifies Risks

Challenge	A CISO needed assistance in measuring and assessing the financial impact of cyber risks, especially during discussions with board members on properly allocating resources. They also needed a way to assess the most significant financial risk of each business unit in their portfolio.
Solution	With ThreatConnect's Risk Quantifier, the organization was able to assess risk portfolios across each member company, enabling the CISO to allocate and prioritize resources effectively.
Outcome	This allowed the CISO to justify security investments, identify and track critical assets, and prioritize vulnerabilities, according to financial impact.

Enterprise in Need of Central Threat Intelligence

Challenge	A large technology company wanted a centralized repository of its threat intelligence to unify contextualized data, improve collaboration, and enable prioritization.
Solution	Using ThreatConnect, the enterprise was able to automate the aggregation of internal and external threat intelligence data. This freed its analysts to focus on higher-level tasks and incident response.
Outcome	ThreatConnect's custom dashboards provided the company with improved awareness of its threat intelligence operations, as well as concrete metrics and data on its security posture. It also allowed them to visualize trends and better understand the impact of both their security measures and the threats they faced.

Manufacturing Company Unaware of Cyber Risk	
Challenge	This client was unknowingly letting in a high level of cyber risk as it was deploying digital services and applications.
Solution	ThreatConnect generated a clear financial view of inherent, residual, and acceptable levels of risk—showing their business leaders the financial impact of improving their security controls
Outcome	ThreatConnect delivered data for over 250 applications and 30 legal entities, with financial cyber risk now becoming a critical talking point during C-suite and board-level conversations.

Build Cyber Resilience Today With ThreatConnect

Trusted by nearly 300 enterprises and government organizations and tens of thousands of security professionals worldwide, ThreatConnect unlocks the full potential of your organization's security operations, helping it become resilient to any threat that comes your way.

As threat actors evolve and attack surfaces expand, organizations must align their security efforts with financial risk in order to stay ahead.

Start building cyber resilience with ThreatConnect today.

ThreatConnect. now a part of Dataminr.

ThreatConnect.
now a part of Dataminr

SECURITY TEAMS AREN'T FAILING. THEY'RE BEING SET UP TO FAIL.

Analysts are burning out. CISOs can't get the right data to justify spend. And attackers? They're evolving faster than most defenders can keep up.

- 55% of teams have missed critical alerts due to ineffective prioritization
  - 84% of analysts say alert volume is affecting their personal lives
- Only 28% of CTI programs inform budget or resourcing decisions
- Meanwhile, attackers are exploiting vulnerabilities 180% more often year over year

You're not lacking data. You're lacking context. You're not short on tools. You're short on alignment. And you're not alone.

Trusted by 250+ enterprises. Proven to cut MTTR by 50% or more.

"We went from 7 hours to 37 minutes. ThreatConnect let us show real ROI and make better decisions."

— Director of IR, Forbes 2000 Healthcare System

ThreatConnect was built for this moment.

We unify threat intelligence, risk quantification, and operational response in one platform —so your teams can:

- Contextualize threats in real time, mapped to business impact
- Prioritize by financial risk, not gut feel or CVSS scores
- Act with automation that overlays directly into your daily workflows—no integration required

Whether you're a SOC analyst drowning in false positives or a CISO trying to explain risk to the board, ThreatConnect connects the dots—between data, risk, and action.

Security is hard enough. Your tools shouldn't make it harder.

See how modern teams are building cyber resilience

Request a Demo

Studio A
by TechnologyAdvice

Custom Content Created by StudioA

Research-driven content that delivers actionable insights
and empowers business decisions.

TechnologyAdvice

SPONSORED BY

ThreatConnect.
now a part of Dataminr.