EXTRAHOP

2025

Global Threat Landscape Report

Table of Contents

The Evolving Threat Landscape

When Threats Become Systemic Risks

The cybersecurity landscape has undergone a dramatic transformation over the past year, as a series of monumental incidents exposed the profound and far-reaching consequences of modern cyberattacks.

Consider the ransomware attack against Change Healthcare that paralyzed a portion of the U.S. healthcare infrastructure. Attackers leveraging compromised credentials exfiltrated sensitive data belonging to an estimated 192.7 million individuals, making it the largest healthcare data breach on record. Beyond the data theft, the incident crippled essential payment processing, pharmacy services, and medical claims, forcing many healthcare providers to operate manually for months.

Similarly, the CDK Global attack orchestrated by the BlackSuit ransomware group delivered a powerful blow to the automotive industry, bringing thousands of North American car dealerships to a standstill for weeks and resulting in over a billion dollars in estimated losses. The attackers even launched a second attack during recovery efforts, exacerbating the disruption.

And the infamous Ticketmaster/Live Nation breach exposed the personal and financial information of 560 million customers, and was reportedly the result of a broader security incident involving the cloud data platform, Snowflake.

These high-profile events serve as a stark reminder of an ever-expanding attack surface, fueled by pervasive digitalization, complex interconnected systems, and increasingly sophisticated threat actors wielding a formidable arsenal of tactics.

Against this critical backdrop, ExtraHop embarked on a global initiative, surveying security and IT decision-makers across a range of industries to gain a deeper, more nuanced understanding of the current threat landscape.

The ExtraHop Global Threat Landscape Report delves into the specifics of their expanding attack surface, identifies the adversaries targeting them and their preferred attack methods, assesses their perceived level of risk, and, crucially, evaluates their organizational readiness and efficacy in defending against these threats when disaster inevitably strikes.

Key Findings

ATTACK SURFACES
REPRESENTING THE
MOST SIGNIFICANT
CYBERSECURITY RISK

Public cloud
(AWS, Google, Azure, etc.)

Third-party services and integrations

Gen AI applications

MOST COMMON
INITIAL **POINT OF ENTRY**
FOR ATTACKERS

Phishing

MOST DETECTED
THREAT ACTORS

RansomHub

LockBit

DarkSide

RANSOMWARE'S
PRICE HIKE

5-6 **Average number of ransomware incidents**
per organization in the last year

70% **Paid** the ransom

$3.6 MILLION Average **ransomware payout**

TIME IS MONEY

2 WEEKS
How long organizations estimate
ransomware actors had access to their systems,
on average

2 WEEKS
The average length of time it took
organizations to respond to & contain a security alert
from initial detection to resolution

37 HOURS
Average downtime
per cybersecurity incident

The Expanding Attack Surface

As organizations rapidly adopt emerging technologies, navigate complex device interdependencies, and manage sprawling supply chains, their IT infrastructures become inherently more complex. This escalating complexity inevitably leads to a larger attack surface.

When asked which element of this attack surface represents the most significant cybersecurity risk, respondents indicated that the threats are ubiquitous. However, several critical areas consistently stood out.

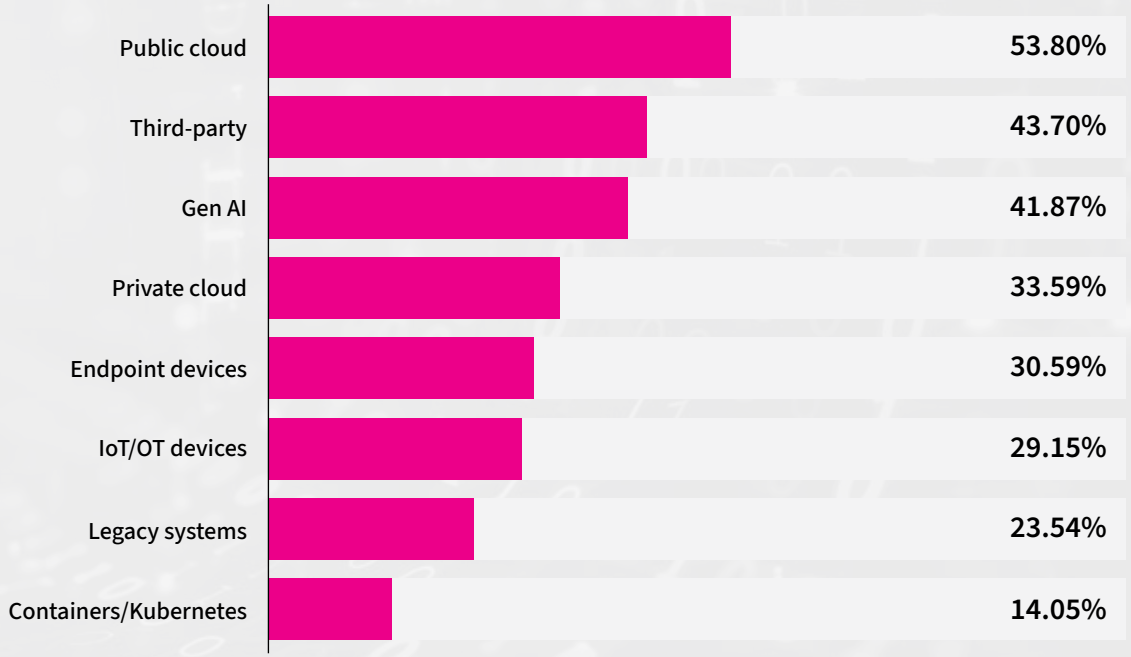
Public Cloud

Security and IT decision-makers around the globe overwhelmingly agree that the public cloud poses a significant risk to their organization (53.8%).

Perceived cybersecurity risk was highest in the U.S. (61.6%), and in the technology sector (59.2%).

The 2024 Snowflake data breach demonstrated the growing risks cloud technologies pose. At least 165 Snowflake customers, including major technology organizations like Pure Storage and AT&T, were affected, resulting in a compromise of their customers' data.

Riskiest attack surface



Supply Chain

Third-party services and integrations are a concern for 43.7% of the organizations surveyed.

This tied with public cloud as the number one risk within the telecom industry, an unsurprising outcome given Salt Typhoon's attacks earlier this year. The threat group targeted major providers like Verizon, AT&T, T-Mobile, and Lumen Technologies by compromising third-party vendors and contractors to infiltrate networks.

Generative AI

Generative AI applications (41.9%) ranked third, with a perceived risk larger than that of legacy systems (23.5%) and endpoint devices (30.6%).

On the global front, France shows the highest level of concern (59%), while the UAE exhibits the lowest (36.8%).

TOP 5 TIPS FROM CISA TO MITIGATE SALT TYPHOON'S IMPACTS

1. Monitor all devices that accept external connections from outside the corporate network.
2. Monitor user and service account logins for anomalies.
3. Ensure the inventory of devices and firmware in the environment are up to date.
4. Establish a baseline of normal network behavior and define rules on security appliances to alert on abnormal behavior.
5. Confirm that TLSv1.3 is used on any TLS-capable protocols.

More here.

The emergence of EDR killers and fileless attacks point to a crucial need for defenses that can withstand and proactively counter emerging, sophisticated endpoint-focused techniques.

The Attacker's Playbook

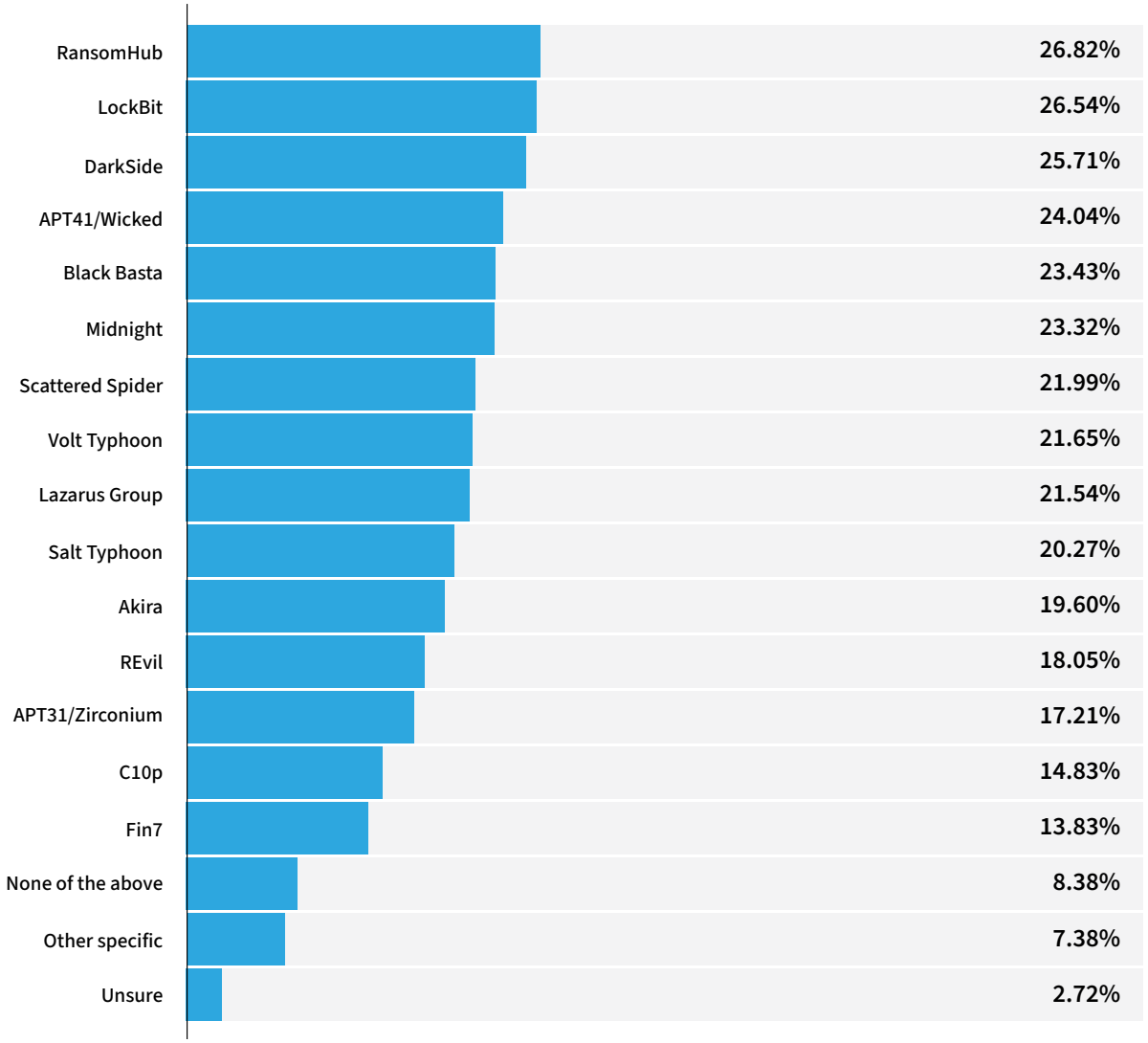
An attacker's playbook is similar to that of an ultra-cheap used car dealer's; last year's model is given a new coat of paint, creating an impression of elegance and sophistication at a glance — but a closer look reveals superficial changes.

Prolific Threat Actors

The past year revealed a dynamic and ever-shifting threat landscape, marked by the reemergence of familiar adversaries, a persistent barrage of attacks from established groups, and the arrival of formidable new players.

Our findings indicate a sustained and varied threat landscape, characterized by ongoing activity from numerous malicious actors. However, when asked which were most detected over the last 12 months, RansomHub (26.8%), LockBit (26.5%), and DarkSide (25.7%) took the top spots.

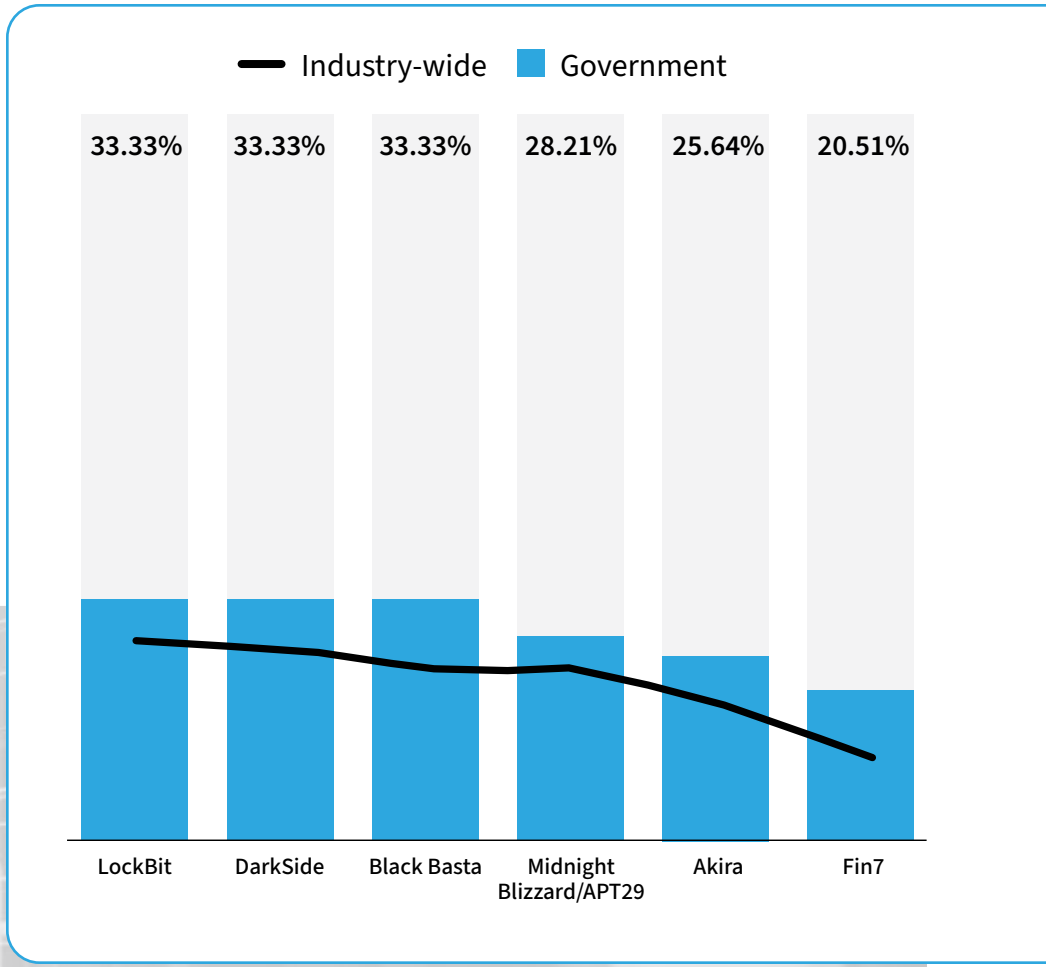
Most detected threat actors



The data shows that LockBit presents a significantly elevated threat in Germany, registering a 37% detection rate compared to other regions. This aligns with the group's high-profile attack on Deutsche Telekom in 2024, during which the country's largest telecommunications provider was targeted in a ransomware incident.

The government sector increasingly finds itself a prime target for these threat actors. A number of groups, including LockBit (33.3%), DarkSide (33.3%), Black Basta (33.3%), Midnight Blizzard/APT29/Nobellium/Cozy Bear (28.2%), RansomHub (25.6%), Akira (25.6%), Volt Typhoon (23.1%), and Fin7 (20.5%), stand out as being particularly active in the government space and have demonstrated significant impact.

Consider both Midnight Blizzard's breach of Microsoft's email system that led to the exfiltration of correspondence between the United States' Federal Civilian Executive Branch (FCEB) agencies and Black Basta's attack on the Chilean government just last year.



Common Tactics

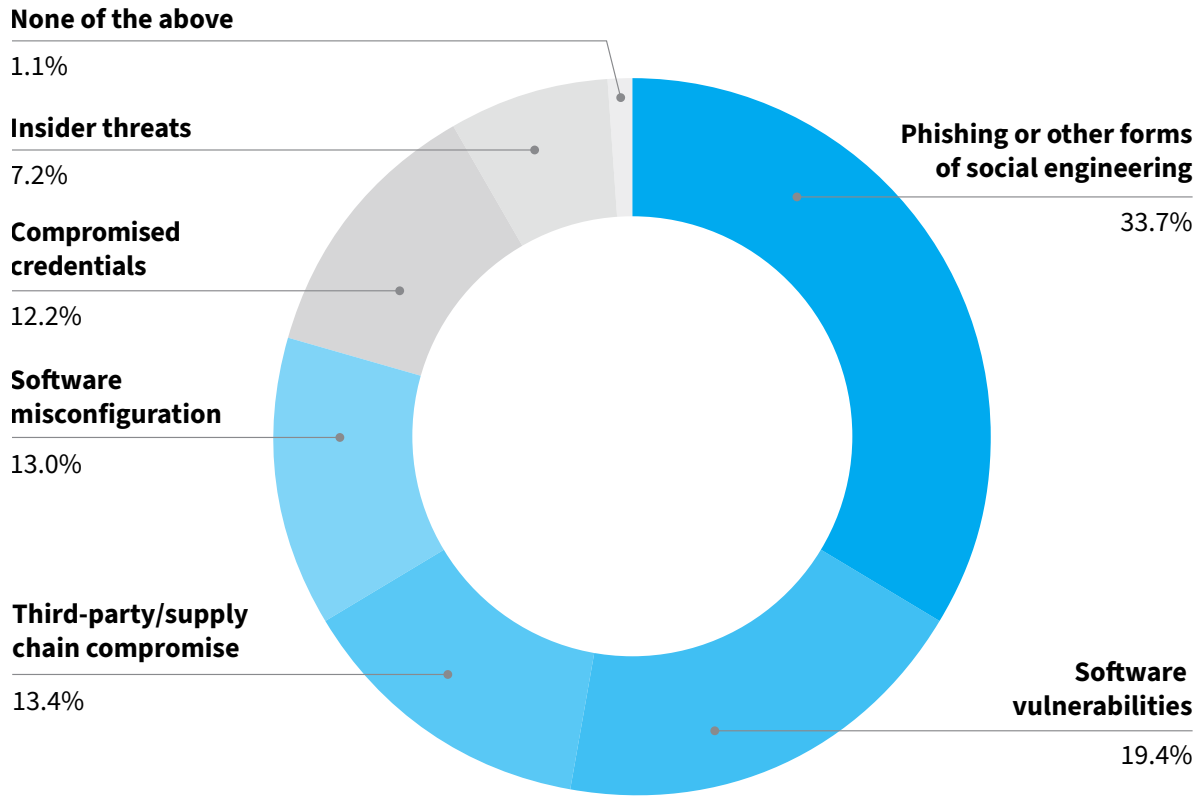
When looking at how threat actors are carrying out their attacks, their tactics aren't all that different.

Phishing and social engineering emerged as the leading initial points of entry for attackers, with 33.7% of IT and security decision-makers citing them as the most common infiltration methods.

Software vulnerabilities represent the second-most common entry point (19.4%), followed by third-party/supply chain compromise (13.4%).

Over the last year, we've observed compromised credentials (12.2%) are increasingly becoming a primary gateway for attackers. Once obtained, these stolen login details allow malicious actors to gain unauthorized access, move laterally within networks, escalate privileges to access more sensitive systems, and deploy further attacks like malware or ransomware, often operating undetected for extended periods.

Most common initial point of entry for attackers



SCATTERED SPIDER

Scattered Spider has maintained an aggressive operational tempo over the last year, with detections reported by almost a quarter of respondents. The group's opportunistic approach is evident in its targeting of various industries, including retail, insurance, and aviation.

What makes their campaigns particularly effective is a sophisticated combination of social engineering and technical skill. They routinely bypass multi-factor authentication (MFA) and compromise help desks to secure initial network access. This access is then sold to ransomware groups like ALPHV/BlackCat and RansomHub, who use it to launch their own attacks.

The Booming Ransomware Economy

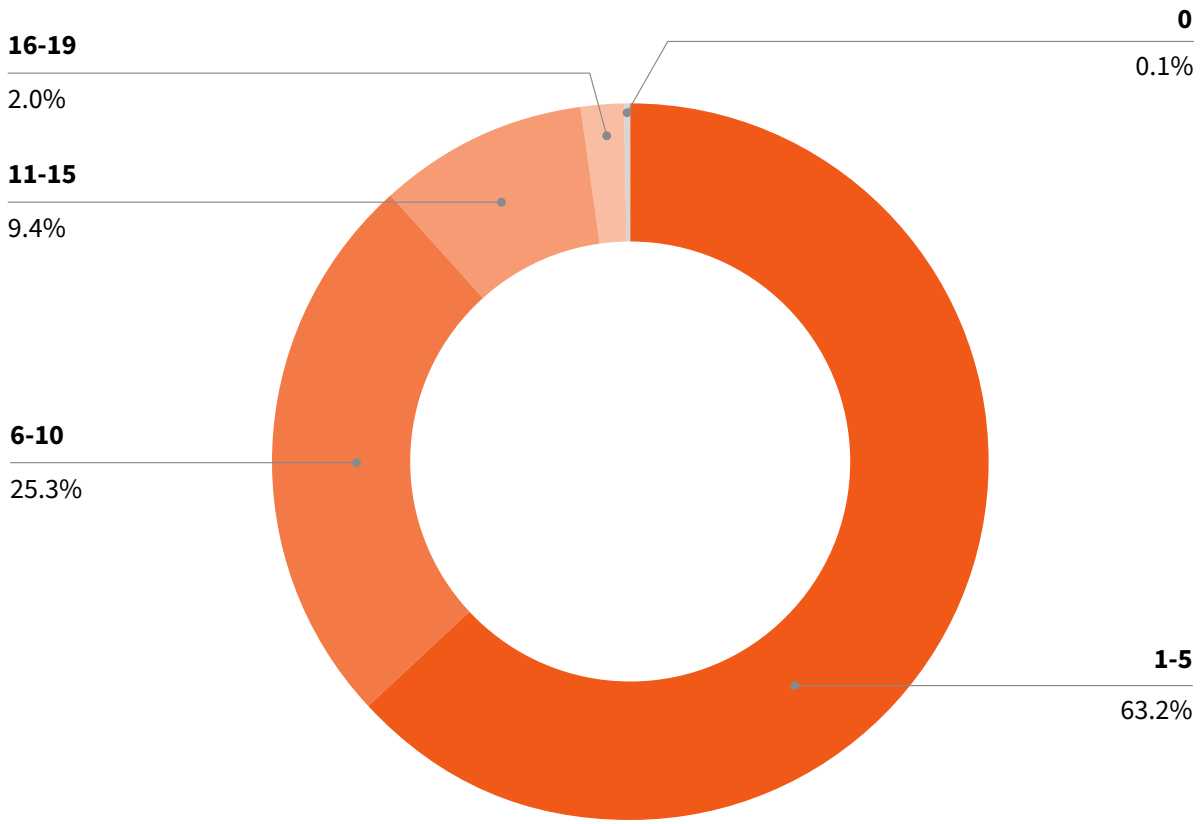
Cybercriminals are transitioning from many widespread, opportunistic ransomware attacks to carefully targeted campaigns, resulting in fewer but more intensive incidents.

Frequency

On average, respondents indicated that their organizations experienced somewhere between 5 and 6 ransomware incidents over the last 12 months, about a 25% decrease from the nearly 8 incidents in 2024.

Although the total number of incidents has declined, the percentage of organizations hit with 20 or more ransomware incidents annually has tripled, rising from 0% to 3% year-over-year. This trend is particularly evident for organizations in critical industries such as healthcare (20%) and government (10%).

Number of ransomware incidents in the last 12 months



Cost

While 70% of respondents said their organization paid the ransom, a new trend has emerged: For the first time, there has been an overall decline in the number of ransom payments made to threat actors. The number of organizations that say that they never paid a ransom has tripled, from only 9% last year to 30% this year.

However, for those who did pay, ransom costs have gone up substantially.

This year's survey found the average ransom payment was more than $3.6 million — a million dollars more than last year's average of $2.5 million.

The average amount organizations paid up when hit with a ransom varied by country. In the UAE, for example, organizations faced an average of 7 ransomware incidents, the highest number globally. What's more, it also paid ransoms that were 26% higher than the global average, with an average payment of $5.4 million. Australia, on the other hand, experienced the fewest ransomware incidents globally, averaging just four per year. It also had the lowest average ransom payment, at $2.5 million.

When looking at the vertical split, the healthcare sector made the highest payouts ($7.5 million), followed by the government sector (just below $7.5 million) and the finance sector ($3.8 million).

GROWING RANSOM PAYMENTS IN 2024

Unnamed Fortune 50	CDK Global	Change Healthcare
$75 million	$50 million	$22 million

THE AVERAGE
ransom payment
WAS MORE THAN
$3.6 million

The Attacker's Advantage

Organizations are struggling to detect and respond to ransomware in a timely manner, giving adversaries a major advantage.

Delayed Detection

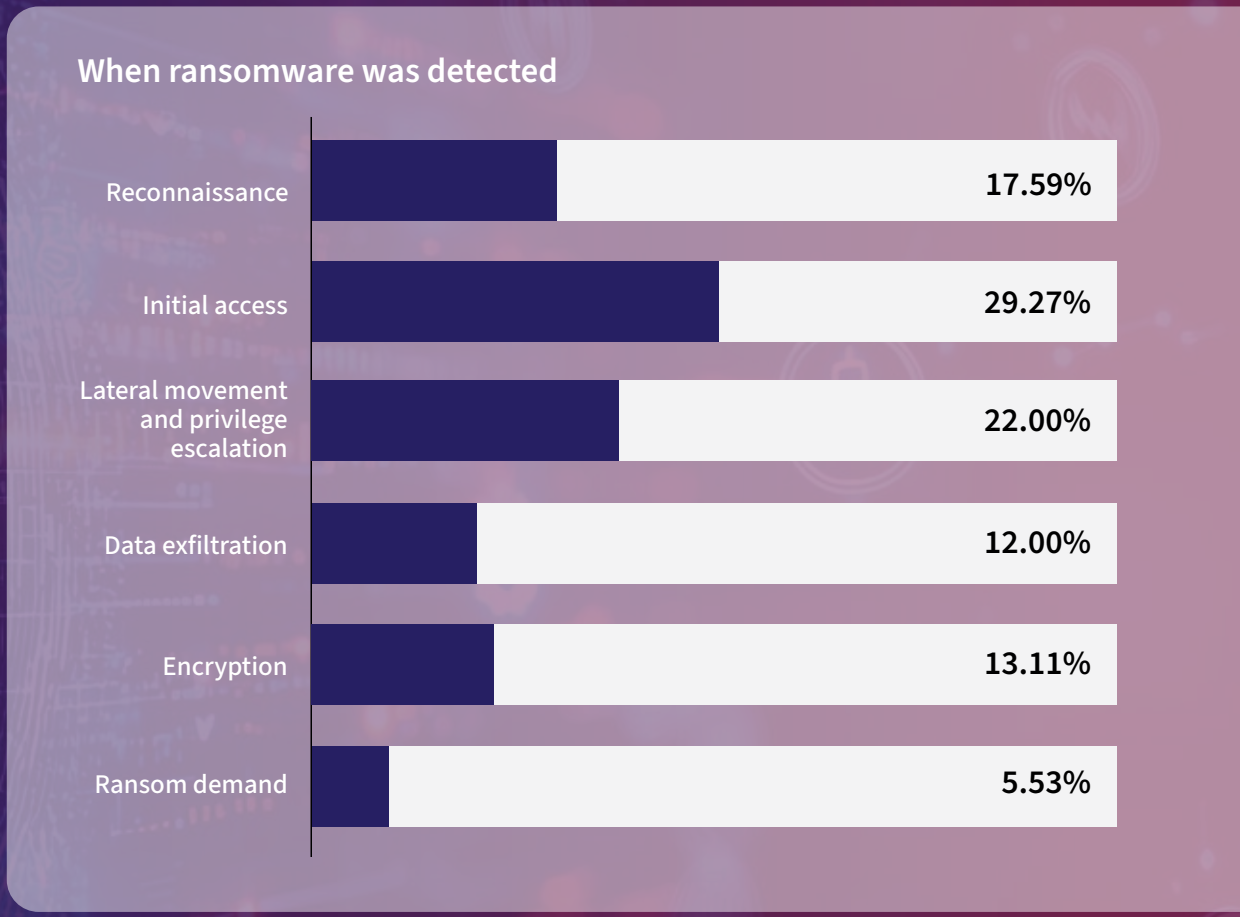
Organizations often aren't able to detect ransomware until well after the initial point of entry, which provides attackers with ample time to sleuth through the network and cause extensive damage.

Nearly a third of respondents (30.6%) only recognized they were being targeted by ransomware during or after data exfiltration had already begun.

Extended Dwell Times

When asked how long threat actors had access to their systems prior to a ransomware incident, respondents cite an average of nearly 2 weeks. Notably, the government and education sectors report significantly longer dwell times, about 7 weeks and 5 weeks, respectively.

However, actual dwell times often far exceed perceived durations. High-profile incidents starkly illustrate this: The SolarWinds attackers gained access in September 2019, but remained undiscovered until December 2020. Similarly, the Kyivstar breach saw attackers present for at least seven months before detection.

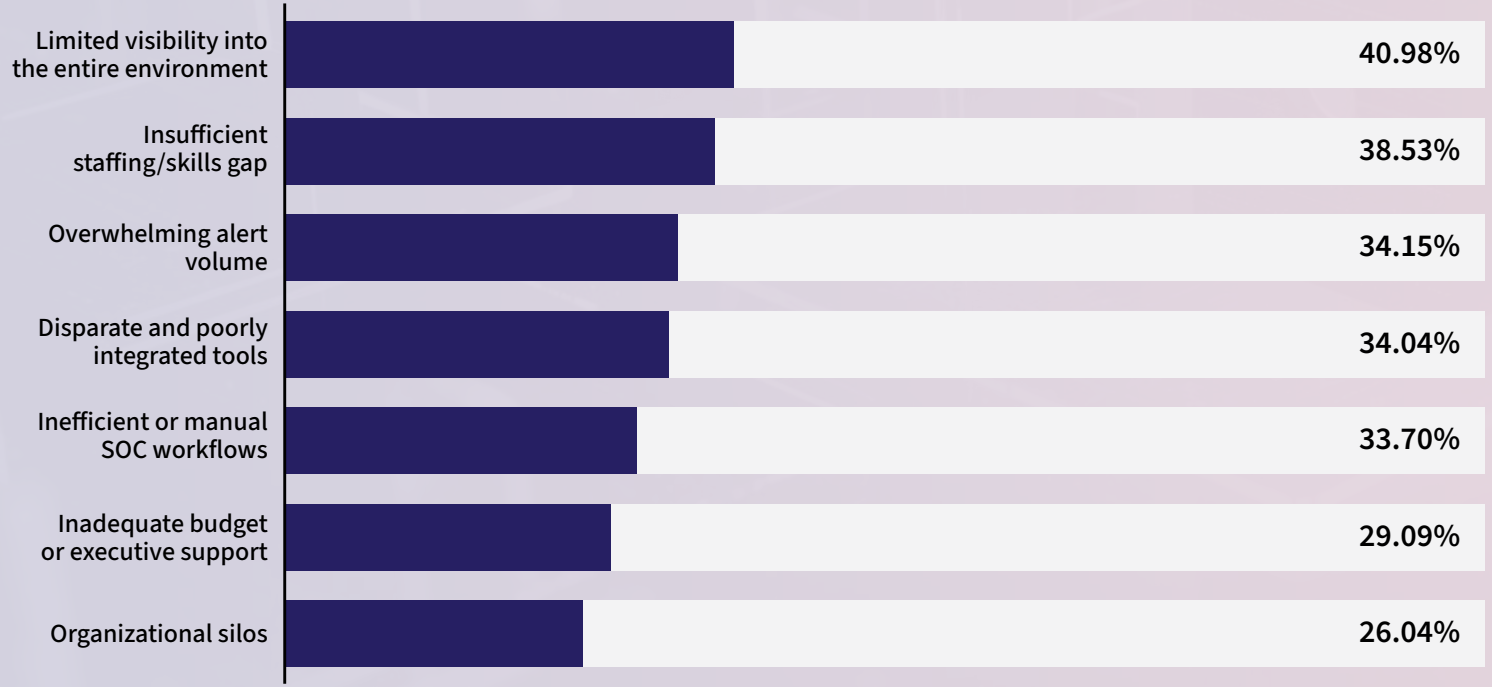


The SOC's Achilles' Heel(s)

Organizations are struggling to gain a defensive advantage in an adaptive and evolving threat landscape.

When asked about the challenges that most hinder a timely response to security threats, respondents uncovered a crucial insight: Organizations aren't grappling with one primary issue but rather a complex web of equally pressing obstacles.

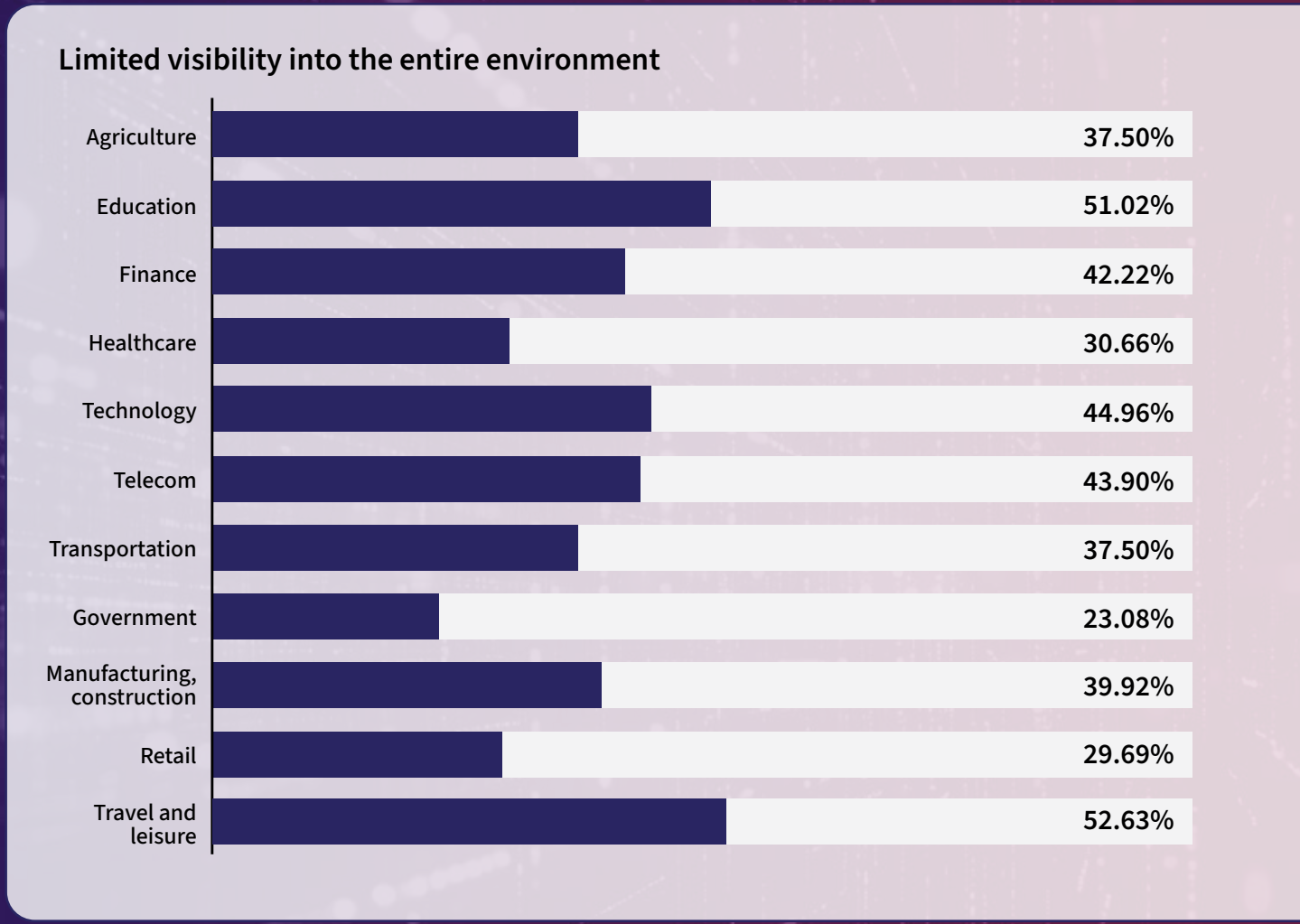
The responses showed a remarkably even distribution across various critical areas, underscoring the pervasive struggle to achieve effective defense. These challenges range from a lack of visibility across their digital footprints and the ongoing cybersecurity talent shortage, to the debilitating impact of an overwhelming volume of alerts that can drown out critical signals.



The visibility challenge is particularly acute in the technology, telecom, finance, and education industries.

DID YOU KNOW?

With a focus on delivering comprehensive network visibility, ExtraHop detects ransomware every 1.5 days across its customer base. Learn more here.



The Security Response and Operational Resilience Crisis

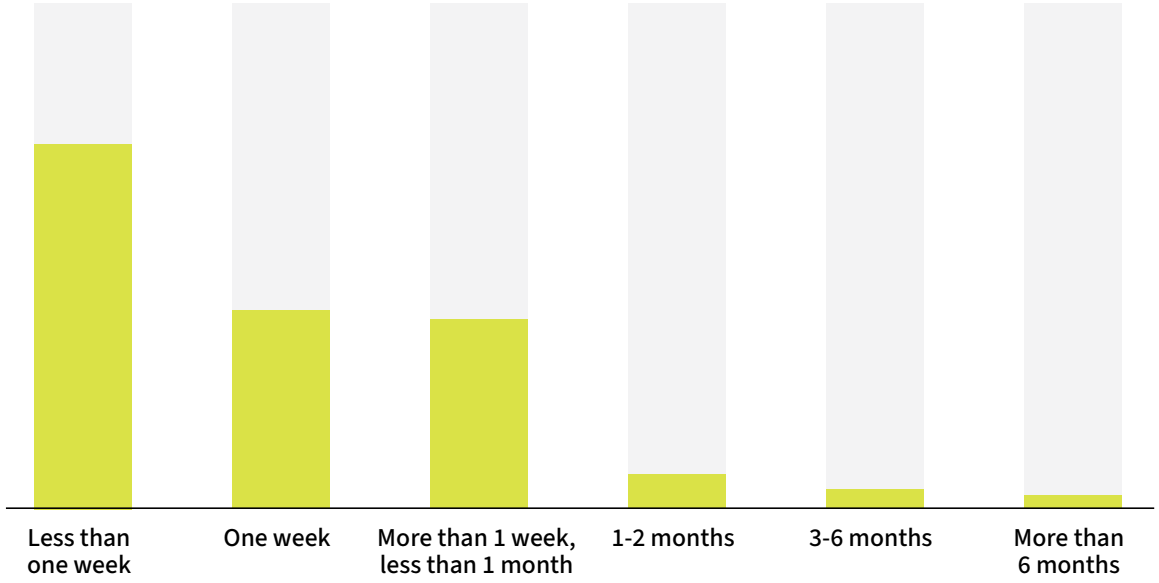
While the evolving threat landscape and expanding attack surface make a security team's swift response more critical than ever, many organizations are struggling to keep up. The resulting delays can significantly impact business operations, leading to prolonged downtime, loss of customer trust, and severe financial penalties.

Time to Respond

On average, it takes organizations just over 2 weeks to respond to and contain a security alert, from initial detection to resolution.

The U.S. experiences an average of 2.8 weeks, while critical industries globally, like government and transportation, face upwards of 3 weeks.

Time to respond to and contain a security alert from initial detection to resolution

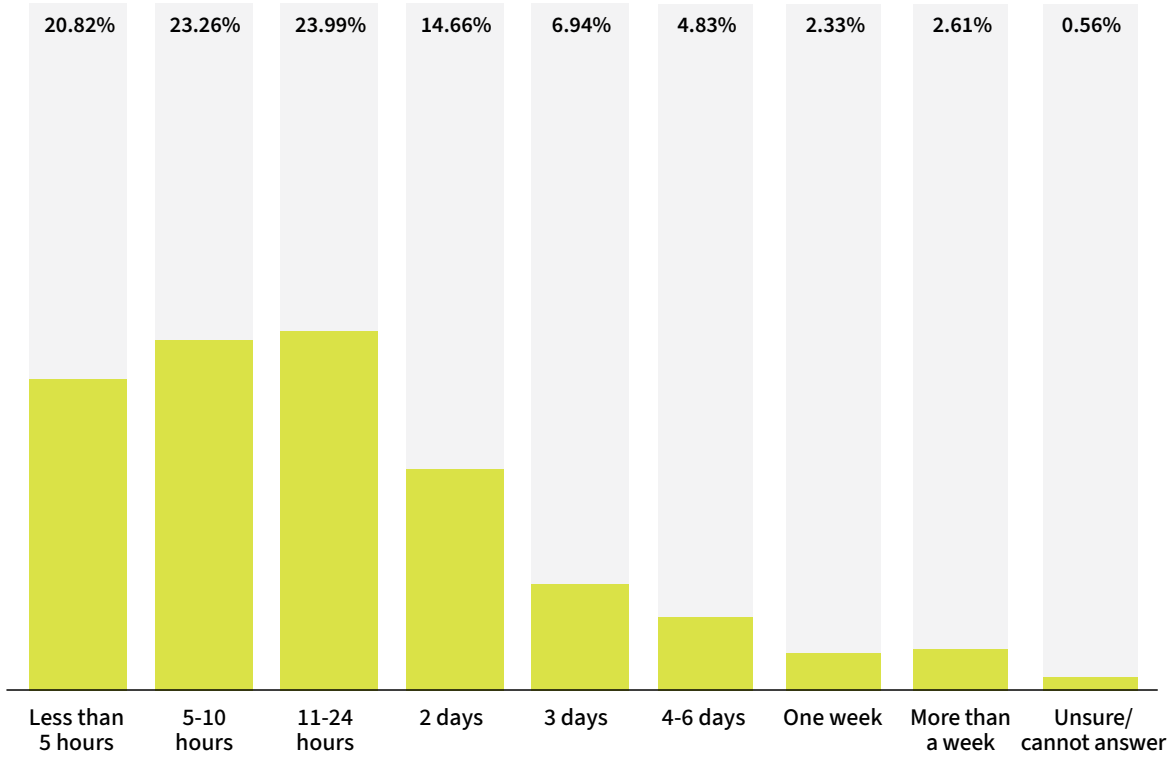


Business Impact

When asked how much downtime organizations experienced after a cyber incident, respondents reported an average of 37 hours.

More than half (55%) said they experienced 11 or more hours of downtime on average, and nearly a third reported downtime extended for two days or more.

Average downtime per incident



When looking at the industry breakdowns, respondents in the transportation industry reported the highest average amount of downtime (74 hours).

In August 2024, the Rhysida ransomware group attacked the Port of Seattle, which operates Seattle-Tacoma International Airport, knocking some systems offline for more than three weeks.

Bigger Targets, Smarter Threats

Cybercrime has evolved into a sophisticated business. Modern-day threat actors have moved past simple attacks, adopting a profit-driven mindset with highly targeted campaigns designed to maximize financial gain. This new approach is fueled by the growing complexity of IT environments, which creates a wider attack surface for criminals to exploit.

The combination of sophisticated attackers and a broader attack surface is a dangerous one. It makes attacks harder to detect and gives criminals a significant head start. Two weeks is a long time for an intruder to go unnoticed, and with security teams taking another two weeks to respond, attackers have a full month to cause serious damage.

Playing defense isn't enough. We must get ahead of these threats by making it harder for attackers to get a foothold and by dramatically shrinking the time they have to operate.

3 Steps to Protect Your Organization Today

1. Understand Your Attack Surface

As attack surfaces become more complex, you must have a comprehensive understanding of your risks. This means knowing exactly what's in your network and where vulnerabilities exist. A robust solution gives you the visibility you need to inventory and understand what's at risk, helping you scale defenses as your environment grows with new containers, cloud services, endpoints, and IoT devices.

2. Monitor Internal Traffic

Don't just secure the front door; watch what's happening inside. Many modern attacks bypass traditional perimeter defenses and, once in your network, move laterally to find what they're looking for. By monitoring east-west traffic, you can spot this malicious movement and intervene early. This gives you the power to stop attackers before they can escalate their attack, effectively shortening their dwell time and protecting your organization from major harm.

3. Stay Ahead of Evolving Threats

The threat landscape is in constant flux. You need to understand not just what attackers are doing today, but what they'll be doing tomorrow. This includes keeping up with their evolving tactics and the new challenges posed by emerging technologies like generative AI, which can be used to create more convincing phishing attacks and more sophisticated malware. Partnering with a solution provider that has deep threat intelligence can help you stay on top of these trends and build a proactive security strategy that anticipates and neutralizes future threats.

Methodology

In conjunction with Censuswide, ExtraHop surveyed 1,800 security and IT decision-makers (director level or above) working for organizations with 1,000+ employees in the U.S., U.K., France, Germany, Singapore, Australia, and the United Arab Emirates in July 2025.

About ExtraHop

ExtraHop empowers enterprises to stay ahead of evolving threats with the most comprehensive approach to network detection and response (NDR).

Since 2007, the company has helped organizations across the globe extract real-time insights from their hybrid networks with the most in-depth network telemetry. ExtraHop uniquely combines NDR, network performance management (NPM), intrusion detection (IDS), and packet forensics in a single, integrated console for complete network visibility and unparalleled context that supports data-driven security decisions. With a powerful all-in-one sensor and cloud-scale machine learning, the ExtraHop RevealX™ platform enhances SOC productivity, reduces overhead, and elevates security postures.

Unlock the full power of network detection and response with ExtraHop. To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®