The True Cost of a Cyberattack 2025 Edition

Avoid the Hidden Price Tags, Pitfalls, and Damage That Cyberattacks Can Wreak on Your Business

HUNTRESS

Table of Contents

Introduction

Cyberattackers Have ALL Businesses in Their Crosshairs

The unfortunate truth is that hackers now see businesses of all sizes as lucrative targets. You may think you're safe, that your company isn't big enough to be on their radar, but these malicious actors are eyeing your organization as a way to profit quickly.

Like many businesses, you might find it challenging to "do more with less." Today, due mainly to economic and geopolitical concerns, many organizations' cybersecurity budgets are on the chopping block, which impacts business' cyber defense and resilience abilities.

This can lead to tragic outcomes. What many businesses are learning the hard way is that the cost of recovering after a cybersecurity attack can be much higher than the initial investments required to protect their business.

Recent studies reveal that data breaches are a major worry for IT professionals, especially with more people working remotely. Here's the kicker: **95% of data breaches come down to human error.**[1]

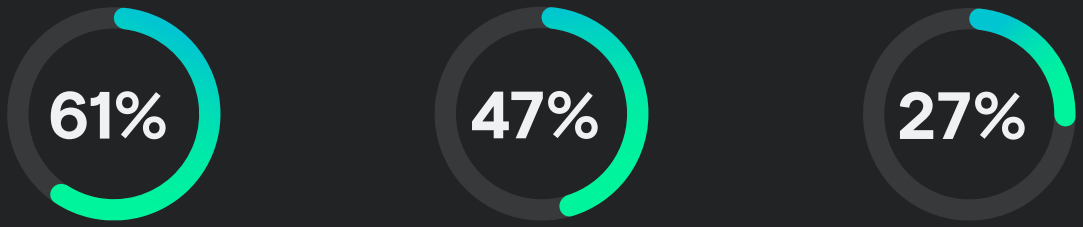
Put simply, data breaches can lead to major financial losses for your business. Customers may leave you. Your reputation may suffer. And your duty to remediate—along with other liabilities—may add up at a stunning rate.

In the most extreme situations, failing to identify and shut down a cyberattack before it causes damage could cost you the loss of your entire company.

> This ebook reveals the evolving risks and solutions you need to know. Read on to learn how to **protect your business from the fallout of cyberattacks.**

Cybersecurity Gaps by the Numbers

Research from Huntress[2] revealed the following resource gaps for mid-sized enterprise businesses:



don't have dedicated cybersecurity experts

don't have an incident response plan

don't have cyber insurance coverage

These gaps create opportunities for malicious hackers to infiltrate networks, steal sensitive data, disrupt operations, and extort ransoms.

These gaps are also why 24% of mid-sized businesses report that they've either suffered a cyberattack or don't even know if they've suffered one in the last 12 months.

HUNTRESS

Challenges

Cyberattacks Are Becoming More Complex to Resolve

Not all cybersecurity solutions are within reach for some businesses. In fact, they're bundled to include features most businesses don't need or can't justify paying for. The cost of running a 24/7 security operations center (SOC) is out of reach for most businesses. Cybersecurity experts can command premium salaries. Plus, the cost of cyber insurance may seem equally high.

These price tags can leave organizations like yours underserved, unprepared, and vulnerable. But if a cyberattack happens, the damage can carry into many parts of your business, including:

- **Financial losses** such as fines, fees, and other associated costs, especially concerning matters of compliance.
- **Reputational damage** resulting in the loss of customers, including those whose data was breached and others who may learn of the breach.
- **Legal liability** for the consequences of a data breach, complicating an already complex situation.

Understanding these impacts can help you determine if your current cybersecurity solutions are appropriate in scope.

For example, cybersecurity is absolutely non-negotiable if you're responsible for managing healthcare data. Under the Health Insurance Portability and Accountability Act (HIPAA), Personally Identifiable Information (PII) breaches can result in fines exceeding $71,000 per violation.[3]

Let's look at the extent of the possible consequences to businesses like yours and discover how you can mitigate risk.

Penalties for HIPAA Violations

As of 2025, the US Office for Civil Rights (OCR) enforces civil monetary penalties across four different tiers.[3]

- **Tier 1 (Lack of Knowledge):** Up to $35,581 per violation
- **Tier 2 (Reasonable Cause):** Up to $71,162 per violation
- **Tier 3 (Willful Neglect, Corrected):** Up to $71,162 per violation
- **Tier 4 (Willful Neglect, Not Corrected within 30 Days):** Up to $71,162 per violation (with a cap of $2,134,831 per violation category per year)

The EU's General Data Protection Regulation (GDPR) fines pack a punch:[4]

- **Article 83(4):** Up to €10M or 2% of global turnover (whichever is higher)
- **Article 83(5):** Up to €20M or 4% of global turnover (whichever is higher)

Cyberattacks Are Expensive

The financial cost of cyberattacks has skyrocketed. Here's what the latest data reveals:

$4.9M	Average global cost of a data breach in 2024 (up 10% from the previous year)[5]
75%	of the cost increase comes from lost business and post-breach response activities[5]

Most malicious hackers want access to data for financial gain. That means certain types of data, like PII, may be more attractive to them. Therefore, industries with high volumes of PII, such as healthcare, government, retail, or education, are more at risk.

Industries most at risk

Healthcare

Tech

Government agencies

Retail

Education

What common stolen data sells for on the dark web in 2025:[6]

Credit card (US, with CVV):

$10 - $120

Online bank login:

$200 - $1,000+

Facebook account:

$45 - $50

Medical records:

$500+

HUNTRESS

Direct and Indirect Costs

Regardless of your industry, a successful cyberattack comes with heavy financial costs, direct or indirect.

Directly, hackers may demand large sums of money, threatening to divulge data publicly or use it in other malicious ways if your company doesn't pay. Even for smaller businesses, ransom demands may be in the millions, and timelines for you to respond and take control of the situation may be unreasonably tight.

It's worth noting that the US Federal Bureau of Investigation (FBI) standard advice is NOT to pay ransoms. Even if you choose to pay, there's no guarantee your business will get any of its data back.

The hard reality is that if you aren't prepared to identify and stop a cyberattack before data is compromised, you're on the hook financially.

That's because indirect costs rack up quickly. The disruption to normal operations may require additional labor efforts and lengthen typical cash cycles. Then, there are expenses related to hiring firms to help rebuild various systems. There may also be costs associated with identity theft, credit monitoring, or legal ramifications.

Cyberattack Costs by the Numbers

The financial cost of a cyberattack is highly detrimental to smaller organizations.

$115,000	Median ransom payment in 2025 (down 23% from $150,000 in 2024)[7]
64%	of orgs hit by ransomware in 2025 didn't pay (up from 50% in 2023)[7]
60%	Approximate number of small businesses that shut down within six months of a cyberattack7
$65k	Average cost of downtime on local government after a cyberattack[9]
$22k	Estimate an automotive manufacturer might lose **for every minute** of downtime[10]

These numbers indicate that robust cyber defenses are crucial to protect your business.

Real Attacks

Ransomware nearly crushed a road contractor who endured **a week of critical service outage** and **three months of recovery** after the attack.

Road and bridge contractor E.R. Snell suffered a ransomware attack when malicious actors gained access via an employee's email account.[11] The attackers snuck a keylogger on an on-premise mail server to secure administrative access, encrypted E.R. Snell's files, and deleted the cloud backups.

Critical services were out for a week, with other services out for three. During the downtime, multiple departments shifted to manual processes. The company paid insurance and betterment fees, hired an outside accounting firm to rebuild five months of data—which took another three months—and hired an outside IT firm to rebuild more than 200 computers.

HUNTRESS

Cyberattacks Hurt Your Reputation

When a data breach happens, your customers' trust is also breached. Your business may suffer widespread reputation damage as word travels via notices, social media, and other channels.

Don't forget that your reputation matters more than ever today, as other brands are saturating markets to win the spotlight. A loss of reputation may lead your customers to switch to your competition, and prospects may choose to stay away from you altogether.

Real Attacks

Data dumps can be **traumatizing.** A public school faced a devastating ransomware attack, **exposing 300,000 files with sensitive information** and leaving staff, students, and their families to **suffer financially and emotionally.**

MINNEAPOLIS PUBLIC SCHOOLS
Urban Education. Global Citizens.

Minneapolis Public Schools lost staff and students after hackers dumped more than 300,000 files online in a sweeping ransomware attack.[12] The records contained contacts, Social Security numbers, medical information, discrimination and sexual assault complaints, and more.

The school's lack of an incident response plan further harmed staff and students. Many individuals and their families learned of the breach from reporters. Staff struggled to obtain credit monitoring and identity theft protection. Worse yet, students experienced post-traumatic stress disorder, and not surprisingly, their families pursued legal remedies.

Failures to protect sensitive data and work with trusted experts in the aftermath created a full-on crisis for Minneapolis Public Schools, including lasting reputational damage.

HUNTRESS

Cyberattacks Risk Sensitive Data

Malicious hackers are notoriously stealthy. They don't always attack the second they get into your environment. Once they've bypassed your preventive tools, they may sit in your environment and wait until they can inflict maximum damage.

Research from 2025 shows the global median dwell time from compromise to discovery is 11 days.[13] That means malicious actors can often sit quietly inside your environment for days—or even weeks—before you notice. And the longer they sit unnoticed, the more damage they can do.

This is especially harmful when your business is responsible for sensitive data. Attacks can result in more than just company financial losses. Individual data may be exposed, resulting in identity theft, credit card fraud, and emotional harm like stress, anxiety, and trauma.

60%
of data breaches involve a human element, like malicious insiders or falling for phishing scams[7]

32%
involve credential abuse[7]

23%
involve social engineering actions[7]

2.8B
More than 2.8B passwords were posted on criminal forums in 2024[7]

HUNTRESS

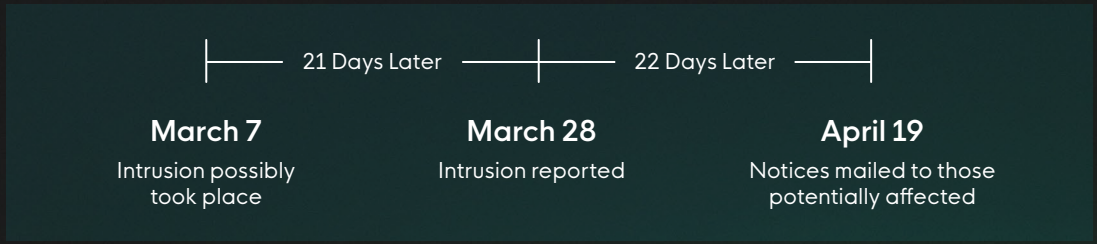
Real Attacks

Hackers stole **two million people's healthcare data** in an attack on an imaging provider.

Shields Health Care Group, an imaging services provider for more than 50 healthcare facilities, experienced a breach involving the healthcare data of two million individuals.[14]

Information included full names, Social Security numbers, driver's license numbers, dates of birth, home addresses, provider information, diagnoses, billing information, insurance numbers, and more.

Shields identified the incident on March 28, 2022, but reported the intrusion may have happened as early as March 7. They didn't mail notices until April 19.



This major delay in identification gave malicious actors plenty of time to collect and use data for financial gain before individuals could monitor their personal impact. If only the cyberattack had been identified and reported in a timely manner, millions of people could have avoided extensive risk.

Shifting Impacts of Cyberattacks

In 2015, when digital transformations began taking hold across industries, *Harvard Business Review* (HBR) published an article titled "Why Data Breaches Don't Hurt Stock Prices."[15]

It posits that the lack of market response to enterprise-level breaches was due to shareholders' lack of sufficient information or tools to measure impact.

By 2023, another HBR article, *"The Devastating Business Impacts of a Cyber Breach,"* [16], reveals an apparent change. It reports breaches result in an average stock price dip of 7.5%, with market cap losses in the billions.

Companies with extensive resources suffered these losses to resolve impacts. But most businesses don't have this kind of financial might—existing resources need to stretch further and lift harder.

As data breaches gain more serious attention, businesses like yours face the challenge of finding new ways to combat the impacts of cyberattacks.

⇩ 7.5%

The **average stock price dip** for a publicly traded company after a cyber breach, according to HBR[16]

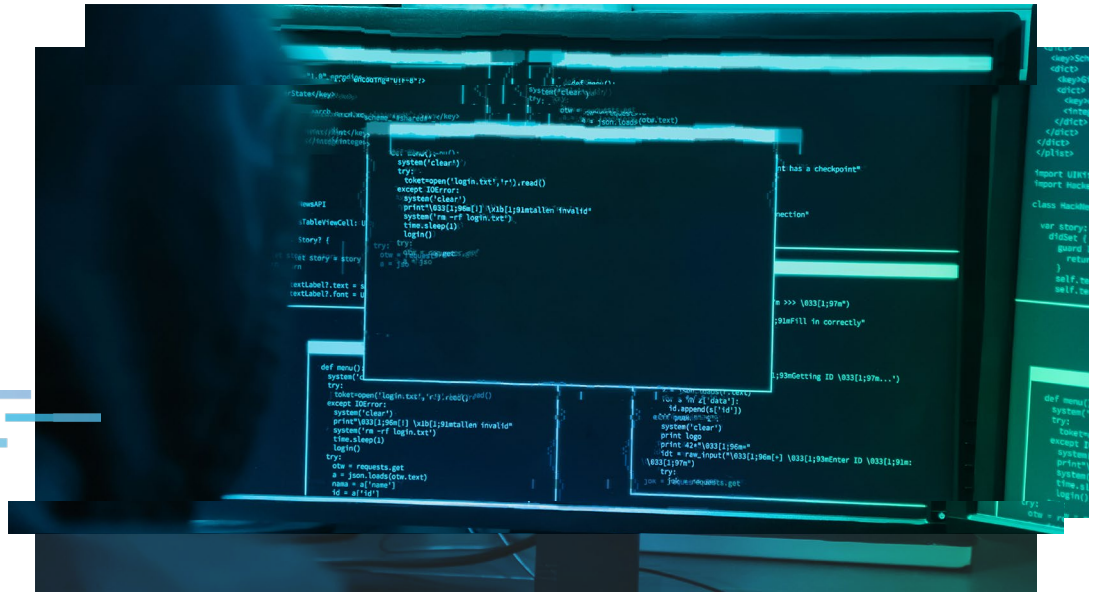
Solutions

Threat Detection and Response

We've discussed how cyberattackers can catch businesses off guard, resulting in serious losses. In most cases, this happens when organizations miss the "detect" and "respond" components within their layered security stack.

While prevention-based technologies like antivirus and firewalls have an important role in obstructing attackers' attempts at initial access, they shouldn't be the only lines of defense. Solutions designed to detect, isolate, and respond to malicious actors are available without the heavy costs associated with enterprise solutions.

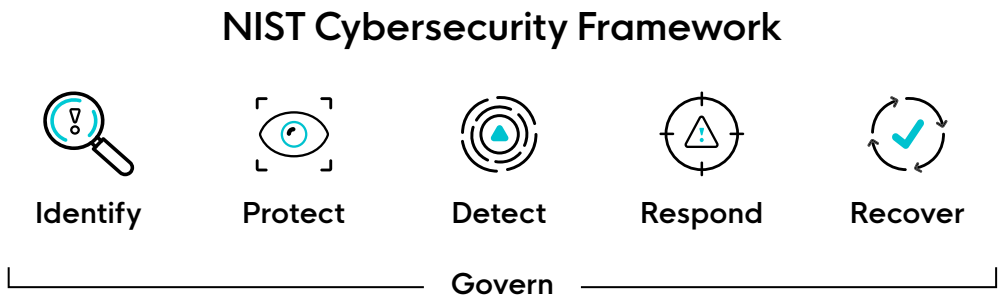
Let's dive into what this means for your business.



Why Is Threat Detection and Response So Important?

To stop hackers, you must have a strong, layered security stack in place. After all, attackers are cunning. They've figured out ways to slip past your preventive defenses. That means you need more layers—detection and response layers—to snare hackers before they can deploy ransomware or inflict major damage.

The Cybersecurity Framework from the National Institute of Standards and Technology (NIST)[17] illustrates how layers of security solutions should work together to minimize the risk of cyber threats. It focuses on five core components:



HUNTRESS

Together, these "layers," or successive tiers of security software solutions, can maximize an organization's ability to defend itself from an attack.

Detection and response are twin pillars that fortify an organization's security posture. They serve as the early warning system and swift reaction force against the ongoing cyber threats that target businesses like yours.

Detection and response operate in a symbiotic relationship within the cybersecurity ecosystem. The faster and more accurately an organization detects a threat, the more effectively it can respond, mitigating potential damages and reducing the overall impact on your operation and reputation.

54%
of organizations experienced malware infections in 2025[18]

44%
of data breaches involved ransomware in 2025 (up from 32% in 2024)[18]

88%
Ransomware hits smaller organizations harder—affecting 88% of non-enterprise businesses vs. 39% of large organizations[7]

Common Detection and Response Solutions

Your business needs more than prevention. That's where detection and response solutions come in. A few popular solutions can provide these capabilities, mainly endpoint detection and response (EDR) and identity threat detection and response (ITDR).

Managed Endpoint Detection and Response (EDR)

EDR stands as a formidable guardian at the front lines of your organization's digital infrastructure. It's focused on monitoring activities on devices like desktops, laptops, and servers. EDR is designed to detect, investigate, and mitigate potential threats at the endpoint level. By analyzing data from endpoints in real time, EDR solutions can identify suspicious behavior, malware, and other security anomalies that may indicate a looming threat.

Managed Identity Threat Detection and Response (ITDR)

ITDR protects against one of the biggest threats today: compromised identities. Passwords and MFA alone just don't cut it anymore—attackers are stealing credentials, hijacking sessions, and using trusted access to bypass the usual defenses. ITDR keeps an eye out for suspicious activity like business email compromise (BEC), account takeovers, stolen credentials, rogue apps, and unusual logins. It detects and responds quickly to stop attackers before they can escalate or cause serious damage.

HUNTRESS

Managed Security Information and Event Management (SIEM)

SIEMs collect logs from a range of sources, like endpoints, firewalls, VPNs, and apps, to spot suspicious activity and help meet compliance requirements. But traditional SIEMs are built for big enterprises with the resources to deal with noisy logs, constant rule tweaking, and sorting real threats from false alarms. For many organizations, this means high costs, heavy workloads, and little ROI. A modern SIEM should do better. It should filter out unnecessary data to cut costs, focus on important signals, and offer 24/7 monitoring by experts who turn alerts into action. With features like automated log parsing, community-driven intelligence, and built-in compliance reporting, advanced threat detection can be both effective and affordable.

Managed Security Awareness Training (SAT)

SAT programs help your employees spot and handle cyber threats like phishing, social engineering, and credential theft. While technology can block a lot of attacks, human error is still one of the biggest weaknesses that malicious hackers love to exploit. For SAT to really work, it needs to be more than just a tool to help you tick a compliance checkbox—it should deliver engaging, expertly designed lessons that stick. Features like animation can make it easier to remember, and hands-on activities like phishing simulations and real-time coaching reinforce what's learned. With cyber threats getting more advanced, solid training not only reduces mistakes but also boosts your organization's defenses and builds a culture where everyone plays a role in keeping sensitive data safe.

Real Attacks

A retailer thwarted a **BEC** attack, preventing hackers from **redirecting invoice payments** and **inflicting financial damage.**

A retailer experienced a Microsoft 365 attack where a malicious hacker assigned themselves privileges and permissions, likely to manipulate invoices and divert funds.[13]

With the help of Huntress' Managed ITDR, suspicious logins were flagged from areas uncommon to the business, including Nigeria and Ireland. Experts from Huntress SOC analyzed rare user agents and eradicated the threat before hackers could direct invoice payments to their own bank accounts.

24%

of IT professionals rate cloud security breaches as top emerging threats[18]

24%

of threats in 2024 involved infostealers[18]

HUNTRESS

Using Managed Solutions to Stay Ahead of Evolving Threats

Cyber threats will always evolve. Today, malicious actors are discovering they may work more effectively in groups, combining their strengths and expanding their reach.

Detection and response are critical capabilities, but they're not something you can just "set and forget." These tools require consistent tuning and monitoring by security experts—experts that businesses don't always have in-house and can't afford 'round-the-clock' coverage.

This requirement for expert tuning can leave some organizations at a disadvantage. Many just don't have the in-house resources for this close management, especially as cyberattackers consolidate their powers.

That's where a managed cybersecurity solution comes into play—one backed by an elite 24/7, AI-assisted SOC that supplements your team.

SOC experts manage, triage, and respond to threats targeting your business, containing and helping to remediate threats to minimize impact. These experts investigate alerts and distinguish real threats from false positives, which saves you hours of time and ensures continuous monitoring of your environment. This also helps to reduce your organization's alert fatigue while improving the ability to catch and stop threats before they can inflict damage.

Financial gain (27%) and data theft (23%) are the most common motivations for threat actors[18]

HUNTRESS

Time

Limited resources mean limited time. Some organizations may struggle to manage alerts, parse false positives, and train staff on new or unknown threats.

Speed is crucial to cybersecurity because:

258 Days	The average time to identify and contain a security breach is 258 days.[5]
$5M+	Data breaches lasting less than 200 days average a cost of **$3.87M**, while those extending beyond 200 days rise to **$5M+**, a staggering difference of **$1.14M**.[19]

A managed solution brings advanced cybersecurity expertise to identify both known and emerging threats more effectively. By delivering real-time insights, it enables teams to detect suspicious activity sooner and respond swiftly to eliminate threats. This proactive approach minimizes dwell time, preventing hackers from lingering and causing further damage.

Money

Business decision-makers may think that managed solutions are too expensive. For example, they may choose an EDR just to check the box for compliance purposes.

But incident costs justify the cost of a managed solution:

$4.4M	2024 average cost per data breach worldwide[4]
$3.31M	The 2024 average recovery cost for a company of <500 employees.[20]
$169	The 2024 average cost per stolen record, the highest in years.[21]

A managed solution can help prevent these costs while freeing up budget for other aspects of your business. For many businesses, this can represent massive cost savings because they don't have to hire and retain expensive in-house security experts.

Resources

Not all businesses are backed by the full force of a 24/7, AI-assisted SOC. Overextended teams may miss alerts and mishandle events. Put simply, a lack of resources can leave your business vulnerable to cyberattacks.

450k+ Approximate number of new malware programs created daily.[22]

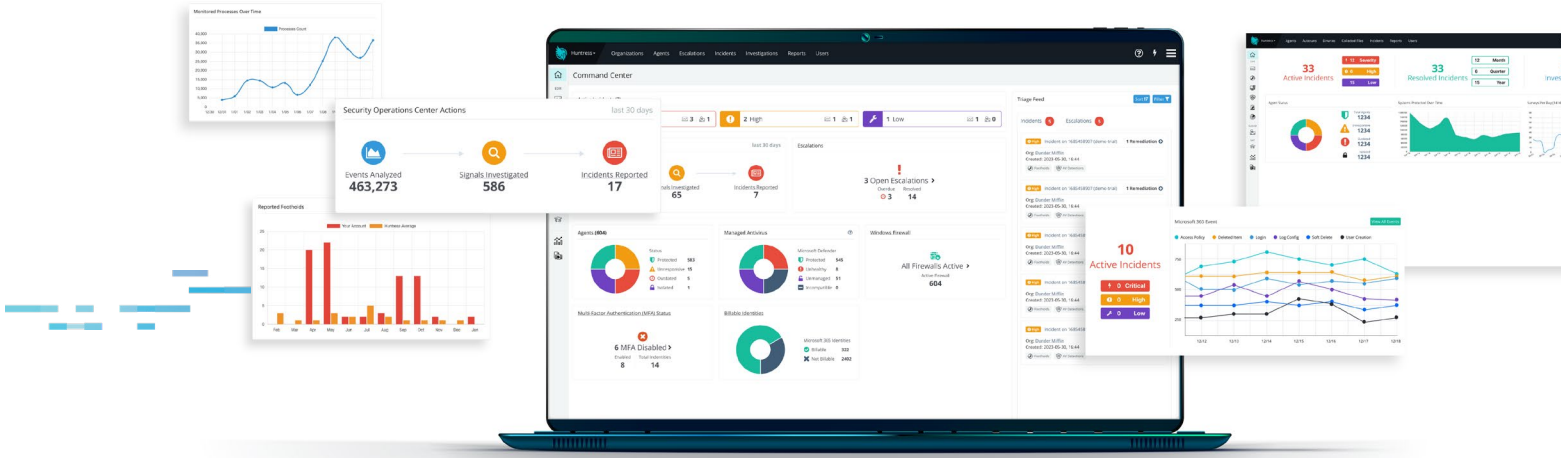
Fully managed cybersecurity ensures you're prepared to stop hackers in their tracks. Managed solutions can give your organization access to top-tier talent so that you can benefit from their expertise and commitment to discovering the latest tradecraft.

Fight Back Against Hackers with Huntress

Many cybersecurity solutions are out there, but most are built for massive, well-funded enterprises. Their hefty price tags reflect all the extra bells and whistles. Not all businesses need all these features—or their high pricing.

Huntress brings enterprise-grade cybersecurity to ALL businesses with the technology, services, and expertise to help you overcome your cybersecurity challenges and help you make confident decisions that move your company forward.

Huntress is easy to use and simple to use, so businesses can keep up with known and unknown security threats.



HUNTRESS

Cyberattacks are an everyday threat. Unfortunately, businesses like yours are most at risk.

Endpoints are proliferating, resulting in new avenues for data access. Cybersecurity budgets are being slashed, leaving IT staff constrained, overworked, or nonexistent. Hackers are fully aware of this. And they're more than willing to take advantage of it.

No matter how sophisticated they seem, hackers are just thieves. They want your money, and they'll gladly jeopardize your business, employees, and sensitive data just to get their hands on some loot. If you're affected by their malicious attacks, the financial burden can be draining, encompassing ransom payments, operational disruptions, and data recovery expenses. In addition, your reputational damage can be just as costly, leading to customer attrition and growing mistrust in your brand. This is why it's imperative that businesses of all sizes now look to fully managed protection for all that's vital to their organization, from endpoints to identities to inboxes and beyond.

As your primary weapon in your cybersecurity arsenal, Huntress can help you:

- Stay protected with our 24/7, AI-assisted SOC, staffed with real experts who always have your back.
- Neutralize endpoint threats quickly and easily with Huntress Managed EDR.
- Protect your Microsoft 365 environments from BEC and other account takeover threats with Huntress Managed ITDR.
- Learn about the latest threats and take advantage of advanced training with Huntress Managed Security Awareness Training.
- Get 24/7 detection, compliance-ready reporting, and actionable insights with Managed SIEM—all at a predictable price.

Stop cyberattacks before they stop your business. Register for a free demo and discover the power of Huntress for yourself.

BOOK A DEMO

HUNTRESS

Sources cited

1. Mimecast. *The State of Human Risk 2025*. Mimecast, 2025. https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/.

2. Huntress. *The State of Cybersecurity for Mid-Sized Businesses in 2023*. Huntress, 2023. https://www.huntress.com/resources/the-state-of-cybersecurity-for-mid-sized-businesses-in-2023.

3. HIPAA Journal. "HIPAA Violation Fines." *HIPAA Journal*. 2025. https://www.hipaajournal.com/hipaa-violation-fines/.

4. European Union, *General Data Protection Regulation*, Article 83 (Fines/Penalties section), "GDPR Fines / Penalties." https://gdpr-info.eu/issues/fines-penalties/.

5. IBM. *Cost of a Data Breach Report 2025*. IBM, 2025. https://www.ibm.com/reports/data-breach.

6. Deepstrike. "Dark Web Data Pricing 2025." *Deepstrike Blog*, 2025. https://deepstrike.io/blog/dark-web-data-pricing-2025.

7. Verizon. *2025 Data Breach Investigations Report*. Verizon, 2025. https://www.verizon.com/business/resources/Tc91/reports/2025-dbir-data-breach-investigations-report.pdf.

8. Cybersecurity Ventures. "60 Percent of Small Companies Close within 6 Months of Being Hacked." *Cybersecurity Ventures*, January 2, 2019. https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.

9. KnowBe4. *The Economic Impact of Cyber Attacks on Municipalities*. KnowBe4, 2020. https://www.knowbe4.com/hubfs/Economic-Impact-of-Cyber-Attacks-on-Municipalities.pdf.

10. Forbes Technology Council. "Unplanned Downtime Costs More Than You Think." *Forbes*, February 22, 2022. https://www.forbes.com/councils/forbestechcouncil/2022/02/22/unplanned-downtime-costs-more-than-you-think/.

11. Viewpoint. "When the Unthinkable Happens: Contractor Shares Lessons Learned from a Ransomware Attack." *Viewpoint Blog*, October 1, 2021. https://www.viewpoint.com/blog/when-the-unthinkable-happens-contractor-shares-lessons-learned-from-a-ransomware-attack.

12. Associated Press. "Schools Face Rising Ransomware Attacks and Data Breaches." *AP News*, July 11, 2023. https://apnews.com/article/schools-ransomware-data-breach-40ebeda010158f04a1ef14607bfed9b0.

13. Google Cloud. "M-Trends 2025: Insights from Frontline Threat Intelligence." *Google Cloud Blog*, May 7, 2025. https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025.

14. Shields. "Notice of Data Security Incident." Shields Health Care Group, March 28, 2022. https://shields.com/notice-of-data-security-incident/.

15. Romanosky, Sasha, David A. Hoffman, and Alessandro Acquisti. "Why Data Breaches Don't Hurt Stock Prices." *Harvard Business Review*, March 27, 2015. https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

16. Johnson, Thomas. "The Devastating Business Impacts of a Cyber Breach." *Harvard Business Review*, May 17, 2023. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.

17. National Institute of Standards and Technology (NIST). *Cybersecurity Framework 2.0: NIST Cybersecurity White Paper*. NIST, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

18. Huntress. "Cybercrime Trends." *Huntress Blog*, August 2025. https://www.huntress.com/blog/cybercrime-trends.

19. Baker Donelson. *Cost of a Data Breach Report 2025*. Baker Donelson, August 22, 2025. https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf.

20. Spacelift. "Data Breach Statistics." *Spacelift Blog*, July 2025. https://spacelift.io/blog/data-breach-statistics.

21. BigID. "The True Cost of a Data Breach in 2024 and Beyond." *BigID Blog*, February 2024. https://bigid.com/blog/the-true-cost-of-a-data-breach-in-2024-and-beyond/.

22. AV-TEST Institute. "Malware Statistics & Trends." *AV-TEST*, 2025. https://www.av-test.org/en/statistics/malware/.

HUNTRESS

About Huntress

Huntress is a global cybersecurity company on a mission to make enterprise-grade products accessible to all businesses. Purpose-built from the ground up, Huntress' technology is specifically designed to continuously address the unique needs of security and IT teams of all sizes. From Endpoint Detection and Response (EDR) and Identity Threat Detection and Response (ITDR) to Security Information and Event Management (SIEM) tools and Security Awareness Training (SAT), the platform provides targeted protection for endpoints, identities, data, and employees, delivering trusted outcomes and valuable peace of mind.

Its 24/7, AI-assisted Security Operations Center (SOC) is powered by a team of world-renowned engineers, researchers, and security analysts, dedicated to stopping cyber threats before they can cause harm. Huntress is often the first to respond to major hacks and incidents, with its expert security team sharing real-time tradecraft analysis and actionable advisories with the community. Currently safeguarding over 4 million endpoints and 7 million identities, Huntress empowers security teams, IT departments, and Managed Service Providers (MSPs) worldwide to protect their businesses with enterprise-grade security accessible to everyone.

As long as hackers keep hacking, Huntress keeps hunting. Join the hunt at www.huntress.com and follow us on X, Instagram, Facebook, and LinkedIn.

HUNTRESS