HUNTRESS

The Real Cost of Identity-Based Attacks

A business leader's guide to understanding the risks of identity threats, the numbers behind them, and the cost savings in proactive security.

Table of Contents

Introduction

Why identity security can't wait

Your usernames, passwords, and login info are more valuable than diamonds to today's cybercriminals. Hacking into one device might only get them data from that machine, but stolen credentials are like VIP passes, giving attackers full access to networks and cloud environments.

Worse, these credentials are easy to find on the dark web, creating a low-effort, high-reward win for malicious hackers. With valid credentials, they can move through systems, escalate access, and create hidden backdoors to stay undetected. Basically, one compromised password can lead to countless opportunities for cybercrime.

If you're a business leader, it's no longer a question of if an identity-based attack will come for you, but when. And if you're not prepared, the consequences can be dire.

And the stats are alarming. For example, a global survey by RSA focused on cybersecurity and identity and access management experts found that over 20% of respondents estimated identity-related data breaches cost their organizations more than $10 million in the last three years.[1]

Identity-based threats are changing how attackers operate, making identity security a must-have for all businesses. These threats impact your bottom line, disrupt operations, and challenge competitiveness.

This ebook is your guide to understanding identity-based threats and how to take action. Backed by research from a range of trusted sources, it makes one thing clear: **the time to act is now**.

2x
more expensive

That's how identity-related breaches compare to the average data breach, according to 21% of respondents[1]

$10M+

What one in five cybersecurity experts say an identity-related breach cost their organization in the past three years[1]

HUNTRESS

The identity threat landscape:

You'll need more than a new password

Identity-based attacks are getting more advanced. Hackers aren't just guessing passwords anymore. In fact, Huntress found that over 35% of organizations said that advanced identity threats were responsible for more than 40% of their security incidents last year.[2] These attacks use a mix of tactics, including:

$50k Median amount for a single BEC incident[3]

40% Share of incidents driven by identity threats for over one-third of orgs[2]

$6.3B+ Amount transferred in BEC attacks in 2024, according to the FBI's Internet Crime Complaint Center (IC3)[3]

Credential theft and session hijacking:

Attackers now use advanced infostealers to grab credentials, session cookies, and access tokens in seconds, skipping the weeks of effort it used to take to break into networks the old-fashioned way.

Phishing and social engineering:

Verizon found that the median time for users to fall for phishing emails is less than 60 seconds.[4] That's about 20 seconds to click a malicious link, then only another 30 to enter credentials!

Account takeovers:

Huntress has found that more than 75% of account takeovers originate from VPNs, proxies, and tunnels, making detection incredibly challenging with traditional security tools.

Adversary-in-the-Middle (AiTM) attacks:

As the name suggests, these sophisticated attacks allow hackers to intercept authentication sessions, bypassing multi-factor authentication (MFA) entirely.

Business email compromise (BEC):

Tactics like modifying inbox rules give attackers a foothold to steal credentials, siphon email data, and disrupt business communications. The FBI found that in 2024 alone, over $6.3 billion was transferred due to these attacks.[3] On top of that, Verizon revealed the median amount for a single BEC incident was about $50,000.[2]

HUNTRESS

The overlooked costs of identity attacks

When data breaches make the news, it's usually all about the big, flashy numbers. But the real cost of identity-based attacks goes way beyond just the immediate cleanup. Let's break it down.

Direct financial losses

Nearly a third of organizations estimate at least $100,000 in losses from identity attacks, with over 50% reporting losses of at least $50,000.[2] But these figures are the tip of the iceberg.

Business disruption

According to RSA, over 40% of respondents said they experienced an identity-related security breach in the past three years. Of those, 66% described it as a "severe" incident that impacted their organization.[1]

Extended recovery times

Only 12% of organizations surveyed by IBM said they've fully bounced back from data breaches.[1] The lasting effects of identity-based attacks can disrupt operations, damage customer trust, and hurt market position for years.

Talent and resource strain

Organizations dealing with security breaches often struggle with a shortage of cybersecurity talent. When teams are stretched too thin, vulnerabilities are easily overlooked, giving threats a chance to sneak in. This not only makes incidents more likely but can also worsen their financial and operational impacts.

Regulatory and compliance costs

As data protection regulations grow stricter worldwide, identity breaches can lead to hefty fines and ongoing compliance costs, adding to the initial impact of the breach.

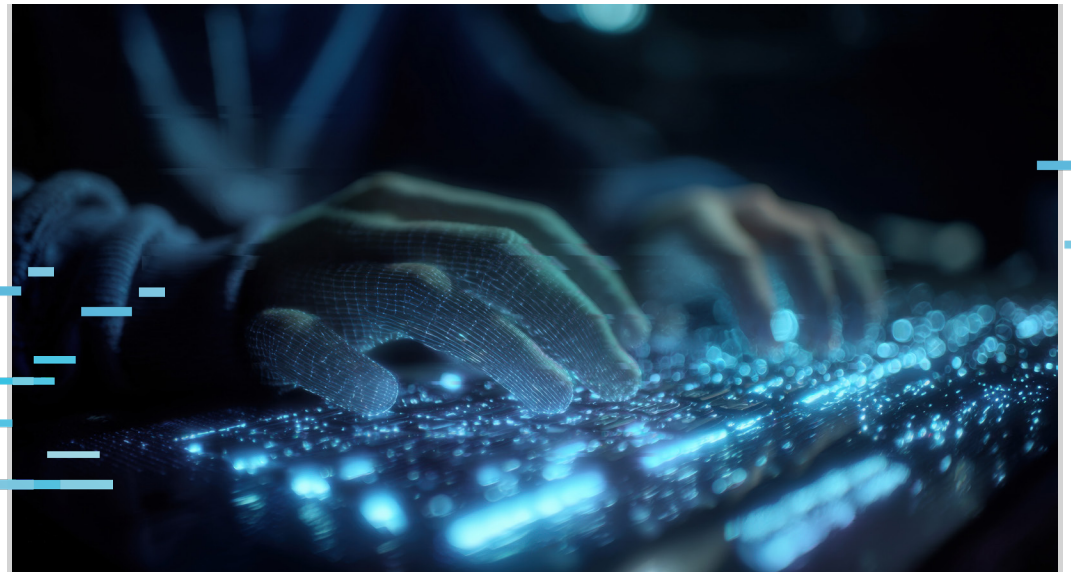
$100k+ Losses from identity attacks reported by nearly one-third of organizations[2]

HUNTRESS

The detection challenge:

Why speed matters

Huntress' latest research reveals a troubling trend: identity threats often go unnoticed for far too long. Nearly 70% of organizations fail to detect or respond to these threats until attackers have already gained a foothold and established persistence within their systems.



20% can't detect threats until data exfiltration occurs

5% don't know about attacks until after the incident is over

5% need weeks before detection happens

~50% can detect attacks within hours

16% need days to identify threats

Delays in spotting an attack can lead to bigger problems and higher costs. The longer an attacker stays hidden in your system, the greater the risk of data breaches, further system damage, and increased financial fallout.

HUNTRESS

How Huntress Managed ITDR transforms your security posture

Tackling identity threats might seem daunting, but with the right solution, it doesn't have to be. Huntress Managed ITDR (Identity Threat Detection and Response) simplifies identity security by addressing the key challenges most organizations are up against.

100% of users would recommend Managed ITDR to a friend or colleague

98% of users say they have no regrets choosing Managed ITDR

7M+ Identities protected under Managed ITDR

HUNTRESS

Managed ITDR Gives You:

Speedy response

With response times within minutes, Huntress can detect and stop identity-based threats before they escalate. Without managed threat hunting, it can take days, if not months, to detect credential-based breaches, and the business value becomes clear.

Minimal false positives

With a false positive rate of less than 5%, your team won't be overwhelmed with alerts that turn out to be nothing. This efficiency directly impacts productivity and resource allocation.

Expert coverage

24/7 expert-driven threat detection by our elite team of AI-assisted security operations center (SOC) shuts down identity-based attacks before they escalate. This means you get enterprise-level security expertise without the enterprise-level staffing costs.

Comprehensive protection

From session hijacking and credential theft to account takeovers and BEC, Huntress provides coverage across the full spectrum of identity threats that can impact your business.

HUNTRESS

The business case for business leaders

Whether you're the one making decisions at your organization or can influence the folks who do, it's important to keep these key points in mind when looking at identity security investments:

Identity is the new endpoint

Hackers aren't only looking at devices. They're looking at credentials with hungry eyes. With 89% of organizations planning to focus on identity protection in the coming year and 74% set to implement ITDR within 12 months,[2] identity is far more than a security trend—it's the new security perimeter.

The math is clear

With the average cost of a credential-based breach reaching millions,[1] even a modest investment in identity security delivers significant ROI by preventing incidents before they occur.

Time is of the essence

Every day without proper identity monitoring gives attackers more time to do damage, increasing the chances of serious reputational harm and financial losses.

Skills-gap remedy

Rather than competing for in-demand security talent, managed identity security gives you immediate access to specialized expertise and coverage.

Business enablement

Modern identity security doesn't slow down business operations. It gives you a faster, more secure digital transformation and collaboration abilities.

HUNTRESS

Minimize your risk and boost resilience today

Identity security isn't a challenge that's going away anytime soon, and the cost of doing nothing about it keeps rising. But for organizations that take a proactive approach, this challenge can actually become a competitive edge.

With today's evolving threats, the orgs that thrive will be the ones that see identity security as more than just protection. It's a business enabler and a force multiplier that helps you onboard customers faster, collaborate safely, and respond to threats in minutes instead of months.

To go even deeper into the benefits of identity protection, download Huntress 2025 Managed ITDR Report.

If there's anything to take away from all this, it's that the risks are clear, the solutions are available, and the benefits speak for themselves. Ready to secure the identities that keep your business moving? Give Huntress Managed ITDR a try.

Start your free trial of Managed ITDR now.

[1] RSA. (2025). 2025 RSA ID IQ Report. RSA Security. https://www.rsa.com/id-iq/

[2] Huntress. (2025). Huntress 2025 Managed ITDR Report: Identity Is the New Security Perimeter. Huntress. https://www.huntress.com/resources/managed-itdr-report-2025

[3] Verizon. (2025). 2025 Data Breach Investigations Report. Verizon https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

[4] Verizon. (2024). 2024 Data Breach Investigations Report: Executive summary. Verizon. https://www.verizon.com/business/resources/reports/2024-dbir-executive-summary.pdf

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 6.7 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