

The True Cost of a Cyberattack

How Threat Detection and Response Can Prevent Financial and Reputational Damage for Small- and Mid-Sized Businesses



Table of Contents

Introduction

Cyberattackers have small- and mid-sized businesses in their crosshairs	4
Cybersecurity gaps by the numbers	5

Challenges

Cyberattacks are becoming more costly and complex for SMBs to resolve	7
Cyberattacks are expensive	8
Cyberattacks hurt your reputation	11
Cyberattacks risk sensitive data	13

Solutions

Detection and response are critical for SMBs	17
Why are detection and response so important?	18
Common detection and response solutions	19
Using managed solutions to stay ahead of evolving threats	21
Fight back against hackers with Huntress	25



Introduction



Cyberattackers Have Small- and Mid-Sized Businesses in Their Crosshairs

The unfortunate truth is this: hackers now see small- and mid-sized businesses (SMBs) 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 largely to economic circumstances, many SMBs' defensive resources are becoming limited, putting their cybersecurity budgets on the chopping block.

This can lead to tragic outcomes. What many SMBs 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.

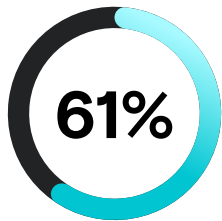
Quite simply, data breaches can lead to major financial losses for your business. Customers may leave you. Your reputation may suffer. And your duty to remediate—along with other liabilities—may add up at a stunning rate.

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

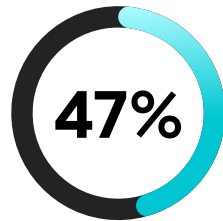
This eBook reveals the evolving risks and solutions SMBs need to know. Read on to learn how to protect your business from the fallout of cyberattacks.

Cybersecurity Gaps by the Numbers

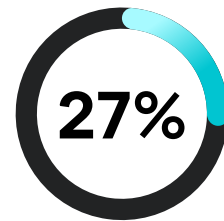
Research from the Huntress report, *The State of Cybersecurity for Mid-Sized Businesses in 2023*¹, revealed the following resource gaps for mid-sized businesses:



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 actors 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.

¹ www.huntress.com/resources/the-state-of-cybersecurity-for-mid-sized-businesses-in-2023

The word "Challenges" is centered on a dark teal background. It is surrounded by several horizontal teal lines of varying lengths and positions, some above and some below the text, creating a decorative effect.

Challenges

Cyberattacks Are Becoming More Costly and Complex for SMBs to Resolve

Some cybersecurity solutions may be out of reach for SMBs. In fact, they're bundled to include features most SMBs don't need or can't justify paying for. The cost of cyber insurance may seem equally high.

These price tags can leave organizations like yours underserved, unprepared, and vulnerable. However, if a cyberattack occurs, 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), breaches of Personally Identifiable Information (PII) can result in fines of up to \$50,000 per violation.

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

\$50,000

Maximum HIPAA fine for data breaches of personal information, per violation



Cyberattacks Are Expensive

If you aren't prepared to identify and stop a cyberattack before data is compromised, you're on the hook financially.

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

Regardless of your industry, a successful attack on an SMB comes with heavy financial costs, whether direct or indirect.

Directly, hackers may demand high sums of money, threatening to divulge data publicly or use it in other malicious ways if your company doesn't pay. Even for SMBs, 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 the standard advice of the US Federal Bureau of Investigation (FBI) is to **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.

\$250,000+	Amount that 20% of mid-sized businesses paid to recover from a cyberattack ²
51%	Percentage of small businesses that fall victim to ransomware and pay cyberattackers the ransom ³
60%	Approximate number of small businesses that shut down within six months of a cyberattack ⁴
\$65,000	Average cost of downtime on a local government after a cyberattack ⁵

These numbers indicate that cyber defenses are crucial to protect businesses.



² https://www.prweb.com/releases/nearly_2_3_of_mid_size_organizations_suffered_ransomware_attack_in_past_18_months_according_to_uncommonx/prweb18292350.htm

³ <https://www.strongdm.com/blog/small-business-cyber-security-statistics>

⁴ <https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/>

⁵ <https://www.knowbe4.com/hubfs/Economic-Impact-of-Cyber-Attacks-on-Municipalities.pdf>

Real Attacks

A road contractor had to rebuild over 200 computers and five months of data after an attack.



Road and bridge contractor E.R. Snell suffered a ransomware attack when malicious actors gained access via an employee's email account.⁶ The attackers snuck a key-logger on an on-premise mail server to secure administrative access, encrypted 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.

⁶ <https://www.viewpoint.com/blog/when-the-unthinkable-happens-contractor-shares-lessons-learned-from-a-ransomware-attack>

Cyberattacks Hurt Your Reputation

When a data breach occurs, 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.





Minneapolis Public Schools lost staff and students after hackers dumped more than 300,000 files online in a sweeping ransomware attack.⁷ 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 reputation damage.

⁷ <https://apnews.com/article/schools-ransomware-data-breach-40ebeda010158f04a1ef14607bfed9b0>

Real Attacks

A public school lost student and faculty trust after a traumatizing data dump.



Cyberattacks Risk Sensitive Data

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 the maximum amount of damage.

Research from 2023 shows the global median dwell time from compromise to discovery is 16 days.⁸ That means malicious actors could be within your environment for much longer—and the longer they sit unnoticed, the more damage they can cause.

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, such as stress, anxiety, and trauma.



⁸ <https://www.mandiant.com/resources/blog/m-trends-2023>

Real Attacks

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

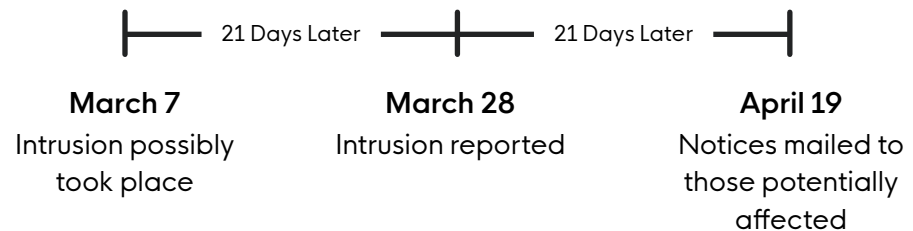


Shields Health Care Group, an imaging services provider for more than 50 healthcare facilities, experienced a breach involving the healthcare data of two million individuals.⁹

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 significant 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.



⁹ <https://shields.com/notice-of-data-security-incident/>

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*.¹⁰

It posits a lack of market response to enterprise-level breaches was due to shareholders not having sufficient information or tools to measure impact.

By 2023, another HBR article, *The Devastating Business Impacts of a Cyber Breach*¹¹, reveals an apparent change. It reports breaches result in an average stock price dip of 7.5%, with market cap losses in the billions.

These losses were suffered by companies with extensive resources to resolve impacts. Unfortunately, most SMBs don't have this level of financial might. For SMBs, existing resources need to stretch further and lift harder.

As data breaches gain more serious attention, SMBs 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

¹⁰ <https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices>

¹¹ <https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach>

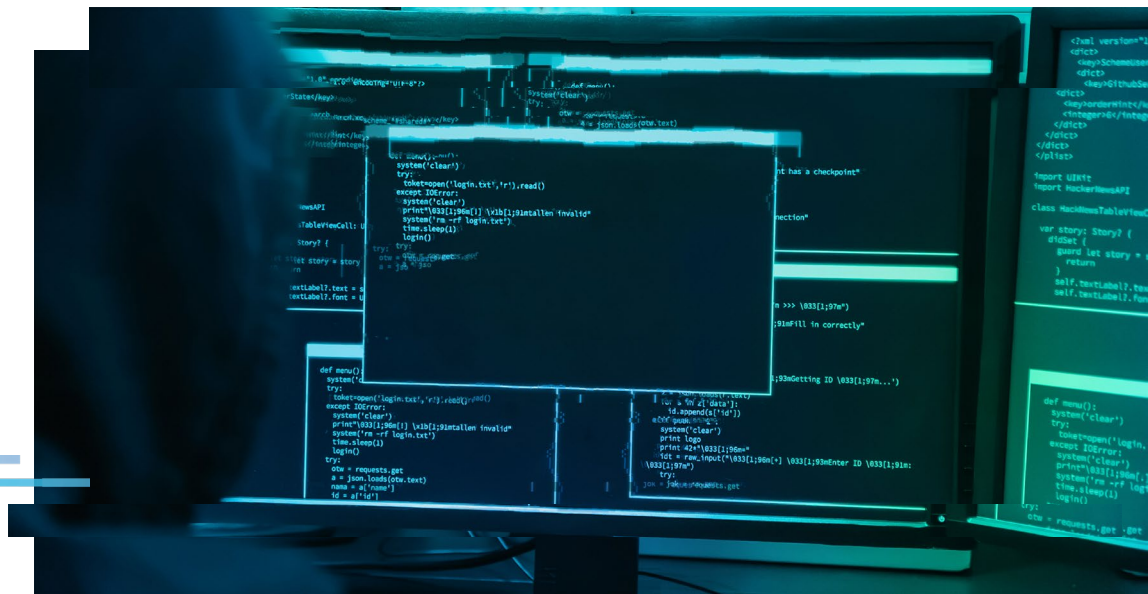
Solutions

Detection and Response Are Critical for SMBs

We've discussed how SMBs can be caught off guard by cyberattackers, resulting in serious losses. In most cases, we see this happen when businesses are missing the "detect" and "respond" components within their layered security stack.

While prevention-based technologies, such as antivirus and firewalls, play an important role in obstructing attackers in their attempts at initial access, they shouldn't be the only lines of defense. There are solutions designed to detect, isolate, and respond to malicious actors from SMB environments—without the heavy costs associated with enterprise solutions.

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



Why Are Detection and Response So Important?

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

The Cybersecurity Framework from National Institute of Standards and Technology (NIST)¹² illustrates how layers of security solutions should work together to minimize the risk of cyber threats. It focuses on five core components:



Identify



Protect



Detect



Respond



Recover

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

Detection and response are twin pillars that fortify the security posture of any organization. They serve as the early warning system and swift reaction force, respectively, 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.

¹² <https://www.nist.gov/cyberframework>

Common Detection and Response Solutions

Your business needs more than just prevention. That's where detection and response solutions come in. There are a few popular solutions that can provide these capabilities, mainly endpoint detection and response (EDR) and managed detection and response (MDR).



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 individual devices such as computers, 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 Detection and Response (MDR)

MDR takes a proactive approach to cybersecurity by combining advanced technology with human expertise. This solution involves outsourcing your day-to-day tasks of threat monitoring, detection, and response to a dedicated team of cybersecurity professionals. MDR providers leverage sophisticated tools and intelligence to continuously monitor your organization's environment, ensuring that potential threats are identified and neutralized before they escalate.





Real Attacks

A retailer stops business email compromise before hackers can manipulate invoices.

A retailer experienced a Microsoft 365 business email compromise (BEC) attack where a malicious actor assigned themselves privileges and permissions, likely to manipulate invoices and divert funds.¹³

With the help of Huntress' MDR for Microsoft 365 solution, suspicious logins were flagged from areas uncommon to the business, including Nigeria and Ireland. Experts from Huntress' security operations center (SOC) analyzed rare user agents and eradicated the threat before hackers could direct invoice payments to their own bank accounts.



¹³ <https://www.huntress.com/blog/business-email-compromise-via-azure-administrative-privileges>

Using Managed Solutions to Stay Ahead of Evolving Threats

With rising pressures on SMBs, a managed security solution can save **time, money, and resources**.

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 SMBs don't always have.

This requirement for expert tuning can leave SMBs at a considerable 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 that's backed by a 24/7 SOC that supplements your security team.

SOC experts manage and triage alerts for your business, helping you remediate as necessary. 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 your ability to catch and stop threats before they can inflict damage.



Time

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

Speed is crucial to cybersecurity because:


277 Days

The average time to recover from a security breach¹⁴

23% Less

Recovery in <200 days costs 23% less than recovery in >200 days¹⁵

A managed solution can provide cybersecurity expertise to cast a wider net and catch known and unknown threats. With a solution that provides real-time insights, teams can catch threat activity earlier and act quickly to wipe out identified threats. This can reduce dwell time so that hackers can't linger and cause more damage.



¹⁴ <https://www.ibm.com/reports/data-breach-action-guide>

¹⁵ <https://www.itpro.com/security/ransomware/ibm-law-enforcement-helped-save-ransomware-victims-dollar470k-in-2023>



Money

SMB decision-makers may believe managed solutions are too expensive. For example, they may choose an EDR just to check the box for insurance.

But incident costs justify the cost of a managed solution:


\$2.98M

The 2022 average recovery cost for a company of <500¹⁶

\$164

The 2022 average per-record cost, the highest in seven years¹⁷

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



¹⁶ <https://prowritersins.com/cyber-insurance-blog/average-cost-of-a-data-breach/>

¹⁷ <https://prowritersins.com/cyber-insurance-blog/average-cost-of-a-data-breach/>

Resources

SMBs aren't typically backed by the full force of a 24/7 SOC. Overextended teams may miss alerts and mishandle events. Put simply, a lack of resources can leave SMBs vulnerable to attack.

350,000

Approximate number of new malware programs created daily¹⁸

277

Number of days hackers may linger in environments¹⁹

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

¹⁸ <https://securityintelligence.com/posts/antivirus-evolution-to-face-modern-threats/>

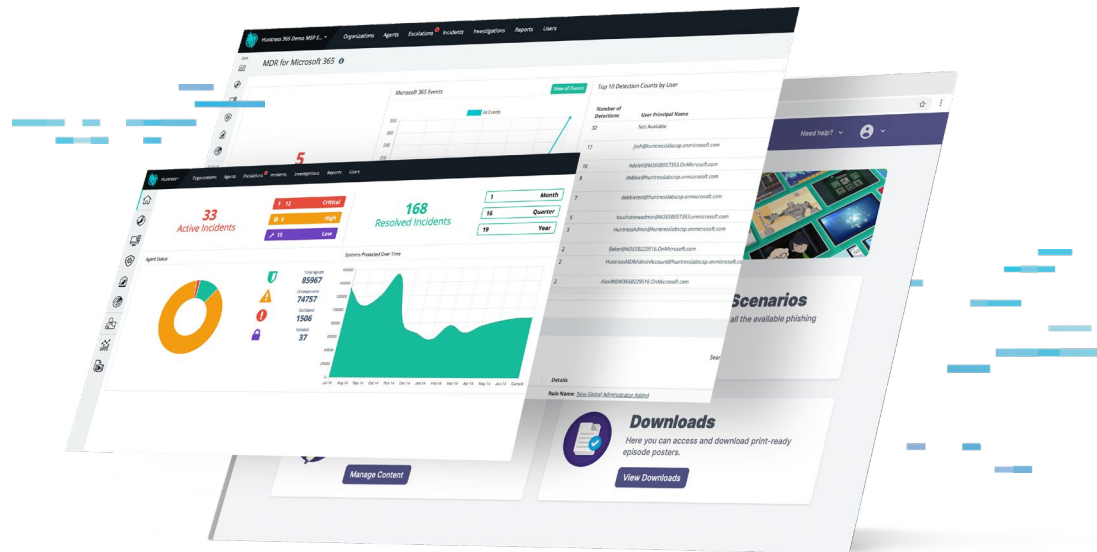
¹⁹ <https://www.ibm.com/reports/data-breach>

Fight Back Against Hackers with Huntress

There are many cybersecurity solutions out there, but most are built for enterprise companies. Their hefty price tags reflect all the extra bells and whistles. SMBs don't need all these features—or their pricing.

Huntress is a champion for SMBs, providing the technology, services, and expertise to help you overcome your cybersecurity challenges and help you make confident decisions that move your company forward.

Huntress provides ease of use and simplicity, so SMBs without a full-fledged IT team can keep up with known and unknown security threats.




Real Attacks

Huntress restored business operations for an SMB client in 30 hours.



For Clear Guidance Partners, Huntress caught an active ransomware incident in its tracks and helped protect a client's critical data.

Huntress Managed EDR and the Huntress SOC team discovered and confirmed malicious activity on a Clear Guidance Partners' client network, including network scans and malicious scripts missed by their antivirus solution. The Huntress SOC provided personalized remediation steps, activating Huntress' Host Isolation feature to isolate the infected hosts and prevent further access for bad actors. As a result, Huntress helped restore business operations within 30 hours.



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 even nonexistent. Hackers are fully aware of these vulnerabilities. And they're more than willing to take advantage of them.

No matter how sophisticated they seem, hackers are simply thieves. They just want your money, and they'll gladly jeopardize your business, your employees, and your sensitive data just to procure some loot. Should you be 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 SMBs 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 SOC, staffed with real experts who always have your back.
- Neutralize endpoint threats quickly and easily with Huntress Managed EDR.
- Keep your Microsoft 365 environments safe from BEC and other account takeover threats with our Huntress MDR for Microsoft 365 solution.
- Learn about the latest threats and take advantage of advanced training with Huntress Security Awareness Training.

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



About Huntress

Huntress is the leading cybersecurity partner for small- and mid-sized businesses (SMBs) and the managed service providers that support them. Combining the power of the Huntress Managed Security Platform with a fully staffed 24/7 Security Operations Center (SOC), Huntress provides the technology, services, education, and expertise needed to help SMBs overcome their cybersecurity challenges and protect critical business assets. By delivering a suite of purpose-built solutions that meet budget, security, and peace-of-mind requirements, Huntress is how SMBs defend against cyberattacks.

Founded in 2015 by a group of former National Security Administration (NSA) operators, Huntress has more than doubled over the past couple of years to protect more than 2 million endpoints, supporting 3,800 partners and more than 115,000 organizations. The company recently closed a \$60M series C led by Sapphire Ventures. For more information, visit huntress.com or follow Huntress on social media at @HuntressLabs on Twitter, Facebook, or LinkedIn.

HUNTRESS.COM

