

The Huntress Advantage

How Huntress Protects SMBs



Table of Contents

Introduction	3
The Managed Security Platform for SMBs Secure your endpoints, email, and employees	6
Unmatched Human Expertise Our intelligence isn't artificial	22
Commitment to Community A true partner in the fight against cyber threats	26
Training & Cyber IQ Knowledge sharing and education for all	33
Partnering with Huntress Managed security backed by dedicated expertise	39
Next Steps	43

Introduction

For years, cybersecurity was viewed only as an enterprise problem. After all, big businesses had all the tech, cash, and sensitive data—plus their reputations—to protect. Attackers knew this and spent most of their time targeting major retail outlets, healthcare providers, financial institutions, and the like. And when one of those targets was successfully breached, it captured mainstream media attention.

Today, things are different.

Businesses of **all sizes** are now completely reliant on technology—and at the same time, bad actors have a far more advanced set of tricks and tools at their disposal. This evolution has placed small and mid-sized organizations squarely in attacker crosshairs.

It's created an unfortunate perfect storm that looks something like this:



Small businesses are technology-dependent, but don't know how to manage IT—and don't understand cybersecurity well enough to protect themselves. Without any budget to hire (nor any ability to retain and grow) security talent, they're fish in a barrel for today's cybercriminals.



Mid-sized organizations often have some internal IT staff and may possess a working knowledge of security—but despite being more mature than their small business counterparts, they too struggle to assemble and manage the complex web of software and human layers that are needed to fight back against determined attackers.



To overcome these challenges, both small and mid-sized businesses will partner with an outside party—generally a managed service provider or value-added reseller—to fill in gaps and acquire the capabilities needed to defend themselves.



Those capabilities tend to be elastic and can scale up or down as needed (overcoming upfront cost barriers), and also place the burden of talent management and expertise on the third party (overcoming workforce and knowledge barriers). Importantly—and often underappreciated—is the fact that these capabilities must address a wide array of security needs that span the full lifecycle of an attack. To truly defend itself, a business must be able to determine: where potential weak points in its infrastructure exist, when an attacker is attempting to infiltrate their environment, when they've successfully done so, when an attack has been carried out, what level of damage has occurred, whether a bad actor has been successfully removed from the environment and whether systems can safely be restored to a pre-attack state. **That's a lot to manage.**



And here's the kicker: those third-party partners? They're also struggling to stay ahead of the curve, often relying on a myriad of disconnected tools and services that are too noisy, tell incomplete stories, or leave gaps in the fence that clever attackers can climb through. And they too face many of the same staffing and skill shortage challenges, given the high demand (and low unemployment rate) of today's cyber talent. That means there's nobody working to ensure that service providers and resellers are empowered to actually deliver on the promises they're making to their customers.



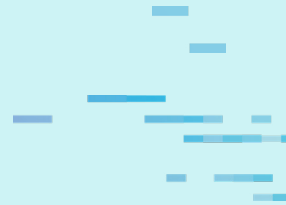
Given these substantial hurdles, how can SMBs properly navigate their cybersecurity pain points, such as greater attack surfaces, scarce resources and expertise, and increasing regulatory requirements?

Huntress is how.





The Managed Security Platform for SMBs



Secure Your Endpoints, Email, and Employees

Huntress, the leading cybersecurity partner for small and mid-sized businesses, provides the technology, services and expertise to help SMBs overcome their cybersecurity challenges and make confident decisions to move their companies forward.

The breadth and depth of our security services—coupled with their ease of use and our total commitment to educating and enabling the community—make Huntress a unique partner in the fight against cyber attackers.



Managed EDR



MDR for
Microsoft 365



Security Awareness
Training



24/7 SOC



There's an interesting dynamic in cybersecurity: the more important it's become over time, the harder it's gotten to manage.

The fact remains that cyber attackers have small and mid-sized businesses in their crosshairs.

And these businesses are under siege. They might represent 99% of organizations in the US, but many still lack the tools, personnel, and knowledge needed to respond to modern-day cybersecurity threats.

In today's online world:

- Attack surfaces are greater
- Available resources and expertise are scarcer
- Regulatory requirements are increasing, as are the high costs of cyber insurance and recovering from an incident

Research shows that "among America's small business owners, only 56% said they are not concerned about being the victim of a hack in the next 12 months, and among those, 24% said they were 'not concerned at all'" [according to CNBC](#).

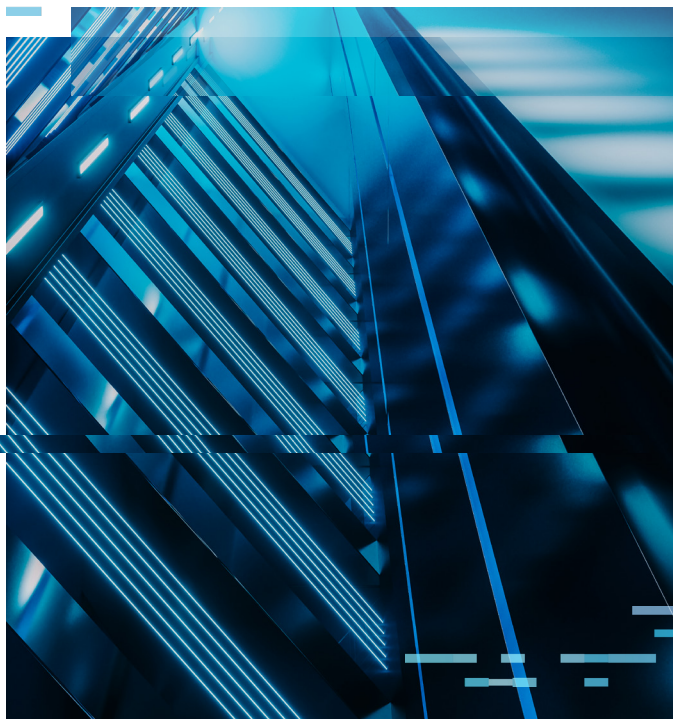
In response, businesses may look to IT or security “platforms” that offer more of a one-stop-shop experience with integrated technology, services, training, and enablement. Unfortunately, these platforms often present their own set of challenges: they require significant expertise or experience to manage, they generate an overwhelming volume of alerts, they deliver wildly inconsistent value across their various capabilities and they're expensive.

So, how can SMBs get the cybersecurity support they need to protect their organization?

Huntress is how.

The Huntress Managed Security Platform is built from the ground up to secure the businesses that need it most, like SMBs. It ensures users are focusing their attention on the things that actually matter and enables non-security professionals to effectively respond to cyberattacks and threats—all at a price that makes sense for the markets we serve.


The “managed” part refers to Huntress doing as much of the heavy lifting as possible—so you don't have to be a certified cyber professional to use it.





At its core, The Huntress Managed Security Platform enables users to:

- ✓ Identify open ports that can lead to potential exposures or easy entry points for attackers
- ✓ Identify, isolate and remove attackers who are attempting to break into their environments with near real-time detection and response
- ✓ Protect against a wide variety of viruses, trojans and related threats with a leading antivirus solution
- ✓ Detect ransomware faster, enabling businesses to respond swiftly and minimize the spread of attacks that can cripple entire organizations
- ✓ Detect advanced malware and persistence-enabled threats, which enable bad actors to maintain long-term access to a device or environment after they've bypassed other security systems
- ✓ Respond to all of these threat types with a combination of automated scripts and actions, handwritten incident reports with easy-to-follow instructions and an incredibly engaged support team that puts the security of our partners above all else
- ✓ Augment internal staff with a global team of highly capable threat analysts and researchers who deliver the crucial management layer of security that our partners are lacking
- ✓ Empower non-security professionals to level up their knowledge and education, and to easily and effectively leverage our platform—with no prior cyber experience required



For the first time, the cybersecurity answers are all immediately within reach for SMBs—and Huntress is how.

We've built our platform around a very specific set of pain points and pressures today's small and mid-sized businesses are facing.

Huntress is how our partners are able to achieve these three important business outcomes:



1 Eliminate Noise and Clutter

Security tools can be **loud**. They're constantly scanning, observing, and trying to determine if something is benign or malicious. That often leads to a ton of alerts and tickets being generated, many of which are false positives or notifications that don't require attention. It also forces businesses to have dedicated security personnel who babysit these systems, sifting through queues and trying to find the important needles in the haystack. That model might be manageable in the enterprise, but not in the SMB.

Huntress removes the haystack.

By manually reviewing all suspicious activity and detections, our 24/7 SOC team ensures that our partners are only receiving alerts for items that require their attention—with clear distinctions between low- and high-priority items, simple execution of recommended automations, and easy instructions for any manual work that's needed.

2 Bridge the Cyber Skills Gap

When trying to solve for cybersecurity, there's a tough reality SMBs are facing: they can't possibly hope to afford, hire, or retain the talent needed to build an effective security team. There's absolutely zero unemployment in the cyber world, and top talent gets snapped up by large enterprises that can afford to pay big bucks in an increasingly competitive market.

Huntress solves this problem in two ways.

First, the Huntress 24/7 SOC team absorbs all of the hunting, investigating, and analysis of suspicious activity—freeing our partners from having to build that internal cyber team and giving them back valuable time to focus on other aspects of their businesses. When incidents do occur, our Assisted Remediation and handwritten incident reports make it easy for users to respond to an attack—even when facing something they've never encountered before.

Second, we dedicate a ton of time and resources toward providing valuable education. With a constant stream of hands-on trainings and workshops, webinars and virtual events, tabletop exercises, and other resources, Huntress is how non-security professionals level up their skills and learn how to think like hackers.

3 Lower Total Cost of Ownership

All those great security features must be expensive, right? On the contrary, it wouldn't exactly align with our mission if we were building a platform that most SMBs couldn't afford.

This is where our meticulously crafted balance of automation, human threat experts, and enablement really shines. By zeroing in on the specific pain points and gaps found in SMBs today, we're able to keep our costs in check and deliver a tremendous amount of value at a price that actually makes sense for the markets we serve.

These are the core problems we aim to solve in everything we do and everything we build. Huntress is how our partners are able to address their top security concerns and find innovative, cost-effective solutions to overcome them.



Security That Fits Your Day-to-day

Our goal is to make life easier for defenders and harder for attackers. But how do we actually do that?

To start, we aim to deliver streamlined security in a way that doesn't add unnecessary complexity to our partners' daily operations. We've developed integrations so Huntress can report incidents and deliver step-by-step remediation instructions directly to your service board, ticket queue, email, or professional services automation (PSA) tool.

As our team reviews and investigates suspicious activity, we only alert our partners when a threat is verified, or some action is required—eliminating the clutter and false positives found in other platforms.

Plus, those reports are handwritten by our team of SOC experts to include clear, easy-to-follow instructions for manual tasks and one-click approval for automated actions. With easy access to alerts, reports, and remediation tools, even non-security professionals can swiftly respond to cyber threats using Huntress.

“

Staffing for security is always challenging. We've got talented techs on our team, but having a platform like Huntress makes it easier for us to respond to incidents—including things we haven't seen before.

We can follow the remediation steps and instructions we get via alerts, and our senior team can focus their time on forensics and investigative work. ”

James Otis
Binattech System Solutions

Leverage the Full Force of the Huntress Platform

With a powerful suite of managed protection, detection, and response capabilities, Huntress delivers protection that goes beyond the endpoint, extending to secure employees, identities, and inboxes.

Backed by a team of 24/7 threat analysts, The Huntress Managed Security Platform defends against ransomware, malicious footholds, business email compromise, and other threats to your organization's security.

The Huntress dashboard combines data and insights from each of our core solutions, providing a top-down view into active incidents and investigations—all delivered through a single interface. Simple enough for non-security professionals to quickly respond to cyber threats, yet powerful enough to oversee your entire attack surface.



Managed EDR

Visibility is key to detecting advanced endpoint threats. Huntress Managed EDR enables you to quickly identify and evict hackers with near real-time endpoint detection and response. By monitoring for malicious processes—and combined with data from other Huntress features—Managed EDR provides unparalleled visibility to weed out endpoint threats as they appear.

Key Benefits:

- Monitor continuously for process executions and associated metadata to increase visibility and make it harder for hackers to hide
- Detect attacks at the source and capture threat actor activity between initial access and desired impact
- Get near real-time forensics with the Huntress 24/7 SOC team who will hunt for threats in your network in the event of an incident

[Learn More](#)

“

In today's threat landscape, EDR is a must-have for protecting our clients. Huntress Managed EDR gives us increased visibility into our endpoints and networks in a way that easily integrates into our technology stack. Additionally, Huntress automatically tunes itself and does not add substantial cost for our business. ”

Anthony Cabral
Clear Guidance Partners



Managed EDR Included Features



Persistent Footholds

Eliminate persistent threats and malicious footholds hiding in plain sight on Windows and Mac devices.

[Learn More](#)



Managed Antivirus

Make the most of your frontline virus protection with Microsoft Defender, managed by Huntress.

[Learn More](#)



Ransomware Canaries

Catch potential ransomware incidents early and quickly respond to minimize downtime.

[Learn More](#)



External Recon

Highlight external vulnerabilities and expose easy entry points before hackers find them.

[Learn More](#)



MDR for Microsoft 365

Huntress Managed Detection and Response (MDR) for Microsoft 365 offers the ultimate solution for Microsoft 365 identity security and protection against business email compromise (BEC) attacks. In addition to monitoring the Microsoft 365 infrastructure in real-time, MDR for Microsoft 365 can identify and respond to various types of security events, including unauthorized access to the system, suspicious email rules, and deviations from security guidelines.

Key Benefits:

- Protect the security of Microsoft 365 users and respond to suspicious user activity, permission changes, and anomalous access behavior
- Receive 24/7 incident analysis and remediation guidance from the Huntress SOC team
- Save time and money with our around-the-clock, human-intelligence-powered detection and response solution, so you can focus on your core business

[Learn More](#)

“
Having a true managed service for email security is a game changer. We were able to resolve an issue within minutes with the help of the 24/7 SOC team. Partnering with Huntress has exceeded our expectations, and we can feel the impact they’ve made in our work.”

Matt Robins
Rudick Innovation and Technology

Security Awareness Training

Sharpen your employees' defenses using training episodes, assessments, phishing simulations and reporting—all a part of Huntress Security Awareness Training (SAT). This program empowers your employees with training that works and drives results, emphasizing constant vigilance and monitoring so that employees can play an active role in your organization's cybersecurity defense.

Key Benefits:

- Take part in training that actually reflects the types of threats businesses are facing today
- Learn specific tactics attackers are using when targeting your organization so that you can keep employees ahead of the curve
- Deliver a powerful—and fun—combination of episodes, assignments, simulations and reports to help employees become more cybersavvy

Learn More



“
Huntress SAT's episodes are enjoyable, even for IT to watch, as well as for other employees to learn. The content is so good, people get excited about it. Our security program was rewarded by building trust between our information security team and our employees.”

Kendra Cooley
Webflow

Security Operations Center (SOC)

The Huntress 24/7 SOC team is the backbone of the entire Huntress platform—and your secret weapon in the fight against hackers. This team of always-on experts takes care of the heavy lifting with 24/7 threat monitoring, world-class support, and step-by-step remediation guidance to help you effectively respond to cyber threats.

Key Benefits:

- A highly trained team of experts who understand exactly how hackers operate
- Around-the-clock threat monitoring and investigation into potential threats, removal of false positives, and creation of custom incident reports that help you remediate verified threats
- Ongoing analysis of hacker tradecraft and new threats to improve our capabilities and keep you ahead of the curve

[Learn More](#)

“
Huntress filters out all the noise. Their SOC team does a remarkable job of verifying threats and only sending alerts when they need our attention or action. Our techs know that when an alert from Huntress comes through, they better look at it.”

Tom Noon
Blue Tree Technology

Other Tools For The Hunt

Fast, easy deployment management. 24/7 expert services and support. Real-time alerts and one-click remediation. Ongoing education and enablement. Elite, proven cybersecurity expertise.

Together, our key features are enabling SMBs to move forward in their cybersecurity journey with confidence— and **Huntress is how.**



Host Isolation

This provides the ability to quickly block incoming and outgoing network activity on infected hosts—significantly reducing the chances of a network-wide cyberattack. During isolation, which can be triggered manually or automatically, the host will be isolated from the organization's network—only allowing connectivity between Huntress and the isolated host. And once isolated, the Huntress 24/7 SOC team will provide assisted remediation steps to resolve the incident and get the host(s) back online.



Assisted Remediation

This feature arms our partners with the ability to combat hackers at the click of a button. Assisted Remediation takes our incident reports a step further by providing partners with one-click execution of any Huntress-provided remediation steps that we can automate. This allows partners to respond to incidents faster—especially when encountering a threat they haven't seen before.



Branded Reports

There's a big catch-22 in security—the better you are at protecting your clients, the less they're going to "see" the value of your offering. To fix that, Huntress includes brandable threat reports that highlight all of the behind-the-scenes activity that's taking place. With these detailed summaries and reports, our partners can accurately measure (and articulate) the value they're getting from Huntress.



Unmatched Human Expertise

Our Intelligence Isn't Artificial

Modern attackers are smart. They're always coming up with ways to masquerade their malicious code, slip past traditional tools, or fool algorithms into letting their malicious program through. How can you expect to beat that?

Huntress is how.

Our 24/7 SOC team is integral to our success. They're trained experts with vastly different backgrounds, including digital forensics experts and leaders with military cybersecurity experience (from places like the Department of Defense, US Coast Guard Cyber Command, and Air National Guard). These diverse minds enable us to do what we do best: hunt hackers down. And they provide a degree of contextual awareness, analysis, and expertise that software-only solutions simply can't match.

When our SOC team investigates something suspicious, they dig in to determine exactly how, where, and why that activity is present. And once they do, we often discover even more than what was initially flagged. The best part? They're enriching every alert we send with their analysis and the actionable intel needed to respond to those verified threats.

Huntress' threat analysts aren't just responding to active incidents—they proactively hunt for potential exposures, notifying our partners about new vulnerabilities and identifying ways to help harden their security policies. They look for emerging threats and attack patterns that are designed specifically to bypass cyber defenses. And the intelligence they gather is fed right back into the Huntress platform—so our software and our hunters are constantly getting smarter.

“

When it comes to threat hunting, humans and automation should complement each other. We simply cannot rely on one over the other because they each have a part to play.

Automation is great for certain aspects, such as catching and flagging known malware patterns. But a human analyst can decipher what is truly malicious or spot a command that was designed to evade antivirus. In my opinion, threat hunting is strongest when you have automation and human analysis working together. ”

Cat Contillo
Security Operations Analyst Team Lead



Huntress 24/7 SOC in Action



Collect

The Huntress agent looks in all the places hackers use to hide, monitoring to threat actors who abuse legitimate applications, bypass other security tools, or are in the process of deploying payloads like malware and ransomware.



Analyze

We move beyond automated detection with contextually aware manual analysis from our SOC team. Our security analysts review endpoint and agent surveys to pick up on shady hacker tactics and catch even the sneakiest threats.



Report

After investigating, a member of our SOC team creates a unique incident report to share their findings surrounding any active breaches or attacks in progress. These reports offer simple, easy-to-understand analyses of threats and their severity—and they explain exactly what steps need to be taken next.



Remediate

Our detailed incident reports are designed to help our partners respond swiftly, and many of the remediation steps we outline can be automated and executed in a single click. Plus, we'll provide detailed recommendations for any other work that should be completed and can step in to help isolate ongoing attacks and minimize damage.



Commitment to Community



A True Partner in the Fight Against Cyber Threats

Our commitment to the broader cybersecurity community is a huge part of our team's mission to provide SMBs with elite, accessible cybersecurity expertise.

To do this, we venture well beyond our platform to respond to industry incidents and events as they're happening. We engage and partner with others who also strive to make the cybersecurity space a better place. Plus, we provide quality cybersecurity training and education for cybersecurity enthusiasts of all knowledge levels.



Navigating Large Industry Incidents

There's one certainty in the world of cybersecurity—
and that's uncertainty.

What starts off as a normal morning can quickly morph into a day of putting out cyber fires, researching, patching—doing everything but sleeping. And unfortunately, we've seen an increase in the number of these events over the last few years.

The Huntress 24/7 SOC team is packed with experts who know how to distill the important action items during active incidents to help the community respond. We know we have a unique set of skills and brainpower at Huntress, and we're committed to using our knowledge for good. From analysts to researchers, our SOC team members are consistently in the trenches, helping partners and the community at large deal with cyber incidents.

Below is a sampling of the type of response Huntress enacts during an active cyber threat.



3CX

3CX is a business communication solution and software that uses Voice Over Internet Protocol—or VoIP—that leverages the internet to transfer phone calls instead of the copper lines of traditional phone systems.

In March 2023, [the 3CX VoIP Desktop Application became compromised](#), delivering malware via legitimate 3CX updates. In response, Huntress immediately added increased monitoring for malicious activity related to the 3CX application, while working to validate this attack vector so that we could provide as much information as possible.

In total, the cyberattack affected more than 600,000 3CX customers, making it a massive supply chain attack. Within our partner base, Huntress sent out 2,783 incident reports where a 3CX desktop application was detected and matched known malicious hashes. At the time, we had a pool of nearly 8,000 hosts running 3CX software.

Because there was a risk of taking phone communication systems offline, we decided not to automatically isolate all 3CX hosts. Instead, we notified the appropriate partners and urged our customers to remove the software if at all possible.



MOVEit

MOVEit is a managed file transfer software product that encrypts files and uses secure File Transfer Protocols to transfer data, as well as provides automation services, analytics, and failover options.

In June 2023, we were made aware of [active exploitation attempts against the MOVEit application](#). As a result, its parent company, Progress, brought down the MOVEit Cloud as part of its response and investigation.

Immediately we fully recreated the attack chain that was exploiting MOVEit and uncovered the initial phase of the attack was SQL injection. This unfortunately opened the door for further compromise, namely arbitrary code execution. That meant we had to work fast to avoid opportunities for ransomware attacks or other malicious actions that could disable antivirus protections and other arbitrary code execution.

We ended up identifying less than 10 organizations in our partner base with the compromised MOVEit software. From those, only one saw a full attack chain. Because of the attack's severity, Huntress offered its Managed EDR service at no charge for newly deployed endpoints for the entire month.

Progress has since urged users to update MOVEit Transfer Software to one of five different patched versions to stop further malicious activity.



LOG4J

The [log4j vulnerability](#) sprung up so quickly that whiplash was nearly unavoidable. And the worst part? This critical vulnerability impacted a significant amount of software, including Apache, Apple iCloud, Steam and Minecraft—just to name a few.

While this vulnerability didn't impact the Huntress platform, our team still spent countless hours researching the threat and providing updates to the community on how they could best mitigate it. We also dedicated an entire [Tradecraft Tuesday episode](#) to covering the latest intel and helping the community navigate this major incident.

Our security researchers teamed up with MSP community member Jason Slagle to develop a Log4Shell Vulnerability Tester, which helped organizations determine which applications on their systems were vulnerable to Log4Shell. This tool empowered community members to evaluate their systems to assess their risk levels to the vulnerability and work to mitigate the threat.

Threat actors have been busy—and so have we since we opened our doors in 2015. But at the end of the day, our goal has been to raise the tide and help the cybersecurity community get better at what they do. And that won't change.

To read more of our rapid response and threat analysis content, head over to our [blog](#).



Giving Back

Our commitment to the cybersecurity community will never stop at our platform. We'll always extend our efforts beyond what we do at Huntress to help the community get better together. We'll continue to find new ways to give back—whether it's helping to navigate new shady activity in the wild or partnering up with organizations just as concerned about the greater good of the community as we are.

We've invested countless hours in the cybersecurity community—but as they say, sometimes you have to put your money where your mouth is. And we were fortunate enough to be in a position to be able to do that in January 2022.

We **announced** a \$100,000 donation to the Dutch Institute for Vulnerability Disclosure (DIVD), a volunteer-led organization with a team of highly skilled security researchers who analyze threats and report vulnerabilities globally. This donation helped fund the organization's continued growth, enabling the first full-time staff to be hired, and it helped DIVD start a bug bounty program to incentivize finding and disclosing bugs in MSP and SMB IT tools.

The coolest part? We weren't alone in our efforts for very long.

Seven of our fellow MSP vendors were fast to step up to the plate and ask how they could get involved—and within a few weeks, we'd secured an additional \$75,000 thanks to our peers in the MSP vendor community.

Training & Cyber IQ



Knowledge Sharing and Education for All

A rising tide raises all ships. How can business owners and IT professionals attain the right actionable security training, education and awareness?

Huntress is how.

This is captured in two central ways:

- 1 Our platform makes it easy for users to respond to security incidents, regardless of how technically savvy they are. No advanced training or certifications required.
- 2 We provide a continuous stream of threat analysis and training to help our audience sharpen their skills and better understand the attackers they're fighting against.

There are several ways we deliver on these commitments, including:



Knowledge

A huge chunk of what we do consists of developing materials and hosting various events—all in the name of cybersecurity education. Here are a few ways we do that.

Tradecraft Tuesday

On the second Tuesday of every month, we host live webinars that highlight recent security news, offer hands-on demonstrations of offensive and defensive security techniques, and more. These are purely educational in nature—no products, no pitches; just tradecraft. [Check out Tradecraft Tuesday here.](#)

hack_it

A multi-day training event with sessions geared toward both technical and non-technical audiences. Hack_it events occur 1-2 times per year, include external speakers and infosec experts, and offer more networking and user interaction than some of our other events. [Binge all our previous hack_it sessions here.](#)

Actionable Threat Analysis

Beyond live events and webinars, we regularly publish written analysis and commentary covering new threats and attacks, unique malware variants and more. These writeups help our readers understand the threats they're facing, and in many cases show them exactly what, how, or where they should be investigating to combat them. Examples can be found [here](#), [here](#), and [here](#).

Resource Library

Want to step up your cybersecurity knowledge and expertise? We'll show you how. Access our library of eBooks, webinars, videos, and more to delve into the latest hacker tradecraft, cybersecurity trends, and security technologies. Resources include:

Blogs

Our [blog](#) is a great place to start if you're on the hunt for educational resources. Specifically, the [cybersecurity education](#) category features an assortment of blogs that cover a variety of cybersecurity topics. If you want to dive deeper into what happens during some of our investigations, head over to our [threat analysis](#) category.

Educational Content

Our content library covers everything from how to build an effective cybersecurity stack to how MSPs can lead their customers to success. One of our favorites is [The Ultimate Buyer's Guide to EDR](#), a comprehensive guide designed to help you find and select the right EDR solution for your business needs.

Webinars

Whether you want to hear peer-approved best practices or how best to respond during an active cyber incident, our webinars and on-demand events have you covered. Not sure where to start? Check out our [Understanding EDR webinar](#). It covers what the technology is, its capabilities, what role it plays in your security practice, and how Huntress Managed EDR might be the solution for you.

Success Kits

Our success kits are designed not only to help you level up your cyber knowledge but to put you and your team to the test. We recommend downloading our [Incident Response Tabletop-in-a-Box](#), a practical exercise to both build and test your incident response plan.

Platform

Fast, easy deployment and management. 24/7 elite services and support. Real-time alerts and one-click remediation. The Huntress Managed Security Platform is how SMBs, managed service providers, and their clients instantly elevate their cybersecurity with the lowest total cost of ownership.

Here are examples of product features that help us deliver on that goal.

Incident Reports

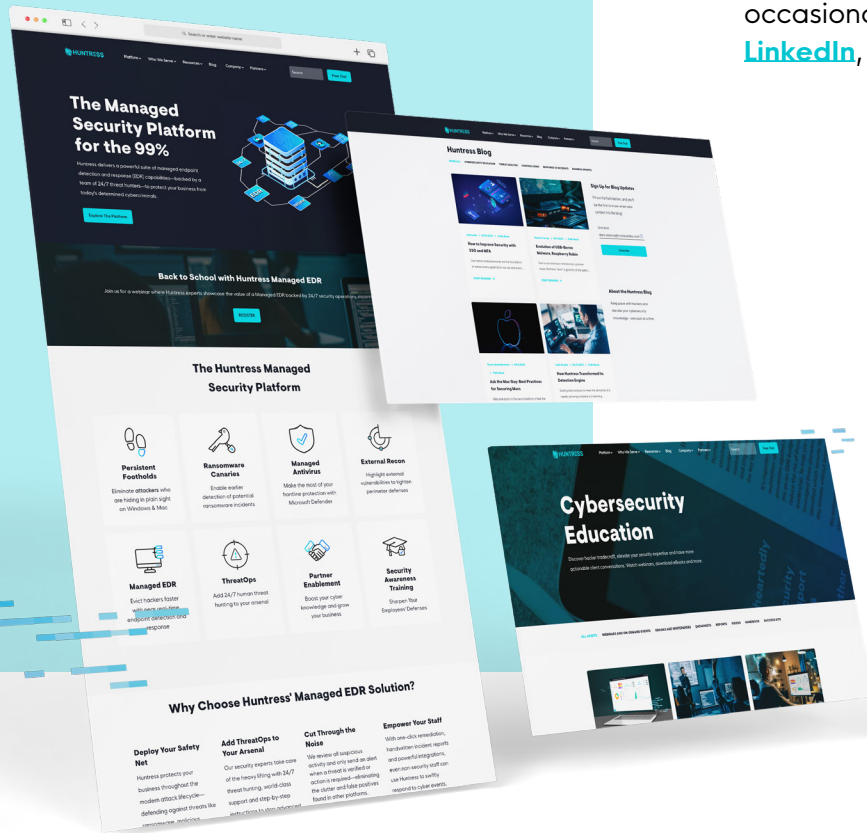
When the Huntress platform discovers an incident, a member of our 24/7 SOC team creates a unique report to send to the affected partner. These reports offer simple, easy-to-understand analysis of the threat and its severity—and they explain exactly what steps need to be taken next. By leveraging our expertise, partners can respond to threats they've never seen before or wouldn't otherwise know how to approach. Learn more about incident reports [here](#).

Assisted Remediation

This feature takes our incident reports a step further, providing partners with one-click execution of any Huntress-provided remediation steps that we can automate. This makes it even easier for users to respond to incidents, and fast. Learn more about assisted remediation [here](#).

Additional Resources to Help You Become More Cyber Savvy

[The Huntress website](#) will always feature our most up-to-date resources, so be sure to stop by often. We've also been known to drop some tips—and an occasional cyber-themed meme—on our social platforms. Connect with us on [LinkedIn](#), [Twitter](#), and [YouTube](#) for the latest.





Partnering with Huntress



Managed Security Backed by Dedicated Expertise

How can small and mid-sized businesses and the third-party resellers that manage their infrastructure get the support they need?

Huntress is how.

- ✓ We complement your toolset with powerful technical capabilities and features that don't conflict with your existing systems
- ✓ We complement your workforce with a team of 24/7 threat analysts and true cyber experts that address knowledge and skill gaps
- ✓ We complement whatever existing cyber knowledge you have with hands-on training, education, events, and other resources
- ✗ We **don't** complicate your defensive abilities with hard-to-use tools that demand cyber expertise
- ✗ We **don't** complicate your operations with confusing billing, weak documentation or lousy support
- ✗ We **don't** complicate your cyber response efforts by shifting blame, pointing fingers or idly standing by when something is on fire

“

It's not just the threat hunters at Huntress; it's the marketing team, the support team—holistically, the entire Huntress team is a partner to F1 Solutions. They're just as excited about my business as I am. ”

Jennifer VanderWeir
President, F1 Solutions



Huntress is How You Can Get...



Outstanding Support

The Huntress platform is intuitive and easy to use—but that doesn't mean our team isn't committed to providing top-notch support and hands-on help when it's needed. In addition to our support documentation, we regularly work with partners to dig into specific incidents and reports, provide security guidance and recommendations, and more.



Partner-Driven Innovation

Our partners are at the core of our roadmap. The features we invest in—and the way we build them—are specifically designed to address the gaps and pressures our partners are facing as attacks continue evolving. We're constantly listening, capturing feedback, running beta tests, and more.



Straightforward Pricing

No hidden tricks, gimmicks, or gotchas. Our pricing model is built around two core principles: delivering a highly valuable cybersecurity platform at a price that SMBs can afford and leveraging a tiered licensing model that enables our partners to earn appropriate margins based on the additional services and value they're layering in when securing their customers.

Next Steps

Now that you're basically an expert on who we are, what we do, and what we stand for, let's talk about where to go from here.

If curiosity got the best of you, and you're just here to learn about us, thanks for reading! We hope you'll stay in touch by connecting with us on social media or [dropping us a line](#). You can also check out our [upcoming events](#) to see where we're headed (physically and virtually). And if you see us at an event, say hi! We're just a friendly group of cyber nerds—promise.

If you're interested in seeing The Huntress Managed Security Platform in action, we recommend [attending a demo](#). You'll be able to explore the Huntress dashboard, learn more about our capabilities and features, and more. Chat live with our team and see what Huntress can do for you.

If you're interested in seeing The Huntress Managed Security Platform in action in your environments, we recommend [signing up for a free trial](#). During your trial, you'll get a first-hand look at the power of our managed platform backed by our team of skilled human threat analysts.

No matter which group you fall into, we hope this guide has given a good overview of what we're here to do and the how and why behind it.

We've been chasing down hackers since 2015—and we've got a lot more work to do.

Stay Secure and Happy Hunting,

Team Huntress



Let's Talk.

We're always happy to chat.

Send us a ping or email us at hello@huntress.com.

Schedule a demo to ask questions, chat live with our team and see the value Huntress can bring to your organization.

