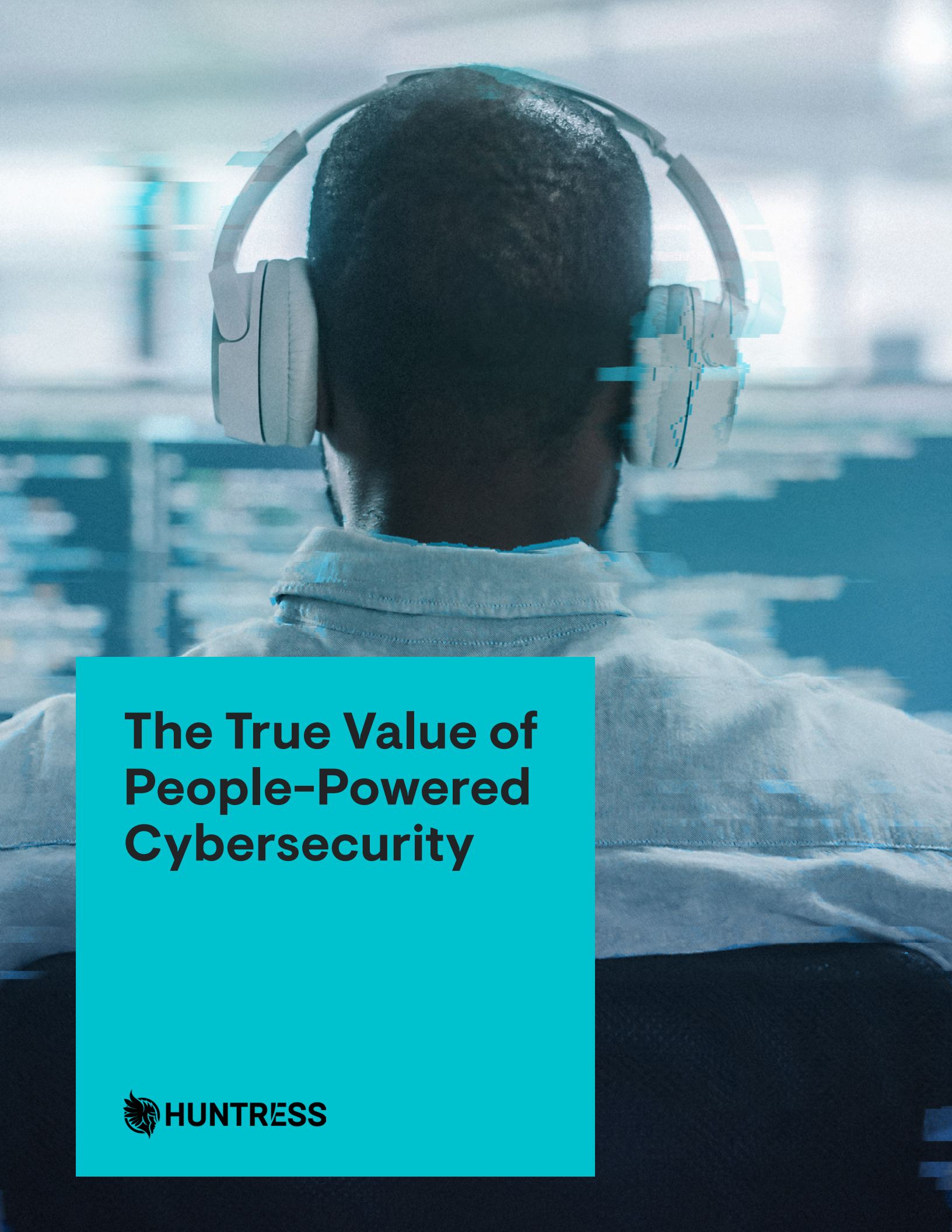


The True Value of People-Powered Cybersecurity

HUNTRESS

Cybersecurity moves fast, and it's become more difficult to manage. As attention to cybersecurity increases across organizations, so do the associated challenges. Every passing month brings more headlines about major attacks, while the rise in remote working adds an extra layer of complexity to security teams as they aim to secure a distributed workforce. A shortage of cybersecurity experts only compounds the issues facing IT teams.

With every passing year, cyberattacks are becoming more complex; hackers are constantly figuring out new ways to slip through defenses. In fact, 63% of decision-makers recognize this, citing it as the greatest reason behind their focus on cybersecurity[1]. If you are one of those decision-makers, you're feeling that pressure and it's likely why you've chosen to read this

Staying in the fight against today's threats requires the right resources, dedication and expertise. While that sounds a lot easier said than done, this paper aims to bring clarity to how that can be accomplished without breaking the bank, exhausting employees, or stressing out management.

Understanding Your Needs

Small and medium-sized businesses (SMBs) desperately need and want enterprise-level security, but unfortunately, that's all most security products have been built for: the enterprise. On top of that, those security tools often come with enterprise-sized price tags.

So how do SMBs ensure they are on top of their game and well-protected from sophisticated threat actors and advanced attacks if they are constantly **understaffed, under-resourced and dealing with budget pressure**? When taking into account that ransomware incidents are up by 13% just over the last year (with a total increase of 25% since 2017)[2], that can leave anyone feeling overwhelmed and under-prepared.

1 Vade, 2022 SMB Cybersecurity Landscape Report
2 Verizon, 2022 Data Breach Investigations Report

Let's take a look at the components mentioned and how they actually impact SMBs today.

	PAIN POINTS	REALITIES
Time	IT teams and employees are stretched too thin due to understaffing. Not enough time to deal with alerts and tuning security tools.	**60%** of incidents are discovered within days, and **20%** of incidents take months to find.[3] **27%** of security alerts are ignored or not investigated.[4]
Expertise	Many employees lack the knowledge needed to properly manage and configure security tools in-house. Employers are struggling to find and retain the cyber talent they need.	**13%** of breaches are caused by misconfiguration errors.[5] **3.5 million** cybersecurity jobs are unfilled today, and that number is expected to go up through 2025.[6]
Cost	Hiring and retaining security talent is expensive. The direct and indirect costs of security incidents are rising.	**$80,000** is the average annual salary for a Security Analyst.[7] **$115,000** is the average cost of a ransomware attack, not including factors like operational downtime, reputational damage, regulatory fines and legal fees.[8]

While those statistics are not meant to scare, they are jarring numbers. And they are a reality for many.

Businesses of all sizes are now completely reliant on technology; but at the same time, attack surfaces are greater, and available resources and expertise are scarcer. This evolution has placed small and mid-sized organizations squarely in attacker crosshairs.

3 Verizon, 2021 Data Breach Investigations Report
4 IDC, In Cybersecurity Every Alert Matters
5 Verizon, 2022 Data Breach Investigations Report
6 Cybersecurity Ventures, Cybersecurity Jobs Report: 3.5 Million Openings Through 2025
7 Salary.com, Security Analyst Salaries in the United States
8 Unit 42, 2020 Incident Response and Data Breach Report

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 an attack has been carried out
- What level of damage has occurred
- Whether a bad actor has been successfully removed from the environment
- Whether systems can safely be restored to a pre-attack state

That's a lot to manage on your own.

So how can SMBs get the expertise they need to rise to the challenge and move forward with confidence? **Huntress is how.**

Huntress: Your Partner in (Combatting Cyber) Crime

At Huntress, we aim to provide the cutting-edge technology, services and expertise businesses need to stand a fighting chance against today's cyber threats.

The reason Huntress exists is because we see a real need among the SMB community for affordable cybersecurity backed by true industry experts who not only talk the talk but walk the walk. The breadth and depth of our managed 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.

Earlier we discussed time, expertise and cost. Here's how Huntress addresses those pain points and empowers SMBs to fight back.

Reduce Noise. Save Time.

Burnout in this industry is a legitimate concern. While this also ties to the cyber skills shortage, if you can only afford so many employees to handle all the IT and security tasks for your business, burnout can and likely will result. Pair that exhaustion with alert fatigue and you've got a recipe for high turnover and possibly disaster.

Additionally, configuring security tools is time-consuming for those not well-versed in doing so. Even if analysts are experienced, configuration, tuning and automation can take up time. Especially if you are only just learning what your baseline looks like.

Consider all the work that is done when responding to an alert. Depending on the alert type, you may have to analyze a file (or multiple files), examine logs, examine registry data, etc. This can take up a lot of time, especially if you're seeing something new for the first time.

It doesn't have to be this way. Huntress can cut out that noise and save your company time and energy by handling alerts for you.

Your Problem	Huntress' Solution
Triaging alerts is taking up too much time. Should we hire more people?	So far in 2023, our dedicated analysts reported identified threats **in less than one hour** from our Managed EDR product. Additionally, **3 out of 4** times our analysts can investigate identified threats without our partners needing to take action—leaving them more time to focus on their business, and less time dealing with alerts.
Configuring and tuning this security tool is harder than we thought. Are we doing this right?	Huntress detections are automated, so assuming data is flowing properly, suspicious activity is automatically seen **within minutes of the event.**
We don't know how to investigate this alert. What if we miss something, and how do we handle a real threat?	Huntress enables your team to respond to alerts and incidents more effectively. When we report an incident, it has already been investigated and corroborated and believed to be malicious. Our incident reports include actionable and easy-to-follow remediation steps that can usually be **executed in one click.**

Tech- and People-Powered

Between the more than 2 million endpoints protected by Huntress and our talented Security Operations Center (SOC), Huntress has a wealth of collective intelligence.

We pride ourselves on having gathered the best minds in the cybersecurity industry—those who come from both the private sector and government, including (and certainly not limited to) Cisco, VMware, the Department of Defense, the US Coast Guard Cyber Command and the Air National Guard.

These diverse minds enable us to do what we do best: hunt hackers down. And the best part? We do it at scale. No matter if it's 50 endpoints or 50,000 endpoints, you'll always have our SOC experts in your back pocket.

Everything we see at Huntress is looked at and verified by a human, which means higher fidelity in the incidents we bubble up, as well as a more personal touch by the following SOC teams:

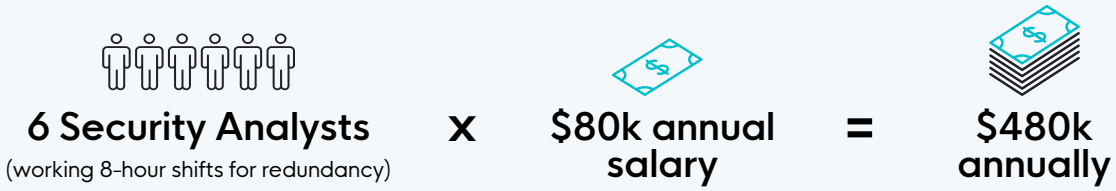
Team	Their Function	Ask Yourself
Detection Engineers	Detection Engineers help create new detections, as well as define logic or create analytics that will help identify compromises in our partners' environments.	Is this something my team can and knows how to take on?
Research and Development (R&D)	R&D works closely with Huntress engineers and product managers to ensure that new features and telemetry coming into the Huntress platform is helpful and viable. Additionally, they provide training so our analysts and threat hunters are constantly learning and have access to the knowledge they need, so they aren't missing detections or bad actors.	Do I have enough in-house staff or time to dedicate to threat research?
Threat Analysts	These individuals perform investigations, craft reports, triage and analyze alerts and respond to intrusions in our partners' networks. This team is located across the United States, the United Kingdom and Australia and is staffed to maintain 24/7 coverage.	Who will be available on Saturday night at 3am to investigate and respond to security events?
Threat Hunters	These individuals proactively search for compromises in environments with the objective of improving the overall Huntress platform and its detections.	Do I have a dedicated threat hunter on my team who knows what to look for?

All of the above is done independently of installing a Huntress agent on your endpoints. That means that when you partner with Huntress, not only do you get instant access to our world-class technology and talent, you also get eight years' worth of Huntress historical knowledge and ingenuity.

Our commitment to elevating the cybersecurity community does not stop at our platform. We regularly put out educational webinars, blogs, videos and other resources that share our expertise and help close the cyber knowledge gap.

Cost: How It All Adds Up

Building and retaining your own team of security experts is expensive. It would cost **almost half a million dollars annually** just to get the minimal amount of experience and coverage in-house that Huntress provides through our 24/7 SOC.



In addition to overhead, dealing with a cyber attack is becoming increasingly expensive and is putting more financial pressure on today's businesses.

The direct and indirect costs of an attack, including downtime and reputational damage, are significant, as are the expenses associated with complying with regulatory requirements and cyber insurance. As a result, businesses must spend more money to protect themselves, which can be a financial burden, especially for SMBs.

Key Findings and Final Thoughts

Again, we are not trying to use scare tactics in this paper to sway you one way or another. These are realities every company faces; the difference is the size of the company and how much capital they have to address these concerns effectively.

Choosing the right cybersecurity partner is an important step in your journey to keeping your business protected, but it is imperative that you select the one that best suits your needs.

Today's businesses must be able to rise to the cyber challenge, and Huntress is how. Huntress is built to provide the technology, services and expertise SMBs need to overcome their most pressing cybersecurity challenges. Our platform fortifies your defenses, anticipates your needs and evolves with the threat landscape—and our SOC is the secret sauce other tools cannot replicate.