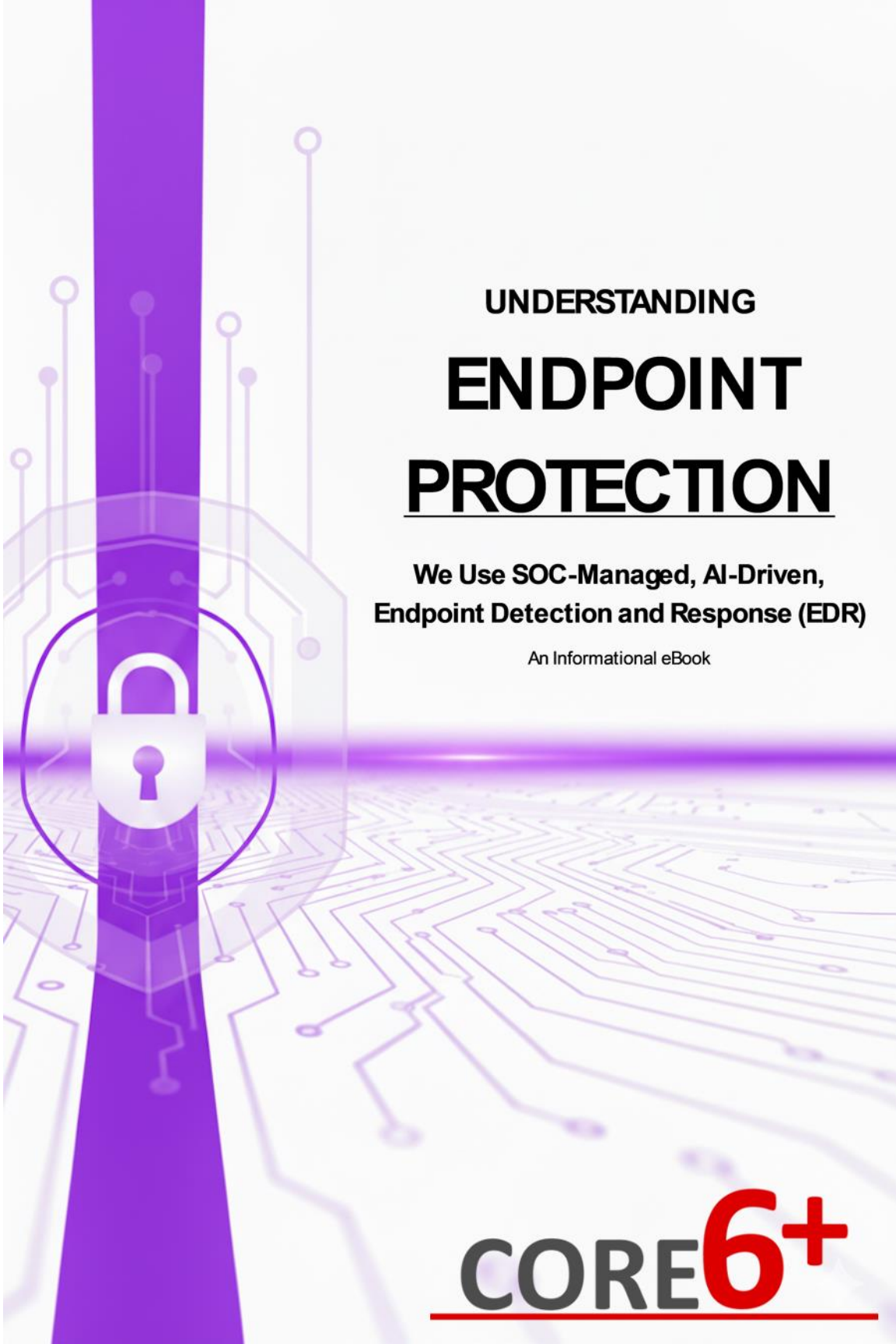

UNDERSTANDING

ENDPOINT PROTECTION

We Use SOC-Managed, AI-Driven, Endpoint Detection and Response (EDR)

An Informational eBook

CORE6+

UNDERSTANDING

ENDPOINT PROTECTION

We Use SOC-Managed, AI-Driven, Endpoint Detection and Response (EDR)

An Informational eBook

Table of Contents: The SOC-Managed EDR eBook

Chapter 4: The Core Benefits of SOC-Managed EDR

- **4.1 Proactive Threat Hunting: Finding Problems Before They Start**
- **4.2 A Digital Time Machine: The Ability to Roll Back a Ransomware Attack**
- **4.3 Fastest Incident Response: Minutes Matter When a Threat is Active**
- **4.4 A Smart Investment: Getting 24/7 Protection at a Fraction of the Cost**

Chapter 5: Conclusion

- **5.1 A Summary of What Matters Most**
- **5.2 The Peace of Mind: A Final Look at the Ultimate Benefit**
- **5.3 A Resilient Security Stance: How SOC-Managed EDR Protects Your Future**

Chapter 1: The Problem with Old Security

1.1 The Security Guard with a List: The Limitations of Traditional Antivirus

For decades, traditional antivirus (AV) software was a good-enough solution for protecting our computers. As a “Scan-Based” application, it worked on a simple principle: think of a security guard with a list.

Think of traditional antivirus as a diligent security guard standing at your computer's door. This guard has a massive book of known criminals—a "list of signatures"—and their one job is to check every person (or, in this case, every file) trying to get in. If the person's face matches one in the book, the guard blocks them. It was a seemingly effective system – until the list got too big to efficiently manage – but it only worked with criminals that were already in the book.

The problem is that today's cyber criminals are no longer already on the list. They are constantly creating new threats, new viruses, and new ways to sneak past the guard. When a new criminal shows up, the guard doesn't recognize them, and they are allowed to walk right in. It was a system that worked on what it already *knew*, not on what it *sees*.

1.2 The New Threats: Why Ransomware, Fileless Attacks, and Zero-Day Exploits Change Everything

The world of cyber threats has evolved far beyond simple viruses that get caught by an old-school AV system. Today's attackers are using sophisticated and sneaky methods that traditional AV was never designed to handle.

- **Ransomware:** This is perhaps the biggest threat to small businesses today. Ransomware is a malicious program that can encrypt all of your files and hold them hostage until you pay a ransom. Traditional AV often fails to stop it because the ransomware looks like a normal file until it's already running on your computer.
- **Fileless Attacks:** These are incredibly difficult for traditional AV to detect because there is no file to scan. These attacks use legitimate software and processes already on your computer to perform their malicious actions. It's like a criminal walking into your home and using your own tools to cause damage—the security guard has no idea what's happening.
- **Zero-Day Exploits:** A "zero-day" is a software vulnerability that is not yet known to the public or the security world. When a cyber criminal finds and exploits one of these, traditional AV has no signature to match it, and the threat goes completely undetected.

These new threats prove that the "security guard with a list" is no longer a viable defense. We need a new way of thinking about security that can see beyond the obvious and protect us from the threats we don't even know exist.

1.3 The Cost of Inadequacy: What Happens When Antivirus Fails

The cost of having inadequate security can be catastrophic for a small business or nonprofit. It's not just a theoretical risk; it's a very real financial and operational threat.

- **Financial Devastation:** The average cost of a small business cyberattack can be in the hundreds of thousands of dollars. This includes the cost of paying a ransom, data recovery services, and fines from a data breach.
- **Operational Shutdown:** A ransomware attack can completely lock down your business, preventing you from accessing your computers, your files, and your critical business tools. This can result in weeks of downtime and a loss of productivity that can be impossible to recover from.
- **Reputational Damage:** A data breach can destroy the trust you've built with your clients and your community. Once a reputation for security is lost, it can be very difficult to get it back.

The simple truth is that in today's world, an antivirus solution that is not a comprehensive EDR solution is no longer an adequate defense. It is no longer a question of "if" but "when" you will be a target.

Chapter 2: The Solution - EDR

2.1 What is Endpoint Detection and Response (EDR)?

If traditional antivirus is a security guard with a list, then **EDR (Endpoint Detection and Response)** is a complete, 24/7 security team with a cutting-edge surveillance system.

EDR is a new class of security solution that moves beyond simply scanning files for known threats. It installs a small software agent on every one of your devices—your laptops, desktops, and servers—and then it continuously monitors everything that happens on those devices. It's a system that is constantly watching, recording, and analyzing every action to find patterns that look suspicious. This is a crucial distinction. EDR doesn't just look for known criminals; it looks for **suspicious behavior**.

This constant monitoring and analysis of "endpoint activity" is what allows EDR to detect new and emerging threats that would easily slip past a traditional antivirus system.

2.2 The Full-Body Scan: A Simple Analogy for How EDR Works

Let’s go back to our security guard analogy. The old guard only checks a book of faces. EDR is more like a full-body scanner at a high-security checkpoint.

- The scanner doesn't just check for a person's name on a list; it looks for hidden objects, strange activity, and suspicious patterns.
- If a person is acting nervously, carrying a strange package, or trying to move through a restricted area, the scanner detects that behavior and raises an alarm. It doesn't need to know the person's name to know that something is wrong.

This is exactly how EDR works. It establishes a baseline for what "normal" activity looks like on your devices. It then uses advanced technologies like machine learning to look for **anomalies**—behaviors that are out of the ordinary. It can see a program trying to make a suspicious network connection, a file trying to modify a system registry, or a user account acting strangely. This ability to see beyond a static list is what gives EDR the power to detect threats that have never been seen before.

2.3 Beyond a Static List: How EDR Goes Further Than Antivirus

The difference between EDR and traditional antivirus is the difference between being **reactive** and **proactive**.

- **Antivirus is Reactive:** It waits for a file to be opened, checks it against its list of signatures, and if it finds a match, it quarantines it. If the file is new and has no signature, it does nothing.
- **EDR is Proactive:** It doesn't wait for a file. It is constantly monitoring for suspicious behavior. If a new, never-before-seen fileless attack or ransomware strain starts to run, EDR immediately sees the unusual behavior, raises an alarm, and takes action to contain the threat.

This fundamental shift in philosophy is what makes EDR the essential tool for modern endpoint security. It's not just a step up from traditional AV; it's a completely new approach to security that is designed to protect you from the threats of today, not the threats of yesterday.

Chapter 3: The SOC - The Human Element

3.1 Why Technology Isn't Enough: The Problem of Alert Fatigue

In the last chapter, we talked about how EDR is a powerful security tool that is constantly watching your devices for suspicious behavior. But what happens when EDR and other security tools start generating hundreds or even thousands of alerts every single day? This is a very real problem for modern businesses, and it's called **alert fatigue**.

Alert fatigue happens when an IT professional or business owner is overwhelmed by the sheer volume of security alerts. The vast majority of these alerts are false positives—a normal file that looks suspicious, a user that is performing a normal task, or a system that is simply misconfigured. After a while, all of these false alarms start to look the same. The IT professional becomes desensitized to them, and the risk of missing a real, critical threat in the noise becomes a very real problem.

Technology is great at generating alerts, but it's not always great at telling the difference between a real threat and a false alarm. That’s where the human element comes in. We need a human brain to make sense of all this data and to know when a true threat is emerging.

3.2 The Human Brain: The Value of a 24/7/365 Security Operations Center (SOC)

This is the key to a truly effective EDR solution. A **Security Operations Center (SOC)** is a team of cybersecurity experts who provide the human brain behind your EDR. This team is constantly monitoring all the alerts that your EDR generates, 24/7/365. They filter through all the noise, and they only escalate a real, critical alert to you when it matters. This is a crucial distinction. The SOC team is not just a passive observer; they are a team of proactive detectives who are constantly on the hunt for a threat.

Think of it like this: your EDR is a powerful security camera system that detects any motion. A stray cat walking by, a tree branch swaying in the wind, a delivery driver—the camera sees it all and generates an alert. The SOC team is the human brain that looks at all the alerts, and they know that a cat is not a threat, but a person trying to break in is. They filter out the noise and they only let you know when there is a real, critical threat.

This is the ultimate benefit of a SOC-Managed EDR solution. You don't have to worry about alert fatigue. You don't have to worry about missing a critical threat in the middle of the night. You have a team of experts that is constantly on guard, and they are only going to let you know when there is a real, critical threat that needs your attention.

3.3 From Alert to Action: The Process of Detection and Remediation

So, what happens when a real threat is detected? The SOC team is a rapid response team that turns an alert into an action.

1. **Detection:** Your EDR detects a suspicious behavior, such as a fileless attack or a new piece of ransomware.
2. **Investigation:** The SOC team is immediately notified, and they begin to investigate the alert. They use their expertise and advanced tools to determine if the threat is real or a false positive.
3. **Containment:** If the threat is real, the SOC team immediately isolates the affected computer from the network. They quarantine the threat and prevent it from spreading to other computers. This is a crucial step that can prevent a catastrophic attack from happening.
4. **Remediation:** Once the threat is contained, the SOC team works to remove it from the computer. This can include removing malicious files, restoring files from a backup, and patching any vulnerabilities that were exploited.

This is a real-time, human-in-the-loop process that is designed to turn a potential threat into a non-issue. It's a level of security that a traditional antivirus system could never provide.

Chapter 4: The Core Benefits of SOC-Managed EDR

4.1 Proactive Threat Hunting: Finding Problems Before They Start

Traditional security waits for a threat to strike and then reacts. **Proactive Threat Hunting** completely flips this script. It's not about waiting for an alarm to go off; it's about actively searching your network for threats that have slipped past your initial defenses.

Think of it like having a team of digital detectives who are constantly on the lookout for a threat. They are looking for subtle signs of suspicious behavior, unusual network activity, or a strange file that might be hiding in your system. This proactive approach allows a SOC team to find a threat, investigate it, and neutralize it before it can ever cause a problem. It's a fundamental part of an effective security strategy that finds the hidden threats that traditional antivirus systems would never see.

4.2 A Digital Time Machine: The Ability to Roll Back a Ransomware Attack

Ransomware is one of the most devastating attacks a business can face. It can encrypt all of your files and hold them hostage until you pay a ransom. But a SOC-Managed EDR solution has a powerful feature that can mitigate this threat: the ability to **roll back** a system.

Think of this as a digital time machine. If an EDR solution detects a ransomware attack, it can immediately isolate the affected computer and then revert it to its previous, uninfected state. This is a game-changing feature that can completely reverse the effects of a ransomware attack, saving you from paying a ransom and allowing you to get back to business without losing your valuable files.

4.3 Fastest Incident Response: Minutes Matter When a Threat is Active

When a cyber attack is happening, every minute counts. The average time it takes for an organization to detect a data breach is a staggering **197 days**, and it takes another **69 days** to contain it. This is a critical window of opportunity for hackers.

A SOC-Managed EDR solution drastically reduces this response time. It provides a 24/7/365 team of experts who can detect a threat within minutes, contain it within an hour, and begin to remediate the problem. This rapid response minimizes the damage, reduces recovery costs, and protects your business from a catastrophic shutdown. It's the difference between a small fire and a raging inferno.

4.4 A Smart Investment: Getting 24/7 Protection at a Fraction of the Cost

For a small business, building an in-house security team to provide 24/7 coverage is prohibitively expensive, often costing over a million dollars annually. A managed SOC, on the other hand, provides the same level of expert protection at a fraction of the cost. The average cost of a managed EDR solution is typically between **$10 and $20 per asset per month**, which is a fraction of the cost of a single security analyst.

This is a smart investment that provides unmatched value. You get access to the world's best security tools and a 24/7/365 team of experts, without the high cost of an in-house security department. It's a way of saying that you are taking your security seriously, without breaking the bank.

Chapter 5: Conclusion

5.1 A Summary of What Matters Most

We've taken a journey into the world of modern cybersecurity, moving from the outdated "security guard with a list" to a proactive, intelligent defense. As we bring this guide to a close, let's quickly summarize the most important takeaways about SOC-Managed EDR:

1. **Antivirus is No Longer Enough:** The threats of today—ransomware, fileless attacks, and zero-day exploits—are designed to bypass traditional antivirus. A new approach is a necessity, not an option.
2. **EDR is the New Standard:** Think of EDR as a full-body scan for your computers. It's a proactive security tool that looks for suspicious behavior, not just known threats.
3. **The Human Element is Crucial:** The SOC is the human brain behind your EDR. This 24/7/365 team of experts filters through all the alerts, ensuring that a real threat is never missed.
4. **You Have a Digital Time Machine:** In the event of a ransomware attack, SOC-Managed EDR can roll back a computer to its previous, uninfected state, saving you from paying a ransom and from losing your valuable files.
5. **It's a Smart Investment:** SOC-Managed EDR provides 24/7 protection and a rapid incident response team at a fraction of the cost of an in-house security department.

5.2 The Peace of Mind: A Final Look at the Ultimate Benefit

The ultimate benefit of SOC-Managed EDR is not just the technology or the team; it's the peace of mind. As a business owner or a nonprofit director, your time is your most valuable asset. You shouldn't have to spend your time worrying about cybersecurity, sifting through false alerts, or dealing with the aftermath of a breach.

With a SOC-Managed EDR solution, you can focus on what you do best: running your business and making a difference in your community. You can operate with the confidence that a team of experts is constantly on guard, and that a single careless click will not lead to a catastrophic shutdown.

5.3 A Resilient Security Stance: How SOC-Managed EDR Protects Your Future

In the end, SOC-Managed EDR is more than just a security tool; it's a strategic investment in a resilient security stance. It's a commitment to a proactive defense that protects your business from the threats of today and tomorrow. It's a way of saying that you are taking your security seriously, and you are not going to leave your business vulnerable. It's the new standard for small business and nonprofit cybersecurity.

Visit https://Core6Plus.com to learn more.

Your Strategic CyberSecurity Provider (SCP)

Core 6+ is your Strategic CyberSecurity Provider (SCP) — a partner focused exclusively on protecting your organization from today's ever-evolving cyber threats. Unlike traditional MSPs that primarily handle IT labor and computer fixes, Core 6+ delivers the world's best, proactive cybersecurity protection applications and defense tools through layered solutions like Gateway Protection, SOC-managed EDR, NOC-managed Daily Patching and Preventative Maintenance, Web Protection and DNS Filtering, Data Backups, and more. Core 6+ augments and works directly with your trusted IT support – whether that be internal staff or external contractor. Core 6+ wants to help augment your team by providing 24/7 real-time, all-the-time protection, Where You Want It Most — giving you the freedom to choose only what you need, at a price you can actually afford.

Traditional MSPs tend to - and often want to - live on one end of the service spectrum with fully "Done For You" services option, which always include high fees and retainers. Whereas, at the other end of that spectrum, where most small businesses and nonprofits are, the only option for cybersecurity protection seems to be: (Pay Way Too Much, or) "Do It Yourself" - literally leaving small businesses and nonprofits on their own, with no professional guidance, and with no real safety net.

Core 6+, as your SCP, bridges that gap. Giving organizations - of every size - the freedom to handle as much of their own IT and computer support as they want and have been doing for years. Core 6+ works with whoever your trusted IT support person is… And, if need be, Core 6+ can help you find local IT Partners to provide complete, hands-on service when needed.

With Core 6+, as your SCP, partnering with your trusted IT support you can get the perfect blend of CyberSecurity Protection, IT independence and the expert (augmented) backup support if, or whenever needed.