Making Everything Easier!™

Tripwire Special Edition

Endpoint Detection and Response

FOR DUMMIES®

A Wiley Brand

Learn to:

- Detect and respond to a breach before significant damage occurs
- Discover, assess, and monitor every endpoint
- Detect, analyze, and respond to advanced threat incidents
- Leverage industry and community-sourced threat intelligence

Brought to you by

tripwire

Ed Tittel
Gajraj Singh

About Tripwire, Inc.

Tripwire is a leading provider of endpoint detection and response, security, compliance, and IT operation solutions for enterprises, service providers, and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context. Together these solutions enable integration and automation across security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. The solutions are available on a broad range of platforms and are trusted and deployed on more than a million business-critical systems.

Tripwire's integrated suite of solutions can discover and assess the security of endpoint assets on organizations' networks, enabling real-time detection, analysis and response.

Tripwire's highly resilient endpoint defense solution includes a broad range of capabilities ideally suited for business-critical endpoints, servers, network devices, and the physical and virtual infrastructure that supports them.

Tripwire products are integrated with more than 70 third-party IT and security solutions that make it easy for customers to realize a better return on investment while automating a number of key processes that dramatically improve overall IT and security effectiveness.

Endpoint Detection and Response

FOR DUMMIES®
A Wiley Brand

Tripwire Special Edition

by Ed Tittel and Gajraj Singh

FOR DUMMIES®
A Wiley Brand

Endpoint Detection and Response For Dummies®, Tripwire Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-26231-2 (pbk); ISBN 978-1-119-26327-2 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz or visit www.wiley.com/go/custompub. For details on licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner
Acquisitions Editor: Amy Fandrei
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Production Editor: Tamilmani Varadharaj
Tripwire Reviewer: Shelley Boose

Introduction

Today's organizations face huge challenges securing and protecting servers, networks, and digital assets. This goes double for mobile users, as they — and their laptops, tablets, and other devices — traipse all over the place. Also, more organizations are moving IT workloads to the cloud, leveraging hosted and SaaS models. With an expanded definition of endpoints that includes any connected device, physical or virtual, it's good that cybersecurity solutions are available to help IT security organizations cope. Such solutions offer protection, monitoring, and support to secure business-critical assets and quickly respond to a breach.

Endpoint security refers generally to a well-described and understood method to protect an organization's data and network as accessed with end-user, connected devices. Today, that not only means laptops and tablets, but also smartphones and other wireless devices. Each device and its connection to the network creates a target and entry point for security threats. However, traditional endpoint security solutions can't keep up with conventional endpoints, let alone all the new "things" coming online in today's networks.

This book is called *Endpoint Detection and Response For Dummies*. It focuses on how to deploy and manage security for many kinds of endpoints. It also digs into how endpoints and security incidents are detected, identified, monitored, and handled, including effective response and remediation. It even discusses the key role of automation in detecting and responding to threats and managing risk. The abbreviation for this — you guessed it: it's EDR.

What's an "Endpoint," Really?

An endpoint is any connected device used to access an organization's data and network. Traditionally, IT pros interpreted this as "anything with a CPU and a keyboard." That definition is now expanding to include "things" (IoT, IIoT and OT), as new devices — even sensors — further increase the attack surface for businesses and organizations. Platforms considered infrastructure in the past now qualify as endpoints and are subject to exploitable vulnerabilities.

Thus, we need to expand our definition of an endpoint to include servers, mobile devices, kiosks, POS, HVAC, medical gear, industrial systems, cameras and, yes, even cars. With more systems — physical or virtual, on-premises or in the cloud — accessing organizational data and networks, the definition will be stretched even further — soon!

How This Book Is Organized

- **Chapter 1** introduces the security landscape in which endpoints operate, what they are, and how they work.
- **Chapter 2** shows what's involved in protecting endpoints, and how to address gaps in EDR coverage.
- **Chapter 3** explores the context in which EDR must operate, and how intelligence translates into action.
- **Chapter 4** explains security maturity models, extending security maturity to endpoints, and creating synergy with security frameworks.
- **Chapter 5** looks at processes, policies, and integration involved in EDR.
- **Chapter 6** provides important steps to follow as you put EDR to work in your organization.
- **Chapter 7** offers ten key points to remember on your path to EDR success.

Chapters are designed to stand alone, so to dig into EDR policies and processes, jump to Chapter 5. Otherwise, keep reading for a better intro to EDR in Chapter 1.

Icons Used in This Book

Each *For Dummies* book features small graphical widgets called *icons*. Scattered throughout the text in the margins, they flag paragraphs to help explain what makes them noteworthy:

This icon highlights points to keep in mind when you immerse yourself in the language and lore involved in EDR. These nuggets are worth noting!

This icon identifies useful info to help you make the most of any investment in EDR. Why not try putting it to work?

Some EDR topics are deeper and more detailed than others and may not be essential to your understanding. This icon tells you that you can skip the upcoming details, if you like.

This icon calls out situations, habits, or practices to avoid. Steer clear of danger!

Chapter 1

Understanding Endpoints

In This Chapter

- Surveying the threat landscape is supposed to be scary!
- Extending and stretching the definition of *endpoint*
- Changing the concept of *endpoint* so we can adapt and evolve
- Understanding EDR and what it does

For many IT and security professionals, a common definition for *endpoint* is something like "anything with a keyboard."

But in an increasingly digital and mobile connected world, with scads of devices seeking access to organizational networks, applications, and data, that definition doesn't include the security threat from the full range of employee-owned devices, virtual machines, point-of-sale terminals, IoT devices, and even servers and industrial systems.

But before we dig into endpoints in detail, let's get a sense of how scary the world outside the organizational boundary can be. Cybersecurity pros call this "the wild," where boogeymen and monsters constitute the "threat landscape."

Here Be Dragons!

Ever since computing got going in the 1940s and 1950s, systems have been subject to threats. Although they can come from bad guys, it's important to understand that simple mistakes from well-intentioned people pose threats, too. As business uses for computing have evolved, the threats that organizations face have evolved as well.

The network is open!

The debut of the PC in the early 1980s and the proliferation of the Internet in the 1990s opened many more points of attack. A huge market for online goods and services has also drawn serious crooks seeking to steal money or information into the mix, above and beyond those curious about how systems work (and how they can be subverted). These days, threats come in all shapes and sizes, from those interested in learning, to activists seeking notoriety, to hacktivists and digital vandals, to organized criminal outfits engaged in nation-state cyber espionage and cyber attacks, to criminals chasing easy bucks.

Increasing use of computers for critical business operation, e-commerce, point of sale, industrial and medical systems, and the Internet of Things — as well as Internet connectivity — has upped opportunities for cyber crime. Organizations store and transmit huge amounts of data — including confidential or proprietary information, customer data, credit card data, and all kinds of financial transactions — all of which pose tempting targets for threat actors.

Computer viruses and other malware (Trojans, worms, backdoors, keyloggers, rootkits, and more) have exploded in recent decades. Although early viruses were simple and fairly harmless, modern malware is sophisticated, dangerous, and destructive. Now, malware is a major tool for criminals and other bad guys after ill-gotten gains or sensitive information.

A threat tsunami

In an all-too-typical cycle, as computers and networks have evolved to improve security and productivity, threats have evolved right along with them. Because they can get access to just about anything, insiders also pose a big threat to organizations (possibly the biggest, according to the FBI and the National Cyber-Forensics and Training Alliance, aka NCFTA). Suffice it to say there is an ever-increasing array of threats on the landscape, many of which bring serious risks to organizations' economic health and well-being.

In April 2015, CNN Money reported that about 1 million new malware threats were appearing daily, based on reports from security teams at Symantec and Verizon. The number of threats with which organizations must cope is a veritable

tsunami. It often seems that thieves work faster than companies can react, launching an ever-increasing number of probes and attacks against organizations of all kinds.

What can you manage?

Historically speaking, most organizations focus their security efforts and defensive controls at the network boundary (or periphery), believing that this is the best way to fend off would-be attackers. But once the fox gets into the chicken coop, he gets a free run. Worse, although boundary controls may keep bad actors from outside from breaking in, this doesn't do anything to protect from internal threats. Ouch!

Security experts often talk about four elements when describing the security landscape. Let's look at each element, to identify which of these an organization can control or manage:

- **Asset:** An organization's hardware, software, apps, and information that should be tracked and audited.
- **Threat:** A person, agent, or thing likely to inflict evil, damage, or loss.
- **Risk:** A characteristic or situation that involves exposure to disruption, damage, or loss.
- **Exposure:** A quality or characteristic in a system, service, or software that increases its vulnerability to attack or unauthorized access.

Organizations can't do much about threats, because threats are outside their control. They must, however, be aware and vigilant, and take pre-emptive actions that can help protect against threats and exposures as much as possible.

Risk is also always present in any environment or system. Risks must be assessed, understood, and managed, so that organizations recognize them and prioritize which threats to focus their mitigation and remediation efforts on first to reduce potential business and operational loss.

In addition, organizations must understand and manage exposure. Assets must be protected and monitored to make sure there's no unauthorized access, tampering, loss, or theft.

Where (How) Do Endpoints Fit?

Remember the original definition? Endpoints are equated with computing gear of some kind — with a keyboard — that users employ to access an organization's networks, services, data, and applications. Endpoints are numerous and they're everywhere, and make an inviting target for attack. Ideally — at least, from an attacker's perspective — a successful attack on an endpoint provides entry into an organization's network, access to its digital assets, and control of the endpoint itself.

You already know that a definition of endpoints must include smartphones, tablets, and other mobile devices. Unfortunately, the classic definition of endpoint — something with which a user interacts, such as a desktop, laptop, tablet, or phone — is insufficient. It must also include servers, printers, private and public cloud workloads, point-of-sale systems, IoT devices, and even network switches and routers.

In short, anything that can be targeted in an attack or used as a conduit to a device that can be attacked must be secured. Experts emphasize that any device with a network IP address that's permitted to interact with an organization's networks is an endpoint — and should be handled accordingly.

IP stands for Internet Protocol, and is an important element of communication on the Internet. Using IP can be understood as a kind of fundamental requirement for Internet access, so obtaining and using an IP address is the ticket to participating in the Internet world.

In the modern age, where sensor networks and all kinds of devices are likely to use a network, it's unlikely that corporations or organizations will grant washers or dryers network access. Even so, many will welcome smartphones, virtual machines and devices, point-of-sale systems, ATMs, medical devices, fuel pumps, and other business-oriented stuff — busting the definition of an endpoint wide open.

A growing scope of Internet-attached devices that are not directly controlled by humans — including sensors, scanners, industrial equipment, and more — is called "the Internet of Things" (IoT). In process control or manufacturing environments, it may be called an "Industrial Internet of Things" (IIoT).

Managing security for these devices or "things" is an increasingly important concern, a huge emerging business issue (analysts speak of tens to hundreds of billions of such devices online by 2020), and a giant potential headache for IT.

A convergence of operation technology and information technology systems and networks is underway in many large industrial and infrastructure organizations. This digital transformation requires that we also include OT devices in the definition of *endpoint*.

Figure 1-1 introduces a hierarchy for devices typically found on organizational networks. The order of the pyramid reflects both the business value of the assets involved and their overall counts (with one possible exception). Where counts are concerned, there are invariably more end-user devices than anything else amid the endpoints, with relatively fewer network devices and business-critical endpoints. Although the number of critical high-value systems such as servers and cloud assets is small, the number of OT items is somewhat open; it may simply reflect the consoles and servers that aggregate sensors and devices, or the sum total of such devices plus consoles.

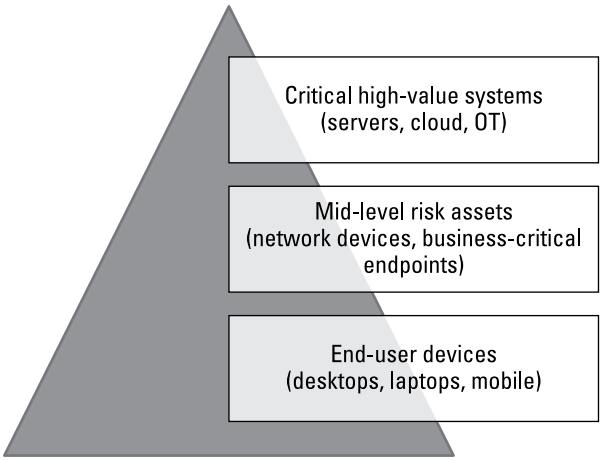

Figure 1-1: Pyramid of asset count and business value.

From a business value perspective, the pyramid reflects the impact of potential compromise or loss. Items lower on the pyramid impose a more modest impact in general (though

a more serious risk of a compromised "lower value asset" is that it can become a pivot point for an attacker to move further into the network toward higher-value assets). That's why the higher one climbs the pyramid, the bigger the overall potential impact of compromise or loss. The pyramid lays out visually the value and priority of assets in an organization, and helps to explain why the levels of protection and monitoring typically increase as one climbs closer to the top. For completeness' sake, it's probably wise to understand that the sensors or "smart circuits" in the elements at the edge of a group "of things" belong at the bottom of the pyramid as well.

In the years ahead, countless networks "of things" will be coming online. Those things will be endpoints on organizational networks, too, and thus, must be protected.

Endpoint Detection and Response

In reality, an endpoint is any system worth protecting. If such a system is compromised, it can inflict a negative monetary or operational impact on an organization, and that's the reason to protect it. Examples of such systems include Internet-facing web properties (which may be used to conduct business, to establish an online presence, and/or as communications hubs), trading systems, SCADA systems, payment processing systems, and national defense or POS infrastructures.

The endpoint security game

Endpoint security starts with protecting and hardening devices — the endpoints — but doesn't stop there. Broad, effective protection means endpoint security must also include ongoing endpoint discovery, monitoring, assessment, and prioritization to minimize the means and probable success of attacks on endpoint systems. This is called "the attack surface" in cybersecurity-speak.

Also, endpoint security must accommodate and use threat, vulnerability, and intelligence data — news and alerts from analysts who monitor the threat landscape — to analyze and respond to any attacks that slip through existing defenses.

The goal is a proactive defense that makes an organization more resilient to attack, reduces its attack surface, and can respond to the threats and risks involved.

Threat intelligence consists of evidence-based knowledge about an existing or emerging threat to assets designed to help guide a considered response to that threat. The knowledge can include security context data, indicators or signatures, implications, and actionable advice. Threat intelligence usually comes from security feeds that may also include actionable advice on how to automate an appropriate response to a threat.

Requirements for EDR

Endpoint Detection and Response (EDR) systems demand at least four types of capability, shown in Figure 1-2. The first item is the detection part; other items comprise the response part. Systems must

- Be able to detect security incidents as they occur.
- Contain the incident at the endpoint.
- Support investigation of the incident.
- Provide mechanisms to remediate affected endpoints.

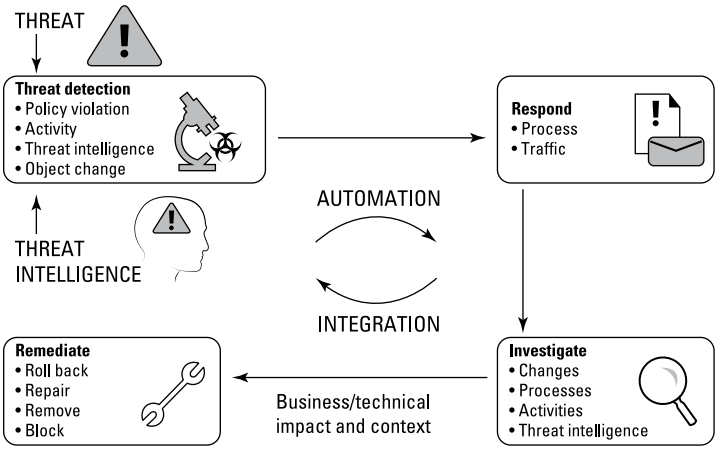

Figure 1-2: Four types of EDR capability.

In broader terms, EDR can go beyond detecting incidents and responding to them. Advanced EDR systems can help reduce the overall attack surface (to whatever extent intelligence and technology allow), limit the impact of an attack, and use intelligence and observation to predict when and how attacks might occur.

An effective EDR system requires that we discover, catalog, and assess all endpoints as they come online and each time they are used thereafter. Based on endpoint discovery, EDR systems then deploy an agent or agent-less mechanism for threat detection, monitoring, and reporting capability that plugs into a management server of some kind, and provides regular data feeds into a database that tracks activity, software configuration, security status, and more.

Chapter 2

Protecting Endpoints

In This Chapter

- Discovering, inventorying, and monitoring endpoints
- Closing cyberthreat gaps
- Dealing with detection and response
- Automating threat protection: Can it work?

Lots of devices qualify as endpoints nowadays. In addition to classic computing devices — desktops and notebooks — a plethora of mobile and other devices also qualify — smartphones, tablets, network infrastructure elements, industrial equipment, kiosks, POS systems, and more. And then there's the whole business-oriented "Internet of Things" to consider. That vast array of systems and sensors in business and industry is increasingly endowed with Internet access.

Any endpoint with the ability to access an organization's network is a potential point of attack. For that reason, an organization should protect its endpoints, prevent as many attacks as it can, and deal with attacks that succeed as quickly as it can. A considerable amount of work is involved, and some great tools are available to help see that it gets done.

Let's dig in and see what's involved in effectively securing endpoints — all the way from recognizing them, to assessing and updating them, to monitoring their activity, to detecting security incidents and then quickly responding to limit the damage or loss and remediate the affected endpoints.

Endpoint Action: Discover, Inventory, Monitor, and Protect

Securing endpoints begins with their *discovery.* You can't protect what you don't know about! And with the proliferation of all kinds of endpoints and applications, it is important to quickly detect any shadow IT or rogue endpoint instance on your network. An EDR system continuously scans the entire extended network across the organization to detect any new endpoint asset (hardware, software, or operating system).

The next step in the endpoint intake process is to take *inventory* of that device. Which versions of firmware, OS, and software is it running? Security analysts can then classify it automatically based on a known set of attributes and scan it for vulnerabilities. Is it patched and up to date? The endpoint configuration and version information is logged and recorded along with all known vulnerabilities, scored for their severity.

After endpoints have been profiled and assessed for vulnerabilities, security pros can decide the level of monitoring — agent or agent-less, real-time or on-demand — and apply the appropriate policy to continuously monitor and protect the asset in line with the organization's security program.

All endpoints are *monitored,* which means at least two things: One, it means their current configuration — firmware, OS, software, patches, security posture, and so on — is continuously checked. Also, the system is monitored for any changes, policy violations, and unauthorized file changes.

The second aspect of monitoring is to observe what endpoints are doing. Monitoring makes sure that any system or file change and access is detected and analyzed for unauthorized or malicious access or intent. This kind of monitoring can be understood as "keeping an eye out for suspicious, untoward, or malicious behavior."

All endpoints must also be *protected.* To some extent, this requirement is addressed by managing device configurations so that updates and patches are kept current, and by making sure that any "drift" from baseline "safe" configuration or any policy violation is immediately flagged and analyzed for unwanted, unauthorized, or malicious incidents.

Device hardening is another kind of protection in which endpoint devices are constantly updated and managed to keep them secure against known configuration weaknesses.

Protection also requires monitoring security intelligence sources to understand emerging threats that affect systems, software, and services related to the organization's endpoints. Organizations must learn about necessary remediations as soon as they become available, and learn how to recognize and respond to threats whenever they might appear.

EDR systems can use small, lightweight programs called *agents* that run on each endpoint in the form of an application, an app, or even a kernel-level add-in on devices that may not support applications or apps directly. An agent provides deep and real-time monitoring, analysis, and response. In some cases, a remote or agent-less approach is used for discovery and less intrusive monitoring and response when an agent is not feasible, acceptable, or requires longer deployment cycles.

Remember, your endpoints can be located on the enterprise network, in the data center, or in the cloud. They can include a broad range of systems such as Windows desktops and servers, OS X, AIX, HP-UX, CentOS, Debian, Oracle Linux, RHEL, SUSE, Solaris, Amazon Web Services, and Azure deployments.

Mind That Cyberthreat Gap!

In an ever-escalating threat landscape, some threats inevitably get past initial defenses and breach the endpoint's security. In such cases, it's absolutely critical to detect the breach quickly, scope its impact, and then respond quickly to contain the potential damage. A lifecycle model called the Cyberthreat Gap addresses potential issues for detection, response, and prevention. In this model each element has its own gap:

- **The Detection Gap:** The amount of time that passes from when a breach occurs until the organization discovers its presence and identifies it conclusively. Industry reports say this gap can sometimes be as long as 18 months.
- **The Response Gap:** The amount of time an organization takes to identify the scope of a breach and to contain its damage. Industry reports indicate that this gap can take four months or longer to be closed.

- **The Prevention Gap:** The time needed to implement measures that avoid a repeat of the breach, or a similar breach. This is an open-ended time frame, and can take months or years to close, depending on the nature of threat involved.

When security breaches occur, organizations need quick answers to three questions. Q1: Has a breach occurred? Q2: How bad is the breach? Q3: How can we contain it and then prevent it from happening again? Answering those questions marches you through the lifecycle and helps to foster a proactive security mindset.

Detection and Response: What's Needed?

Capable EDR systems inventory and manage system state — the configuration of firmware, OS, applications, and so on — against a baseline of what's normal for each of the endpoints. Then the same EDR system monitors endpoint state changes so it can correlate those changes with system events and application logs. Such changes can include installed software, files on an endpoint, the Registry, user privileges and account information, user behavior, running processes, and open ports or communications activity.

A good EDR system uses multiple methods of detection to identify threats on endpoints, to determine if and when those threats took up residence, and to ascertain what kinds of changes or effects have occurred as a result of the threat. These include the following:

- **IOC detection:** This method identifies changes in the system state and compares it to internal IOC (Indicator of Compromise). Sometimes it may be necessary to send the state changes or a suspect file to a threat intelligence service for analysis and evaluation.
- **Anomaly detection:** Changes to a system from a known good base configuration can also help to identify threats.
- **Behavior detection:** Identifying bad, odd, or illicit behavior on a system can indicate a threat. Logging such events helps with threat identification and may identify the time when an incident occurred or began.

- **Policy violations**: System changes (for example, scheduled maintenance or upgrades, new software installs, new users, or account changes) outside approved configuration windows may indicate a threat actor at work.

It is critical to identify successful attacks as soon as possible after they occur. A good EDR system catches them as they start to unfold, identifies them automatically, and helps take immediate response action. The shorter the period in which attacks are active, the less damage they can cause.

War stories: The value of speed and accuracy

Case study 1: A firm implemented an EDR solution to reconcile changes on its endpoints. When a pen-test team exploited a vulnerability on a web server to drop an exploit kit, the change was detected by the EDR system, reconciled with ticketing (as a "bad" change) within minutes, and escalated to an incident response team. Case closed (before it really got going, in fact)!

Case study 2: A gaming company's SIEM received "404, page not found" logs from approximately 20 percent of all transactions on its web servers. At first, the company thought it was a DDoS attack, but their firewalls and network intrusion detection system's events didn't support that theory. Then they thought it was an exploited vulnerability, but their vulnerability scanner revealed nothing relevant. Finally, using EDR with configuration management, they determined that a patch had been deployed improperly on two systems in a ten-server cluster by looking at the system state history. The patch was redeployed and the error disappeared!

Case study 3: A developer and publisher of innovative games used Tripwire's EDR solution to detect an attack on its web servers. Reports showed that files had been created, the owner ID, what the files contained, and the time they were created. The company immediately isolated those files and baselined everything on the system to contain the damage. The company found the malware and quickly deployed patches without having to take its servers offline. The response took hours — not days or weeks — between detection and eradication of malware on their systems. Meanwhile, security headlines continued to reveal names of other compromised organizations, but not this company.

Can You Really Automate Threat Protection?

Indeed, a top-notch EDR system can detect, analyze, and verify threats, include brand-new ones (called *zero-day threats*), and truly nasty ones (called *advanced persistent threats*). Changes to system state can be compared automatically to IOCs, and suspicious files can be automatically uploaded and "detonated" in isolated test areas called "sandboxes."

To help confirm and investigate security incidents (when threats are detected, identified, and analyzed), the state of any endpoint can be compared to its baseline to quickly and clearly see how they differ. This comparison also identifies what needs to change on an affected system to re-establish the baseline. Furthermore, advanced search functions run through the EDR database to help determine the scope of a breach and identify all the endpoints potentially affected by that breach.

Another key component in a capable EDR system is called proactive discovery. Such a component continuously monitors the network to discover all endpoint assets and applications. Security analysts can then automatically classify the assets or applications by examining their attributes, which come from the ongoing inventory. Analysts can scan those assets for vulnerabilities, which may then be remediated. For example, patches or updates may be needed, or malware protection can be added or updated.

When the endpoint asset is "clean," the EDR system can deploy monitoring and reporting processes that make EDR work. Those processes support data collection and automation for the detection and response that give such systems their name. The EDR system also applies the appropriate configuration and monitoring policy for the endpoint and begins ongoing monitoring and protection. This capability includes threat detection and response.

Chapter 3

The Cybersecurity Surround

In This Chapter

- Coming up with context
- Integrating all aspects of security intelligence and services
- Detecting threats in real-time
- Understanding threat intelligence
- Responding in real-time. Automatically? Really?

Truly understanding the scope, depth, and breadth of the threat landscape requires understanding and respecting its features and layout. This requires accurate and insightful threat intelligence — *lots* of it, all the time. That's why protecting and hardening alone aren't enough to ensure proper security: You can only protect against threats you can recognize. But because new threats pop up with astonishing frequency, you have to keep an eye on those aspects and behaviors of systems that are likely to be attacked, and those that are likely to change if a breach occurs.

This strategy involves integrating endpoint, network, and risk and threat intelligence, monitoring, detection, and careful, well-considered responses that occur as quickly as possible. As the inimitable Yogi Berra once said: "You can observe a lot by just watching." Remaining watchful is one of the keys to maintaining proper security and minimizing risk.

The Need for Context

Context describes the world around us and puts current situations and circumstances into place. Where endpoint security is concerned, that means threat context — understanding

applicable and relevant threat details and business context — that reflects the relative criticality and value of the endpoint asset to the business and organization — operationally and financially.

Countless sources of threat intelligence are available, so the best EDR systems can consume multiple sources constantly and filter the information they receive. They do that by focusing on endpoints and other system and software elements in use within the organization and ignoring threats that aren't relevant. That's another great reason for the accurate inventory at the heart of security savviness! For example, if you don't have any Apache servers, however unlikely that may be, your EDR system need not concern itself with threats and vulnerabilities related to Apache. It watches out only for those things it must, but it watches relevant threats very carefully!

What is threat intelligence?

Threat intelligence provides data that you did not already have (such as reputation scoring, attack tools, threat actors, and so on). It provides data (or analysis of that data) that helps you make more and better decisions about defense and helps you figure out what else to look for, or what proactive measures to take.

Making best use of threat intelligence

- Automate what you can: Automated attacks need automated defenses.
- Save analyst resources for subtle, complex data that helps you pinpoint threats that are most likely to affect your organization negatively.

(Source: 451 Research)

Threat intelligence is widely available from many commercial and community sources — for example, Cisco, Check Point, Palo Alto Networks, Lastline, Blue Coat, iSIGHT Partners, CrowdStrike, Soltra, and ThreatStream, among many others. Every organization needs to decide which threat intelligence services are most suitable for it, based on criteria such as origin, freshness, speed and scale, relevance, accuracy, confidence, completeness, and consumability.

Advanced EDR systems integrate with multiple independent threat intelligence services and support concurrent feeds for automated threat detection and validation. Because threat intelligence drives EDR (and much of enterprise security defenses), these decisions are vitally important. Intelligence feeds should be an important part of the conversation with any prospective EDR system vendor.

One more aspect of context is crucial when dealing with cybersecurity: It's called security awareness. This is an ability to prioritize threats and responses. An organization and its security system must quickly address those threats that are truly dangerous to the organization, and deprioritize everything else — no matter how dangerous those threats might be to others.

Integration Trumps All Else

By itself, threat intelligence is interesting and provides a sense of context. But it's what one *does* with threat intelligence that really counts, and that's where the rubber meets the road with EDR. This explains why a recent report from the Enterprise Strategy Group (ESG) identified a lack of integration of threat intelligence programs into enterprise collaboration, communication, and IT workflows as a chief shortcoming for in-house security intelligence programs.

According to a recent IDC study, spending for global threat intelligence services approached $1 billion in 2014; it's expected to approach $1.5 billion by 2018. It's essential for organizations to make sure this is money well spent. Wise expenditures result in actionable security intelligence for endpoints.

The ESG report identifies several shortcomings of do-it-yourself threat intelligence consumption:

- Intelligence programs are often hampered by manual processes. Human security analysts end up doing by hand activities that could easily be automated. Integration with well-designed software tools or services, like EDR, can eliminate such drudgery and free human analysts to improve your security posture. Automation also speeds response, which can make a huge difference in minimizing impact.
- IT teams can overlook providing additional context for threat indicators, regardless of their source. For best results, organizations should receive threat intelligence in real-time and combine it with security awareness. This means the best use of intelligence occurs when it combines all sources of data, including user behavior, to determine the extent of a threat, and an appropriate response.
- Organizations should leverage industry consortia and law enforcement to validate threat findings. Automated processes should trigger instant interactions inside enterprise boundaries.
- Security analysts work most efficiently with threat intelligence when it is automatically pre-filtered to focus on actionable advice for existing or emerging threats. Context can be enriched with human analysis of past and present indicators along the way.

Intelligence is only as good as the protection and response it delivers. Prioritize the threat intelligence that's relevant to your endpoints — and the rest of your security infrastructure — and act on high priority items ASAP!

Real-Time Response

Real-time response means an ability to detect and respond to threats as they appear. An ideal response is fast enough to prevent any threat from establishing itself on organizational networks or having an impact on organizational assets. The next two sections explore the means to this important security goal for endpoints in particular, and infrastructures in general.

Is real-time response possible?

An ability to respond in real-time to threats depends on the type of security systems involved. For endpoints, this means an EDR system that can recognize and distinguish low-risk threats from those that are high-risk. To make real-time response possible, an EDR system must be able to make this distinction and to immediately issue alerts, and have the ability to take action as soon as a high-risk threat is detected.

What makes real-time response possible is an accurate understanding of threat context and business context of the endpoint in question. Likewise, real-time response depends upon the ability to recognize and react to risky or dangerous behaviors or changes, even if no external threat is currently recognized.

The best EDR systems work with threat intelligence to stay current with the threat landscape in real-time, and to apply best-practice responses when a threat is recognized. For high-risk threats, this means sending up red flags and taking automatic action where possible and feasible. Red flags are important for a variety of reasons, including establishing the time when a threat occurred, marking endpoints that may be affected, and enabling monitoring of follow-on changes to build a threat footprint that can be used to drive future intelligence and prevent repeat occurrences.

In addition to intelligence-driven response, a quality security infrastructure (to which an EDR system should always belong) includes a variety of other options. One is monitoring key system files and resources (such as the Windows Registry) to look for unexpected, unwanted, or unauthorized changes in devices, operating systems, and firmware, to name a few. Another is observing and logging communications, paying special attention to unusual or known malicious IP addresses or URLs.

Data and intelligence-driven responses are well within the scope of a good EDR system, as is response based on unwanted or disallowed system, file, or policy changes. What to do about such things is the focus of the section that follows.

It's been said that the answer to any good question always begins with "That depends. . ." Automating real-time responses

to threats depends on the security infrastructure and EDR system in use. It enables a kind of worst-case "nuclear option" should other options fail or otherwise be unavailable. If a sufficiently risky threat is detected, depending on the business context and number of the affected assets involved, you may decide to automate a mitigation (or blocking) response until further inspection and analysis indicates that the threat has been remediated or eliminated.

The nuclear option is best held in reserve because most users, and the organizations that employ them, probably prefer a more nuanced approach. It's appropriate only when nothing else will serve to protect the users' and the organization's interests and assets.

Threat detection looks at a variety of states in real-time to decide if a response is warranted, and if so, what kind. It may look for signs of changes to key processes or files, signs of unwanted or illicit activity, signs that correspond to signatures or profile data from threat intelligence, or changes to objects within the endpoint itself.

The best response is one where automated remediation can be applied in timely fashion. This is the goal toward which all EDR systems must strive. Otherwise, a response must be two-pronged: informing affected users that access is suspended because a security threat has been detected, and launching an investigation to get at root causes. When several things have happened — data that describes the threat has been collected, the business and technical impact has been identified, and context data has been gathered — remediation can get underway. Such remediation, which can be automated or manual, may involve the endpoint in repair routines, rollbacks, de-installation and cleanup of rogue software, and blocking access to IP addresses or resources.

What can be automated depends on how well the threat and its remedy are understood. Those that are well-known or easily understood can often be remedied without human intervention. Numerous threat intelligence exchanges facilitate response automation, so enterprises must develop processes that make it possible to implement automated responses whenever possible. Responding to less straightforward threats requires a bit more work.

Chapter 4

Security Maturity Is in Your Futurity

In This Chapter

- Collaborating between security and IT operations
- Creating synergy with compliance and security frameworks
- Assessing security maturity

On modern networks, the definition of endpoints now includes any device with access to an organization's networks and information. Thus, as discussed in Chapters 1 and 2, the notion of endpoints now goes well beyond laptops, personal computers, smartphones, and other mobile devices.

The analyst firm Gartner, Inc., has developed a model for its subscribers — what it calls "security maturity." This model measures how far along an organization is on a maturity scale, taking into account the organization's information security principles, practices, policies, and tools. Forrester Research, Inc., has published a tool (access requires a subscription) to help organizations assess their information security maturity using the level definitions shown in Table 4-1.

Table 4-1 Forrester Maturity Level Definitions

Level	*Characteristics*
0 — Nonexistent	Not understood, not formalized, need is not recognized
1 — Ad hoc	Occasional, not consistent, not planned, disorganized

(continued)

Table 4-1 ***(continued)***

Level	*Characteristics*
2 — Repeatable	Intuitive, not documented, occurs only when necessary
3 — Defined	Documented, predictable, evaluated occasionally, understood
4 — Measured	Well-managed, formal, often automated, evaluated frequently
5 — Optimized	Continuous and effective, integrated, proactive, usually automated

Source: Assess Your Security Program with Forrester's Information Security Maturity Model, Forrester Research, Inc., November 2, 2015.

Although these models are not perfect, they provide a good starting place to wrestle with the topic of how to practice good endpoint security. Next, we examine a more practical approach to security maturity modeling, after which we offer some expert advice on how security maturity can be improved through technology, automation, and improved user security awareness.

The Security Maturity Model

Figure 4-1 depicts five levels of maturity in a typical maturity model and how an organization might move from a tactical to a strategic risk- and business-driven security approach. Level zero (0) is best described as cheerful obliviousness, where the organization is completely unaware of security concerns. Level 1 is an ad-hoc, IT-centric approach — a level that should sound familiar to many readers. Then the model advances through intermediate steps, all the way to Level 5. At this point, security is continuous and effective, fully integrated with business concerns, proactive in nature, and as automated as technology permits. Changes in technology, compliance, and economics cause constant adjustments to the security regime. An organization at Level 5 may be described as context-driven and fully risk-aware, able to understand potential impacts of business, technology, and security risk choices and decisions.

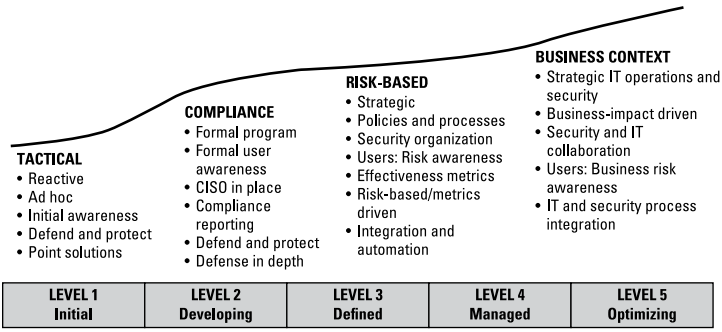

Figure 4-1: Levels of maturity in a typical maturity model.

The key to understanding this model is to note increasing levels of formality in security programs. In Level 3, for example, policies and processes are defined, a security organization is likewise defined, and user security awareness is continuously taught and revisited. As the maturity level increases, formal governance comes into play along with an info-centric approach and effective security metrics. A mature organization is one where all the pieces — policies and procedures, governance, metrics, and informed users and information owners — come together. At the highest level, all the players continuously adapt the security environment to keep up with changing technologies and the ever-shifting threat landscape.

From an endpoint security perspective, it is vital to recognize that risk-based and business context-based security processes and implementation are crucial to successful EDR use.

Extending Maturity to Endpoints

SANS used to mean "Systems Administration and Network Security" when used in the context of the organization known as the SANS Institute. This expansion for the acronym has gone by the wayside, although SANS remains active in teaching and certifying cybersecurity professionals. SANS promotes security awareness in government, law enforcement, the IT industry, and enterprises at all levels. SANS played host to security expert G. Mark Hardy in September 2015 for an important discussion of endpoint security maturity.

Check SANS out online at `www.sans.org`. Its certification program is known as the Global Information Assurance Certification program (GIAC), online at `www.giac.org`.

Its reading room is also worth a visit at `www.sans.org/reading-room`. Hardy's presentation is available at `https://www.sans.org/webcasts/100542`.

The point of the security maturity model, as well as Hardy's presentation, is that endpoint security maturity means more than ticking off a list of checkbox items. Achieving security maturity with endpoints must involve the following elements:

- **Doing things right**. Carefully considered, this epigram captures the intent of security maturity models and the SANS model that Hardy proposes to supplement it. Organizations must develop a security focus, identify and secure all endpoints, create a strong security program supported with policies, procedures, governance (and compliance, where applicable), and institute regular monitoring and software updates.
- **Protecting information using secure configurations**. The essence of taking proper care of endpoints is to understand which collection of software, policies, settings, patches, and updates constitutes a secure configuration, implementing and monitoring that configuration, and keeping it current over time.
- **Emphasizing user awareness to account for all network endpoints**. Just as insiders represent a major source of exposure, users in general represent a major point of security weakness. But if trained properly, users can be on the front lines of defense and become an excellent source of security intelligence. When users know they should avoid unsafe behaviors, they allow fewer threats into an organization. If they know how to respond when threats begin to manifest, those threats have less time to take root and cause damage.
- **Apply policy and device awareness to boost security**. A complete written set of security policies should be published, taught to employees so they can apply them, and subject to regular review. Employees should be tested on those aspects of policy that pertain to their jobs.

The Center for Internet Security (CIS) publishes and maintains a set of Critical Security Controls, called CIS Controls, designed to help define and guide strategies for effective cyber-defense. See `http://www.cisecurity.org/critical-controls.cfm` for the list, and pointers to more info.

NIST has also created a cybersecurity framework that likewise identifies an organization's current security state, and describes ways to boost maturity (and security posture). For details, see `http://bit.ly/NISTCyberSecFramework` (PDF file). Other commonly used security frameworks include the ISO 27000-series, IEC 62443, FFIEC Information Security, and COBIT.

Process and People Matter

Employees, customers, users, clients, or whatever else you call those who access your organization's networks, are central to any security program. Recent studies have shown that untrained people can pose significant threats to an organization, simply because they often don't know that certain behaviors are unsafe.

Here's a case in point: CompTIA (the Computing Technology Industry Association) sponsored a study where researchers left an unlabeled USB flash drive in a public place and tracked those who picked it up to see what they did with it. Nearly one in five people proceeded to use that drive in ways that could have posed cybersecurity risks to the devices into which they inserted the drive, and possibly also their employer's networks and systems. Search on "Find a flash drive, pick it up" to read the reporting on this experiment.

The Stuxnet worm that damaged thousands of Iranian gas centrifuges and severely hampered that country's nuclear ambitions was spread onto its secure, isolated ("air-gapped") networks through infected USB flash drives. In fact, a good EDR solution can detect and report on USB drive activity and mitigate this kind of exposure. Something else to check on when picking an EDR solution!

The moral is that people pose security risks because of ignorance or a lack of security awareness. The remedy is to end their ignorance and train them on a regular basis on security fundamentals and the current threat landscape. As threats evolve, awareness and training must do likewise.

Security isn't simply something that people must understand; it's also a *process.* A consistent thread throughout the Gartner, Forrester, and SANS security maturity models is the need for a well-defined policy to govern security, as well as a clearly defined process to apply, verify, and enforce policy

wherever and whenever it makes sense. The emphasis should be on written security policies, easy access to those policies online and in print, regular training on those policies, and also, regular reviews and updates to those policies.

Most organizations that practice a formal security methodology also engage in periodic security audits. These audits expose any weak areas or gaps in current policy, make sure that items active in the current threat landscape cannot be exploited by known attack vectors, and determine whether policy as written matches policy as enacted. Such audits often result in adjustments to policy, changes to security infrastructure, and refinement of threat detection and incident response-handling processes.

Moving Beyond the Check box

Let's face it: people from all walks of life — including security professionals — like things to be simple and straightforward. But as much as we might like to boil potential security problems down to a list of items with a check box next to each one, that isn't the way strong security programs work.

Sure, maturity models are valuable because they provide concrete ways to measure progress, but security means more than knocking off a list of discrete tasks. Tools must be carefully selected. Those tools must be coordinated and integrated to ensure they not only work together properly, but that they don't leave gaps in coverage or capability. Through such gaps, threats might be able to infiltrate themselves onto an organization's endpoints and networks. This danger is an important impetus for regular penetration testing, and a good illustration of why more testing is better than less. Business context can further help prioritize and focus these efforts on operationally and financially critical endpoints, within an organization's budget and resource constraints.

Security awareness comes at the top of maturity models because it avoids the check box mentality. This level of security understanding and awareness does several things: It recognizes the importance of security, seeks to raise security consciousness across an organization, and teaches users to see the security component in all aspects of the workplace. Not coincidentally, this explains why EDR is only part of a larger overall security infrastructure, and why its ability to integrate and interoperate with the other elements of that infrastructure is of vital concern.

Chapter 5

Security Is Process, Policy, and Eternal Vigilance

In This Chapter

- Understanding and formulating security policy
- Baselining endpoints
- Detecting continuously and precisely
- Correlating security controls

Cybersecurity is as much about attitude and state of mind as about tools and technology, if not more so. Those responsible for creating security policy need to have a clear understanding of what they are trying to achieve and make sure the resulting policies are practical and understandable to users. It's also crucial that security policies be enforceable. Let's explore how to make that happen.

Security Policy and Endpoints

In formal terms, a security policy is a document that spells out how an organization plans to protect its assets, both physical and digital. There's a lot going on here, so let's dig deeper.

For guidance on this essential cybersecurity topic, SANS again provides key information, this time from its Reading Room, in a document entitled "Security Policy: What it is and Why — The Basics." Find it online at: `http://bit.ly/SANSSecPolBasics`.

Paraphrasing the SANS document, security policy states clearly what must be done to protect digital information. A properly crafted policy states in writing what to do, so that how it gets done can be established, and then measured or audited. Security policy also protects people in an organization, recognizing that decisions or actions in situations where information is at risk also involves personal liability to corporate officers involved.

The areas that a security policy is meant to address are clearly spelled out in the SANS document; this alone makes it worth reading:

- Risk assessments
- Password policies
- Administrator responsibilities
- User responsibilities
- Email policies
- Internet policies
- Disaster recovery
- Intrusion detection

All in all, a well-constructed security policy lays out the blueprint for implementing and practicing security within an organization. Any violation of these policies should be monitored and prioritized for analysis and response because these can be the mechanism that makes early detection of an impending or ongoing breach possible!

Organizations that seek to attain a high level of security maturity should review and adjust their endpoint security policies, including proactive risk assessment and controls, detection of emerging and zero-day threats, how to analyze and document them, and most importantly how to respond to contain the damage or loss and then remediate and repair the endpoints. Establishing these processes and publishing a RACI model, which identifies who within the organization is Responsible, Accountable, Consulted, and Informed, sets the foundation for solid collaboration across the security and IT operations teams as well as accelerating organizational response in case of an actual incident.

Baselining Endpoints

A good EDR implementation requires that we quickly identify new endpoints as they appear on an organization's networks. Such systems generally make an inventory of what's installed on each endpoint device including some or all of the following: firmware, operating system, applications, and communication software, along with the versions and updates or patches applied to these various components.

Normally, an EDR system requires an endpoint to meet security requirements regarding software and firmware in accordance with the security policy and issues an alert on any unauthorized access, violation, or change of configuration. At the same time, the EDR system may alter or add to an endpoint's configuration to make sure that proper controls are in place for safe use and secure communications.

Some advanced EDR systems also install an agent, a lightweight software program that allows the EDR system itself to access the endpoint, monitor its activity and configuration, and make changes to that configuration as and when such changes are necessary. However, given the vast array of endpoints that need protection, alternate remote and agent-less (or mixed) deployments may be more prudent in some situations for faster time-to-value and cost optimization or for other purely technical reasons. The key is to establish this practice as part of your security program and to give due consideration to the business context of the endpoints to be secured as they fit into your security- and risk-planning goals.

Baselining is a key concept in cybersecurity. It refers to establishing a detailed sense of what's "normal" and "safe" for systems and devices to ensure a secure environment. This notion of what's "normal" can be essential when monitoring systems, because it provides something against which to compare current state, configuration, and activity, and often allows threats to be detected by inference even when no direct evidence or means of recognition is available or known.

Baselining endpoints establishes a point of reference for subsequent monitoring and management. Like everything else in the security world, baselines must change when what's "normal" changes. Thus, it's best to think of a baseline as a snapshot of the ideal or desired state of an endpoint, which

must be refreshed whenever changes are made by intent or design (adding or updating the OS or software, applying patches or fixes, adding or changing network services or configuration, and so forth and so on).

Ongoing Detection and Response

The real job of EDR focuses on what happens after an endpoint is admitted to the network. Warfare and other high-risk activities are often described as "interminable tedium punctuated by moments of sheer terror." To some extent, the business of EDR is much like that except it actually boils down to "constant monitoring and comparisons to the baseline, punctuated by occasional but rapid detection and response to any deviation from the baseline."

The mechanics of endpoint detection depend on careful observation of numerous aspects of the devices and software involved, and the behaviors that they exhibit, and a constant comparison of these to the baseline for that device (and other devices like it, to give an "average baseline" more weight):

- Observation of changes to key system and application files which may indicate a threat is active (this pertains particularly to configuration files, application and other software files, account information, and so on).
- Observation of key system and application objects, such as the Windows Registry.
- Observation of communications behavior, including ports and services used, IP addresses referenced, and so on, because certain addresses and/or ports and services can be highly suggestive of threat activity, if not proof positive.
- Comparison of system state and behavior with threat intelligence, where such intelligence provides indicators to recognize active and emerging threats.

The value of EDR goes beyond detection to response. Good EDR systems provide as much automation as possible to help speed response and contain threat scope and effects, while alerting human operators to investigate or get involved, especially when a fully automated response is neither possible nor desirable.

Integrated Security/IT Controls

The full value of EDR and other elements of a security infrastructure is realized when multiple members of the security and IT operations team work together to help identify and respond to threats. Because endpoints are such inviting and common targets for attack, EDR systems often end up working in tandem with other security and IT solutions to identify, resolve, and prevent attacks. This is particularly true when deciding which security controls must be in place, and put to work to help with detection, response, and prevention.

When "Mmm" goes to "Uh-oh!"

There's a point during detection when suspicious behavior manifests as threat activity (perhaps even specific to a known, particular threat). That's when focused attention shifts into response mode, and when pre-emptive and defensive measures must start falling into place.

Security experts advocate an approach to security called "defense in depth." It requires building multiple layers of protection that support each other, so that if one security control fails to contain or neutralize a threat, another layer is ready to take over and provide additional protection. Thus, file protection on an endpoint would be nicely complemented by file protection on network servers, so that if an endpoint file is compromised, a threat would not then be able to copy that compromised — and possibly dangerous — item to a server or other endpoints. This approach can keep the threat from propagating while a response to eliminate it at the compromised endpoint can proceed.

Correlation Enables Triage

From a security perspective, correlation is all about noticing patterns that combine multiple observations. It might mean noticing that, shortly after a configuration file was altered on an endpoint, a connection to a questionable or malicious IP address commenced, and certain abnormal file changes were observed. By themselves, these events are suspicious; taken as an unholy trio, they clearly indicate the presence of an

attack or compromise (and might even be identifiable from the combination of all three events).

The best EDR systems continually interact with other elements of an organization's security infrastructure to, whenever possible, make such correlations. This usually means interacting with a Log Management system, Vulnerability Management, or a Security Information and Event Monitoring (SIEM) environment; internal and external sources of threat intelligence; and working with Security Configuration Management systems to make sure baselines and changes are properly analyzed for actionable response and remediation.

Information coming from other security components helps with all aspects of the EDR lifecycle. Intelligence and configuration data provide context and establish patterns associated with threats, to aid in their detection. Automated response information from intelligence and other sources helps inform response to threats, perhaps even without requiring human intervention. Actions taken in the EDR system during detection and response ultimately can also drive prevention efforts once the threat is resolved. And this cycle repeats itself endlessly, as new threats continuously emerge. . .

Chapter 6

Putting EDR to Work

In This Chapter

- Meeting the prerequisites
- Choosing the right candidate
- Implementing EDR
- Coping with constant change in the EDR lifecycle

On the assumption that you find EDR an interesting and possibly useful fit for your needs, you may think it's time to charge off and start working on EDR right away. Effective EDR requires planning to select the right system, create a supporting infrastructure, policies, and processes, and ensure support from the various security and IT teams that need to collaborate for its success. Making EDR work also takes time and effort, as does living with it once it's in place.

Before You Get Started. . .

To implement EDR and get a good return on your investment, numerous components must be in place. If you haven't yet looked at Chapters 4 and 5, they deal with security policy, security process, security awareness, and even security maturity. Before you let slip the dogs of war . . . er, rather, the hounds of EDR, you must address the concerns raised in those chapters. When you choose and deploy an EDR solution, be sure your security framework is mature enough to realize a good return on your investment.

Here's a list of tasks you should complete before you can choose and deploy an EDR system:

- **Formulating a security policy.** EDR works in the context of a complete enterprise security policy, as described in Chapter 5. Without a delineation of the risk assessments, administrator responsibilities, Internet, and intrusion detection policies, you won't know what you're trying to protect or how best to protect it.
- **Doing things right.** EDR is part of a comprehensive security focus that includes assessing, securing, and monitoring all endpoints. These activities take place in the context of a security policy with procedures for its enactment, governance, and compliance, if called for. EDR is a critical part of your security infrastructure, but not its be-all and end-all.
- **Discovering and profiling endpoints.** An EDR system must either include this ability or integrate tightly with monitoring tools to identify and profile any new endpoints that join the network. Asset categorization and risk assessment then informs an EDR security analyst on the risk posture of those assets to help select an appropriate policy for hardening, monitoring, and protecting them against current and emerging threats.
- **Using secure configurations for protection.** Risk assessments guide how endpoints should be hardened and protected. These assessments help minimize the attack surface and reduce risk. EDR works best in conjunction with security controls that establish, maintain, and protect secure configurations for endpoints. Often this means including or working with a Security Configuration Management (SCM) system to define configurations, and then using EDR and other security tools to look for telltale unauthorized or anomalous changes to them. Also, configuration policy tests can help in predicting points of failure in endpoints that might otherwise be exploited in an attack.
- **Deploying integrated threat intelligence.** As discussed in Chapter 3, threat intelligence is essential for EDR to successfully deliver on its promise to reduce the detection, analysis, response, and remediation gaps. Thus, it is vital to research and identify the most suitable threat

intelligence service feeds based on criteria described in Chapter 3. You may decide to select one or several commercial or community intelligence services. You may even decide to augment them with on-demand, cloud-based, sandbox malware analysis service. The EDR system that you select must support integration and automation for the threat intelligence services needed to protect your organization against current and emerging threats.

- **Developing and cultivating user security awareness.** Chapter 4 introduces the idea that users must be informed — preferably at regular intervals — about security fundamentals, safe computing, and security issues related to their job roles and responsibilities. To support effective EDR, users need to understand how to take responsibility for their own security and behavior. This helps reduce insider threats of the accidental or misinformed variety.
- **Establishing management support and team collaboration.** For an EDR (or any security program) to succeed, it is crucial to establish organizational leadership support. Also, for EDR to be effective in real life, it requires continuous alignment and collaboration across the security and IT operations teams. Look for an EDR system that delivers the integration and automation necessary to help those teams collaborate in real-time. This will reduce misalignments and minimize manual sharing of time-sensitive information. This is critical when teams are scrambling to detect, analyze, and respond to an actual security breach!

All of the foregoing considerations can help guide your investigation and evaluation of any EDR system. The solutions that score best for your endpoints, your policies and procedures, and your risks and threats, are the ones from which you should make your final choice.

Choosing an EDR Solution

First and foremost, any viable EDR candidate must support all endpoints on your network. After that, you can look more deeply into features and functions to create a checklist against which to evaluate potential candidates. Of the many

factors and items that should be in that list, the following are among the most important:

- **Accommodates all your endpoints.** The candidate provides deep visibility into endpoint security, activity, communication, and configuration, as well as detailed monitoring of critical files and objects for all endpoint types.
- **Supports response automation.** The candidate integrates with various threat intelligence services. It provides mechanisms that enable manual and automatic responses to recognized or demonstrated threats.
- **Works with other elements of security infrastructure**. The candidate integrates with threat intelligence, security configuration management tools, security information and event management solutions, log management, file integrity and change monitoring systems, vulnerability and risk management, and so on.

Security vendors that qualify for inclusion in any list of EDR candidates are those with which your organization already does business. If any of them offer an EDR solution, by all means add them to your list!

- **Minimizes risks to your organization, and understands (or can apply) your business context.**
- **Provides or includes adequate support for installation, set-up, and break-in of the solution.** This is likely to be a cost-plus item, and should be budgeted accordingly.
- **The cost of purchase and deployment, plus all recurring costs, fits within your security budget.** If you can't afford it, don't buy it.

When working with vendors to investigate, evaluate, and select an EDR system, the more you can tell them about what you need and want, the better off you — and they — will be. Provide them with a written list of must-haves and nice-to-haves, and then ask them to show how their solution addresses each one of those items.

Solution vendors want your business, but once you decide not to pursue some option, let the vendor know ASAP. That way, the vendor doesn't spend time and resources chasing an unlikely opportunity. Your courtesy will be rewarded the next time you need to conduct business with the same outfit.

Implementing EDR

When you're ready to take delivery of an EDR solution, please recognize that deployment to production endpoints is *not* the next task to undertake. There's some method to this madness. To ensure the best results when EDR goes into production use, please follow these steps:

1. **Test deployment** is by nature exploratory and experimental and should occur in a test lab, on a test network. You need non-production access to the rest of your security infrastructure, a representative sample of endpoints, and other equipment that is not on your production network to begin running an EDR solution. During this phase you learn to install, configure, and use EDR, work with the vendor's support and deployment staff to get things working, and make a first pass at integrating with other elements of your security infrastructure. You also begin testing threat detection and automated response capabilities.
2. **A pilot project** takes results of your test deployment out onto a carefully selected subset of the production network, and enlists participation from willing and well-informed volunteers to try things out, see how they work, and provide feedback. This step provides illustrations of "typical user behavior," which always includes unanticipated surprises not foreseen in the test lab. This process is likely to repeat; one pilot project may lead to another, or keep cycling through changes, as you and your users converge on a customized implementation tailored for the unique requirements of your organization. Give this process time to work itself out, because the better the pilot program works, the less trouble you'll have with full deployment.
3. **Production deployment planning** is essential before large-scale rollout. This means talking to the IT department to find out how and when they schedule deployment activity. Often, it's once a quarter over a holiday or long weekend. You need to understand how deployment is specified and configured, and how you will be expected to deliver the EDR documentation and system. Consider how to provide access to support staff — it's essential to have your own support team

and the EDR vendor's team on tap, if not on hand — during deployment rollout.

4. **Production deployment** occurs during a scheduled time window, under the aegis of the IT department's deployment team. This is normally a 24-48 hour affair, especially for organizations big enough to operate 24/7. A week or two before deployment, train rank-and-file security professionals who will be working with the EDR system on its proper use. This is the team that will deal with detections, responses (automated and manual), and feeding incident information into the prevention task that inevitably follows encounters with each new threat. The full rollout of an EDR system is when your organization reaps the benefits of its hard work and investment in this important security technology. After you're through the deployment process, you can get on with the rest of the security lifecycle.

Talk to your EDR vendor: Chances are good they've helped other customers get up and running. At a bare minimum, they can give you feedback on the four steps just outlined. They may even have deployment documents and advice to share.

Living with Your EDR Solution

Anybody who's familiar with the software lifecycle knows that over 90 percent of the time spent living and working with technology solutions occurs after deployment ends. This is where most of the work and activity occurs, and is therefore worth at least as much planning and consideration as the deployment phase.

Training and exposure are crucial ingredients in making an EDR solution work. If your organization plans to automate responses that follow threat detection, the people responsible should be involved in the pilot project. You may even choose to include these people in the initial test lab phase. The more exposure the response team has to the workings of the EDR system, the better off your users will be.

EDR users need to make sure their roll-out plan includes the resources necessary to integrate EDR tools with the rest of their security infrastructure. They also need to plan for initial and ongoing development to turn threat intelligence data into manual remediation or automated responses.

Chapter 7

Ten Top EDR Desiderata

In This Chapter

- Understanding EDR and its uses
- Baselining and prioritizing for EDR
- Building security maturity to support EDR
- Managing and maintaining EDR

Every *For Dummies* book, including this one, ends with a "Parts of Ten." Although the number of elements may not be exactly ten, the idea is to provide readers with a summary of key points and concepts from the rest of the book.

You know: Moses had his Ten Commandments, Blake Edwards had his "Perfect 10," and we'll never know what heights David Letterman wouldn't have climbed without his infamous and hilarious Top 10 lists. Ours may be somewhat lacking in hilarity, but not in importance. Here goes. . .

EDR Is Discovery-Based

For endpoint detection and response to work, all endpoints must be discovered whenever and wherever they access the organization's networks. The whole exercise rests on watching *all* active nodes, and then recognizing and managing endpoints as they seek to join in the fun. Endpoints are inspected and cataloged (see the next item, on inventory); based on a risk assessment and asset classification, an appropriate security policy is applied for endpoint configuration management, monitoring, detection, and response.

For EDR, the Inventory Tells All

EDR systems require an endpoint inventory that catalogs the organization's hardware, firmware, OS, and applications. This information is carefully established to maintain adherence to security policy, and then watched equally carefully to look for changes that could indicate the presence or behavior of a threat. This database of continually updated information ultimately describes endpoints and their security status.

It's All About the Gaps

In today's threat landscape, the gaps between detection, response, and prevention are critical. The detection gap is the time it takes to discover a breach and identify it conclusively. The response gap is the time it takes to identify the scope of a breach and to contain its damage. The prevention gap is the time it takes to implement measures to protect against a repeat of the same attack or a similar attack. The goal of EDR is to minimize these gaps — ideally to make them almost non-existent!

Identify and Prioritize

When threats present themselves, they must be identified and scoped. But they must also be prioritized so that organizations act quickly to address threats that present the highest risks to the most critical assets based on business context. EDR systems must use threat intelligence, business context, and security context to automate this process.

Now, Address Those Gaps

When a suspicious change or threat has been identified, the severity and priority of the threat drives how quickly it must be addressed. In a structured environment, EDR systems (and other security infrastructure elements) track all risks and drive remediation workflows to address the underlying problems. Automation in the EDR system (across the detection, analysis, and response processes) can also help close gaps without requiring extensive human intervention, or in some cases without any human intervention at all.

Baselining What's Normal

Baselining takes stock of endpoint configurations and their system state, plus applications and communications behavior, to create a snapshot of what's "normal" and "safe" for each endpoint. This information provides a vital point of reference and comparison for an EDR system when evaluating changes to configuration state or "drift" for evidence of an active threat or breach.

Advancing Security Maturity

EDR works best within an overall security program that includes security policies, user security awareness, governance and compliance management, and an understanding that security is an ongoing process and mindset. When the security environment is mature, EDR is much more efficient and effective at reducing the time and resources required to detect and respond to threats.

Correlations Make Security Work

Within an overall security infrastructure, EDR is just one of many components that reduce security risks, improve compliance with security policy, and limit damage or loss. Ultimately, security data comes from many sources, including threat intelligence, vulnerability intelligence, security configuration management, file integrity and change management, system and network monitoring, and more. Correlations across data from all of these solutions is necessary to paint a full picture of security risk.

Establishing EDR

EDR works best when formal, well-documented security policies and training establish a security-savvy corporate culture and guide end-user activity. Key elements of this process also include assessing risks associated with endpoints, establishing clear, effective user policies for Internet access and use, as well as developing and maintaining general security

awareness for all employees. Creating and maintaining an accurate inventory of hardware and software devices and selecting appropriate threat intelligence feeds help round out this must-do list of tasks.

The EDR Lifecycle Is Never Done

EDR is a never-ending journey because of the sheer volume of ever-changing threats with which organizations must contend. Some studies show that anywhere from hundreds of thousands to a million or more new threats manifest each day. This massive volume of threats requires constant vigilance and automation around endpoint state, configuration, and behavior. Reducing security risks requires attention to threat intelligence and correlating that information with careful attention to key files, objects, and configuration settings.

That's why EDR involves a constant, ongoing round of activity. For threats that have already been detected, responses must be formulated and enacted. Once enacted, this information feeds into the prevention cycle to keep similar threats from recurring. In addition, there's a constant need to stay alert for signs of new threats, and to make sure detection is working as it should be, starting the whole cycle over again.

As new endpoints, and new versions of operating systems, applications, and firmware appear, they must be inventoried, assessed, and hardened as much as possible to resist attack. The baseline for each type of endpoint must be considered carefully on an ongoing basis to minimize its attack surface.

In the EDR world, a never-ending cycle of improvement is required to close the gaps in detection, response, and prevention. Organizations that manage to reduce these gaps to their barest possible minimums are those that are least likely to fall victim to serious cybercrime. They are also the best-positioned to maintain a safe, secure network that minimizes risks of attack and exposure. These organizations can protect endpoints and users alike against an increasingly hostile and dangerous threat landscape. This level of EDR success is a sort of "Holy Grail" for information security, but well worth the continuous pursuit that is necessary to cope with threats while continuing to conduct business — all while improving productivity and profits.

Defend and protect every endpoint

Your endpoints are the primary target for cyber criminals. To effectively defend your organization, you need to proactively discover, monitor, and assess every endpoint on your network. You must also have deep visibility into threat, vulnerability, and intelligence data so you can quickly and precisely analyze and respond to attacks.

- ***Proactive defense* — *Take immediate steps to reduce the attack surface of your most critical endpoints***
- ***Adaptive security* — *Learn why deep visibility into endpoint states can help you respond to emerging and zero-day threats***
- ***Advanced detection* — *Correlate real-time IOCs, behavior anomalies, and policy violations to detect endpoint threats***
- ***Verify advanced threats* — *Leverage threat intelligence and ISACs to drive effective EDR***
- ***Automation and integration* — *Get faster, more precise threat detection and response by improving security and IT collaboration***

Open the book and find:

- **Specific steps you can take right now to detect and contain endpoint attacks**
- **How to combine threat intelligence and automation into a potent weapon against cyber attackers**
- **Why integrated security solutions act as force multipliers in endpoint defense**
- **Save time and money using deep visibility into endpoint state and behavior to drive threat response priorities**

Go to Dummies.com® for more!

Ed Tittel is an author, trainer, and consultant with more than 100 technology books to his credit. **Gajraj Singh** is Vice President—Product Marketing at Tripwire, a leading security and compliance company, and a security veteran.

FOR DUMMIES® A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-26231-2
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.