Brought to you by:

ManageEngine
Endpoint Central

Endpoint Security

for dummies®
A Wiley Brand

Manage your attack surface

Build cyber-resilience

Leverage AI and ML for security

Endpoint Central
20th Anniversary
Special Edition

Audrey O'Shea

About ManageEngine Endpoint Central

ManageEngine Endpoint Central is an endpoint management and security solution that offers end-to-end device life cycle management, along with security capabilities like attack surface management, endpoint protection, threat detection and response, and compliance governance. Remote troubleshooting, self-service capabilities, and proactive analytics help reduce downtime and improve the overall end-user experience. Available both on-premises and as an SaaS solution, Endpoint Central is used by more than 30,000 enterprises globally, fitting perfectly into their existing IT infrastructures and enabling interoperability. For more information, visit manageengine.com/endpoint-central.

"With attacks increasingly sophisticated and relentless, and the network perimeter dissolving, it's more important than ever to learn how cybercriminals are exploiting a wide range of attack vectors - and how your business should respond. This book explains how you can go beyond relying on legacy defences, and use modern technology, real-time monitoring, behaviour analysis, and threat intelligence to detect, block, and respond to threats."

— Graham Cluley, cybersecurity expert

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Endpoint Security

Endpoint Central 20th Anniversary Special Edition

by Audrey O'Shea

for dummies®
A Wiley Brand

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Endpoint Security For Dummies®, Endpoint Central 20th Anniversary Special Edition

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

Copyright © 2026 by John Wiley & Sons, Inc., Hoboken, New Jersey. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.dummies.com/custom-solutions. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-32908-3 (pbk); ISBN 978-1-394-32909-0 (ebk); ISBN 978-1-394-32910-6 (ePub)

Publisher's Acknowledgments

Development Editor: Rachael Chilvers

Project Editor: Tamilmani Varadharaj

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager: Matt Cox

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

If you're finding yourself trying to protect more company assets with less, you've come to the right place for help. Cybersecurity is always changing. Cybercriminals are leveraging AI and devising new and more effective attack vectors daily.

Cyberheroes and IT decision makers need to be armed with the right information to stay a step ahead of cybercriminals, and this book intends to help you do just that.

About This Book

This book helps you understand how the cybersecurity environment is changing and the steps you can take to create a more secure environment now and as future trends emerge. It's designed to enrich your knowledge and help you understand current trends. You'll learn the importance of endpoint security and provide pointers to help you build a culture of cyber resilience. The information should be of particular interest to people in the following job roles:

- **IT decision makers.** Gain a better understanding of the nitty-gritty aspects of cybersecurity and what tools can provide better protection while streamlining IT activities.
- **IT managers.** Although there's no silver bullet, there are things you can do to improve your odds of successfully preventing a cyberattack. Learn about advanced tools to stay lean and resilient.
- **SysAdmins and IT technicians.** Gain a better understanding of the big picture and how you can foster a more secure environment.
- **C-Suite/director.** Learn the jargon and acronyms of cybersecurity. Gain an understanding of the challenges faced by cybersecurity professionals, examine tools to help them become more efficient and effective, and explore the return on investment (ROI) of artificial intelligence (AI) investments.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Icons Used in This Book

This book uses the following icons to point out particularly noteworthy information:

Tip icons provide practical advice or point out important concepts that can make your life easier.

Remember these key concepts that are extra-important.

Warnings alert you to dangers you may face along the way.

Beyond the Book

Staying current in cybersecurity can be challenging. To leverage the knowledge and experience of other IT professionals consider the following feeds:

- AlienVault (OTX)
- Krebs on Security
- Graham Cluley

For a plethora of informative articles and videos on endpoint security, visit `www.manageengine.com/endpointcentral`.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Seeing what today's cybersecurity professionals are facing
- Decoding different types of attacks and their behavior
- Going inside the mind of an attacker

Chapter 1
Stating the Current State of Endpoint Security

The stakes are high in cybersecurity. Every year companies lose millions of their profits to cybercriminals. It's not only money that's lost, but also reputations, lawsuits, and sometimes whole companies succumb to the success of cybercriminals.

Identifying the Current Threat Landscape

Cybercriminals are rapidly adapting to changes in technology, and businesses must too. There aren't enough skilled cybersecurity professionals to fill vacant positions, so you need to find ways to make cybersecurity more streamlined.

Rising cyberattacks

It's no secret that cyberattacks are on the rise, with multiple studies showing a year-over-year increase of more than 30 percent in the number of attacks from 2023 to 2024. Ransomware, which locks systems until a ransom is paid, has become such a problem that countries are banding together to fight it. TRM Labs, an organization supporting countries and financial institutions in fighting cyber theft, stated that just one bad actor, LockBit, stole

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

£160 million using ransomware. That's just one ransomware criminal out of many.

Ransomware-as-a-service (RaaS), where thieves don't even have to do their own coding to attack unsuspecting organizations, is also on the increase. Ransomware aside, breaches are increasing, with many of them happening in the cloud. IoT malware attacks have doubled in the past year, likely because they are the easiest endpoint to hack. Business email compromises are up 70 percent, and the PowerShell tool that's so useful to IT is being used and abused for criminal pursuits. Dealing with phishing through unwanted phone calls and emails is a daily occurrence for many people.

Finally, as reported by ManageEngine, there were 90 zero-day vulnerabilities exploited in 2024. That's a zero-day attack every four days!

Moving the perimeter

Hybrid work models are making corporate security more challenging than ever. With data spread across clouds, end users working remotely, and endpoints everywhere, the traditional IT perimeter is dissolving — and it's up to you, the cybersecurity expert, to secure it all. In a bring-your-own-device (BYOD) world you likely have smartphones, tablets, and internet-of-things (IoT) devices holding data in addition to data stored in the cloud, on company laptops, desktop computers, and servers.

WARNING

Shadow IT is comprised of devices, software, or services (like software-as-a-service, or SaaS) that you haven't approved, or perhaps don't know about yet, which are attached to your organization and its data.

There's also shadow data that's either intentionally or accidentally stored on unapproved personal devices or forgotten copies of older data such as old backups and data kept "just in case" when new systems are employed. Shadow data can exist in unsanctioned places on company computers where someone has downloaded it for their convenience, or perhaps on a computer at home where work and home use have merged. Productivity tools, a proliferation of cloud storage platforms, and user-friendly collaboration tools are also places where your data may be hiding.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Luckily data discovery tools can help you. Software to manage the threat of shadow data should be able to:

- Monitor incoming and outgoing traffic from websites and servers and stop any traffic that isn't authorized
- Enforce strong encryption on any corporate data in transit or at rest
- Categorize online applications as approved or not, and provide an interface for removing disallowed apps
- Monitor and analyze user data activity to identify internal threats

TIP

An example of this type of software is ManageEngine Endpoint Central.

In addition, companies must have a comprehensive acceptable use policy that employees agree to as part of their onboarding process. This policy should address what staff are and aren't allowed to do with your data. New hires need security awareness training to prevent potential problems and foster a climate of security consciousness.

Protecting more

As technology advances and drives adoption, the world becomes smaller with companies working globally rather than locally. Your data is now in the cloud, on multiple systems and networks, and sometimes in multiple countries.

Not only is the location of your data expanding, but data itself is growing at an exponential rate, measured in zettabytes. Consider all the data generated by just your organization: sales transactions, streaming, research data, enterprise resource planning (ERP) and customer relationship management (CRM) systems, to name just a few. Imagine the consequences if sensitive data is lost. For a hospital, losing patient records means compromising health and trust; for a civil construction company, losing SOPs and contract details could lead to project delays, legal issues, and lost business. Every piece of data has value and carries potential risks — making its protection essential to ensure continuity and trust.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Deconstructing an Attack

REMEMBER

Two terms you'll hear often in cybersecurity are *attack vector* and *attack surface*. An attack vector describes *how* the attack is done, and an attack surface is *where*. For example, if you have employees with devices worldwide, then you have a very large attack surface. If an attacker used social engineering to get login credentials from an employee, then social engineering is the attack vector.

Different types of malware cause different problems. The problems they inflict are called the *payload*. A payload can be anything from a funny pop-up to annoying adware to truly catastrophic problems for a company. Here are some common attack types and what they do:

- **Virus.** A virus moves from system to system attached to something else, like an email, a shared file, or a macro. Polymorphic viruses change themselves in an attempt to hide from antivirus.
- **Worm.** Worms don't need to piggyback on another file. Once they're in a network they can spread across it, resulting in a slow or non-functioning network.
- **Trojan.** A trojan is attached to an app that a user downloads and installs on their system. Sometimes they know the trojan is there because of its activities, but other times the trojan's job is to create a backdoor; a hidden entry point that an attacker can use later to access a system.
- **Spyware.** Spyware's job is to watch you and gather information about you. Often spyware is used to send targeted advertisements, but it's also used to record your keystrokes. In that situation, it's a keylogger and can record banking information, usernames, passwords, and personally identifiable information (PII) that can be used to steal your money, identity, or access to the company's sensitive data.
- **Adware.** Adware can get into your system when you click a bad link or by visiting a questionable website. Once it's in your system it will continually pop up advertisements. Usually, adware is just very annoying but it can interfere with employee productivity.
- **Rootkit.** Rootkits are spread by any method available and will hide in the basic input/output system (BIOS) where they're notoriously difficult to find and eradicate.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Botnet.** A botnet is a group of computers that have been infected for a specific purpose. They're managed by a botherder and may sit dormant for weeks or months until the botherder gives the signal to attack. Botnets are often used to inflict distributed denial of service (DDoS) attacks that flood a server with requests so legitimate users can't access it.

Newer attack types include the following:

- **Fileless attacks.** Fileless malware hides from traditional, signature-based antimalware programs by residing in memory, where it leaves little or no trace of its presence.
- **Cryptojacking.** Cryptojacking attacks infiltrate a computer to use its resources for mining cryptocurrency. The computer may be nearly impossible for the user to run because its processing power is being used by the hacker.
- **Ransomware.** Ransomware is the bane of modern organizations. It infiltrates a system, then will lock it down until the organization pays a ransom, usually in cryptocurrency.

Cyberattacks can result in loss of money, intellectual property, or reputation, and even lawsuits or other legal consequences.

Thinking Like an Attacker

Know your enemy! If you want to outsmart an attacker, you first need to understand them.

Understanding their motivations

In the early days of computing and the internet, hackers were hacking for the thrill, bragging rights, or the personal satisfaction of knowing they could do it. While financial gain has always been a driving force behind cyberattacks, it was historically difficult for attackers to extract money directly from their targets. However, the rise of cryptocurrency has dramatically changed this, providing a secure and anonymous method for cybercriminals to receive payment. In today's ransomware-as-a-service environment, financial motives have become the predominant driver of attacks. Occasionally the objective is to access data or corporate intellectual property and sell it to someone else, engaging in corporate espionage.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

If a hacker is out for revenge, they may disrupt operations with a DDoS attack or ransomware lockdown.

Visualizing the attack process

Attacks tend to follow the same pattern, as illustrated in the Figure 1-1.

FIGURE 1-1: The pattern of an attack.

Attackers begin by doing reconnaissance and finding a loophole or a weakness (also known as vulnerability), exploiting the weakness to access the system, and deploying their attack. At the expansion stage, an attacker often uses lateral movement to get deeper into the system. Lateral movement happens when a bad actor logs in with stolen user credentials, then moves through a system from the device to software to the network, working their way through the victim's network to acquire more credentials (such as domain admin control), sensitive information, install a backdoor, or install their payload such as ransomware.

WARNING

Backdoors enable the attacker to revisit the compromised system in the future to gather more information or when they're ready to attack with ransomware or other payloads.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

ATTACKING TRENDS

Attackers are always devising new ways to break in:

- **SEO poisoning.** Attackers often have their own websites for the purpose of enticing unsuspecting people to visit and click something, unwittingly downloading and installing malware on their system. Search engine optimization (SEO) is poisoned by bad actors who use SEO algorithms to force their websites up on the search engine's list in the hopes of increasing traffic to their websites.
- **AI.** Attackers use AI to increase their speed in finding vulnerabilities and exploiting them. That means that cybersecurity needs to employ AI to stop them. It's like an arms race going on in cyberspace. (The rest of this book has more information about using AI to protect your organization from cybercriminals).
- **IoT.** IoT devices are everywhere, and notoriously easy to hack into. Bad actors will take advantage of them whenever they can.
- **Cyber-physical.** These attacks, such as bringing down power grids, traffic lights, or subways, are becoming more common. They use cyber means but have the potential to cause physical damage to property and large groups of people.
- **Supply chain attacks.** Cybercriminals are attacking supply chains to find a path that will enable them to attack their real target, a larger company.

A theoretical threat on the horizon is cybercriminals using quantum computing to crack encryption schemes. At that point, we'll need to employ quantum computing to block attacks, like using AI security to block AI attackers now.

PROTECTING TRENDS

The cyber heroes have their own trends and stars on the horizon to look forward to:

- **Attack surface management (ASM)** is a different way of approaching cybersecurity. With attack surfaces growing at exponential rates, and the corporate perimeter being a thing of the past, cyber heroes are turning the tables and looking at their

(continued)

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

(continued)

systems from an attacker's point of view. They often use the same tools that attackers do in an attempt to beat them at their own game, paying attention to social engineering and vulnerabilities at endpoints. Endpoints, after all, are where everything happens.

- **External ASM (EASM)** does the same thing as ASM with the caveat that the focus is on external, as in internet-facing, surfaces. External IT assets are anything accessible by the public such as web servers, email and file transfer protocol (FTP) servers, virtual private network (VPN) gateways, remote desktop protocol (RDP) servers, and domain controllers. Again, these endpoints need to be secured.
- **Endpoint Protection Platform (EPP)** offers integrated security features such as antivirus, anti-ransomware, and device control. EPPs are designed to protect endpoints from known and unknown threats while providing real-time protection and automated response capabilities. By proactively defending endpoints, EPP solutions offer a strong line of defense against threats like ransomware.
- **Endpoint Detection and Response (EDR)** takes endpoint security a step further by focusing on continuous monitoring, detection, and real-time response. Unlike EPP, which prevents attacks, EDR is like a CCTV camera that's always on, providing visibility and analytics, enabling security teams to detect and respond to suspicious activity that might bypass traditional security measures. EDR is an essential component for rapid incident response and threat mitigation, giving organizations a much-needed advantage in identifying and neutralizing attacks quickly.
- **Extended Detection and Response (XDR)** builds on EDR and integrates data from multiple security layers — network, endpoint, server, and cloud — to provide a comprehensive view of the organization's security landscape. By correlating and analyzing data across multiple environments, XDR helps security teams detect threats more quickly, prioritize responses, and improve the overall security posture through centralized visibility.

Endpoint security is the focus of successful cybersecurity because endpoints are your organization's attack surfaces; the places where everything happens.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Knowing why visibility is important
- Improving security posture
- How and why to layer security

Chapter 2
Building Resilient Cybersecurity

Cyberattacks can happen to any organization at any time, and with attackers getting more sophisticated, some even offering ransomware-as-a service, even those who don't have the technical skills can get into the bad actor game by hiring an "expert" attacker. The flexibility of attackers and deluge of new attack vectors mean that cybersecurity teams can no longer merely monitor and react to threats. You need to employ proactive measures.

For an organization's cybersecurity team, building a secure and resilient environment is your best defense against the enemy at your gates, on your virtual private networks (VPNs), or even your employee's email inbox. Before you can employ endpoint security, you need visibility.

Seeing Potential Problems

"You can't protect what you can't see" is a phrase often heard in the cybersecurity world, but what does that mean? For security to be successful, a cybersecurity team needs to have a full account of

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

all the data belonging to their organization. You need to see what people are doing with that data and who has access to it, but first, you need to find it.

Challenging situations

Today's networks have become extremely complex compared to the networks of a decade ago, or even pre-pandemic time. They include on-site and remote workers, bring-your-own-device (BYOD) challenges, data at rest and in transit, data and applications in the cloud, on servers, virtual machines, and internet of things (IoT) devices. As networks have grown and become more complex and distributed, and attackers have become more sophisticated, monitoring a network, its data and devices has become an astronomical task, and working reactively isn't enough.

Cybersecurity professionals need to provide preventive and preemptive security and defense, but before you can do that, you need network visibility. You need to know about and be able to monitor all digital assets including devices, apps, and how data flows from one platform to another. You need a clear vision of everything you're required to protect, all the while maintaining compliance with standards and government regulations, mitigating the unmanaged devices of shadow IT, and avoiding ransomware attacks.

WARNING

Appropriate encryption is vital in today's networks. Having a single unencrypted, unpatched, or misconfigured device adds vulnerability to your system and increases your organization's attack surface. However, sometimes encryption aimed at blocking threat actors has the unintended effect of blinding the cybersecurity team to what's happening or what isn't protected. It can obscure threats from security teams, making it difficult to detect vulnerabilities or suspicious activities within the network. Lacking sophisticated software and means to monitor the entire network is like trying to score a goal in the dark.

Remediating vulnerabilities

There are several points of failure that result in your data being more vulnerable to attack. Here are some of the most common:

- **Patching.** If a software company has issued a patch, then they've already detected a vulnerability that needs to be remediated. Be sure to keep all systems patching up to date.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Misconfigurations.** Misconfigurations can provide an open door to attackers. Ensure that everything attached to your network is configured properly.
- **Browser security.** Attackers jump for joy over unsecured browsers because they provide attackers with a multitude of possibilities for infiltrating your network. Attackers can use unsecured browsers to trick users into installing spyware or other malware on your system, steal sensitive data, and execute phishing attacks. Here again it's important to keep updates current and properly configure browsers. Training users at endpoints is also a must.
- **Application control.** If users can install or run applications of their choice on devices, then potentially anything could happen. Ensuring that only approved applications can be installed or run on attached devices mitigates the possibility of problems from unauthorized applications.
- **Encryption.** The quality of your encryption determines whether your data is visible to others or not. Ensure that you're using up-to-date encryption and that your encryption key(s) haven't been compromised. If they are, you're in an emergency situation and need to solve the problem immediately.
- **Data loss prevention (DLP).** DLP involves discovery and analysis of data so you know what's sensitive and can see data leaks as they happen. Finding the leak means you can put a cork in it immediately!
- **Endpoint privilege management (EPM).** The principle of least privilege means that users only have access to what they need, and only when needed. EMP requires users to ask for and attain access to sensitive data on an as-needed basis. It can also provide an audit trail of access to sensitive data, and credential management.
- **Vulnerability remediation.** If vulnerabilities are identified but not remediated, then the attack surface remains unchanged.

Without taking these measures and remediating the vulnerabilities, it isn't a question of whether your organization will be attacked. The question is when and how much damage will be done.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Unremediated vulnerabilities have serious consequences that can include data and financial losses, as well as lawsuits, damaged organization reputation, and fired employees. Finding and remediating vulnerabilities is the foundation of cybersecurity.

Practicing Better Security Posture from an Endpoint Standpoint

Previously, good security focused on devices and meant reacting quickly to known problems. Today, that isn't enough. You need to take a holistic, proactive, and preventive approach. Enter *data security posture management* (DSPM). Rather than focus on just devices, DSPM focuses on data residing in those endpoints and its security.

Before you can protect your data, follow these steps:

1. **Discover.** Get a clear picture of where data resides and who has what access to it. Data may be in the cloud, on a server, or on an endpoint. A good DSPM solution finds data where it lives. Once it's found, it can be analyzed and shadow data minimized.
2. **Classify.** Classify data by sensitivity. The sensitivity classification levels can assist in developing data loss prevention (DLP) policy and choosing the response actions based on that classification should the data be breached.
3. **Assess risk.** Assess the risk to the data and prioritize security measures on that data. Risks are varied; for example, data being stored in inappropriate locations, users having too much access, or needed security policies and configurations not being applied.
4. **Prevent loss.** The fourth and final step is to fix any problems that are found, and in doing so, proactively mitigate your attack surface and potential risks. Beyond that you'll want software to provide real-time alerts when there are occurrences such as unauthorized permission changes or potential ransomware is detected.

TIP

DSPM can be an intense and difficult process for IT personnel. Finding and analyzing a company's data and shadow data is time-consuming, labor-intensive, and susceptible to human error. To mitigate the time and trouble involved, look for an excellent software solution to make the task easier and more efficient.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Layering and Endpoint Security

An endpoint exists at any device where access to a network can occur. This may be a server or workstation, even if they are virtual. Remote devices like smartphones, tablets, and even IoT appliances are endpoints that could potentially provide an attack surface. Endpoints are where all the action happens, and unprotected endpoints need to be protected from attacks, but what is the best way to secure them?

If you install a firewall between the internet and your organization's network, and think you're secure, ask yourself how that will protect remote devices from being compromised. It can filter traffic coming into your network, but not protect against someone accessing a remote user's browser and installing malware that can attack the network it's attached to.

TIP

The answer is to provide many roadblocks along the way to your sensitive data. This is called *layered security*.

Placing layers

To be effective, layers need to be placed at several spots. Here are areas to consider:

- **Devices.** Consider using antivirus, encryption, and firewalls.
- **Identities.** Multifactor authentication (MFA) is a necessity to help ensure that the person or device logging into your system is in fact that person or device. Require complex passwords and ensure that your environment is a zero-trust environment, where no person or device is assumed to be trusted. Always require authentication before providing access and ensure that you have visibility into user activity.
- **Applications.** Patching must be up to date. Input validation and ensuring that coding is secure are also ways to protect your system at the application level.
- **Networks.** Firewalls and intrusion detection and protection systems (IDPS) need to be employed here. Monitor your network traffic for suspicious activity. Segmenting and encrypting network traffic are also best practices.
- **Data.** The data that you want to protect must be encrypted whether it's in transit or at rest.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Layering at endpoints

Endpoints are the center of the maelstrom because that's where attackers get into your network, so endpoints need particular attention when it comes to layering security. Here are some actions you should take:

- Configure firewalls, email filtering, and encryption
- Require MFA and complex passwords
- Perform patch management
- Vet peripheral devices and removable storage
- Establish web content filters and download filters
- Monitor browser extensions and application privileges
- Ensure regular patch cycles
- Perform application blocklisting/safelisting
- Install security policies
- Train users to identify potential attack attempts such as phishing

TIP

Layering security at endpoints when you have hundreds or thousands of users can be a daunting task. One solution is to find endpoint management software to relieve much of the burden and provide a central point for managers to control endpoint security, such as Endpoint Central by ManageEngine.

ADDRESSING VERTICAL MARKET NEEDS

All organizations have the same basic security needs, but certain vertical markets have additional needs to address.

Healthcare. Endpoint security in healthcare is integral to protecting patient health data and complying with government regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

Education. Educational institutions have many and diverse endpoints to protect. An attack on a school could hinder classroom activities and expose student records and staff credentials. Schools are often

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

subject to different government mandates that require carefully monitoring to ensure compliance.

Government. Cybersecurity attacks on governments can be far-reaching because they have data that helps the government function and relates to national security, supply chains, and citizens alike. Their endpoints are many and diverse.

Enterprise. Centralized endpoint security in an enterprise can enhance employee productivity; enforce compliance; secure remote devices, applications and data; automate patch management; and manage mobile devices, saving an enterprise both time and money while providing security across the board.

Checking the Endpoint Security List for CISOs and Admins

Regardless of your position in an organization's IT department, you can play a vital role in enhancing or maintaining security. Here are two checklists to consider:

Checklist for CISOs

CISOs (Chief Information Security Officers) handle the "big picture" items in the cybersecurity to-do list such as:

- Ensuring regulatory compliance
- Incident response planning and documentation
- Creating acceptable use and other policies
- Determining and documenting cybersecurity strategy
- Planning for disaster recovery
- Creating and ensuring security awareness training
- Creating and documenting cybersecurity and endpoint protection strategy
- Continuous attack surface reduction and management
- Threat intelligence and monitoring
- Supply chain and third-party risk management
- Tracking KPIs and measuring ROI with metrics and reports

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Endpoints are your attack surface and an important part of maintaining cybersecurity daily.

Checklist for admins

Admins and SysOps are often the first line of defense and responsible for daily security tasks like:

- Ensuring backups are done and tested
- Performing/reviewing vulnerability scans
- Investigating alerts and suspicious activities
- Ensuring all endpoints are properly configured, patched, and software updated
- Monitoring for unauthorized devices
- Performing incident response
- Onboarding new employees following policies and procedures and conducting security awareness training
- Enabling and enacting baseline security
- Detecting and denying unauthorized software/application
- Ensuring the encryption of endpoints and removable media
- Enforcing MFA on endpoints
- Revoking unnecessary access privileges
- Leveraging automation for time-sensitive activities such as patch management
- Tracking key metrics such as compliance rates and security status

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Going beyond layered security
- Thwarting advanced threats
- The good, the bad, and the ROI of AI
- Cybersecurity and the future

Chapter 3
Achieving Cyber-resilience with AI-based Endpoint Security

A layered approach to security with roadblocks at the data, network, device, and user login is a great starting point, but there's more work to be done and precautions to take to keep your system safe. This chapter takes a look at those.

Transcending the Layered Approach

Perhaps you've heard the phrase "unknown unknowns." It means that some things are so new, unexpected, or outside your awareness that you don't know specific steps to protect your system against them. For example, before the first ransomware, would you have had a plan to protect against or react to it?

Unfortunately, attackers are continually devising new malware and schemes to damage your organization or reputation. Fortunately, you can take steps to help prevent being caught off guard by the advanced threats of unknown unknowns. To stay ahead of them, you need to go beyond layers of protection and

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

traditional antivirus (AV), which uses known virus signatures to block malware, especially ransomware.


TIP

Instead of using known signatures, next-generation AV (NGAV) software leverages artificial intelligence (AI) and machine learning (ML) to detect unusual activity or behavior to identify malware, even fileless malware that does its dirty work in system memory.

Protecting Against Advanced Threats: A Blueprint

Protecting against advanced threats isn't a one-and-done adventure. It's more like a building with different rooms that you enter regularly. Each one does its part in building the whole. Protecting systems against advanced threats requires the following components, as shown in Figure 3-1:

- **Threat intelligence**. Threat intelligence involves the collection, analysis, and sharing of data related to malicious actors, tools, and tactics, enabling businesses to anticipate and mitigate potential attacks before they cause harm. It relies on sources such as the AlienVault Open Threat Exchange, MISP (Malware Information Sharing Platform), and STIX/TAXII feed (see the nearby sidebar) to share and identify characteristics of newly discovered threats so measures can be taken to protect against them.
- **Machine learning (ML) behavior monitoring.** Continuous ML-based behavior monitoring in real-time looks for behavior patterns and reports on deviations from what it has learned is normal for a system.
- **Detection and response.** Detection takes information from threat intelligence and behavior monitoring to identify potential threats and take preemptive action to prevent them from damaging systems and data.
- **Remediation.** Just as it sounds, remediation means putting systems back to the state they were before the incident occurred. It also includes isolating and disinfecting the malware or threat and revert files and registry values.
- **Forensics.** Forensics is an analysis of what happened and how it was done after the fact. It uses digital evidence that's collected and analyzed to prevent similar future attacks.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

THE STIX/TAXII FEED

Structured Threat Information eXpression (STIX) provides a standard for exchanging information about cyber threats worldwide. Trusted Automated eXchange of Intelligence Information (TAXII) is a transport protocol that supports sharing STIX information. STIX/TAXII provides a method for organizations to share threat information through a common repository which aids in threat hunting and detection. A nonprofit organization called OASIS manages the repository and feed where IT professionals can upload and download threat information.

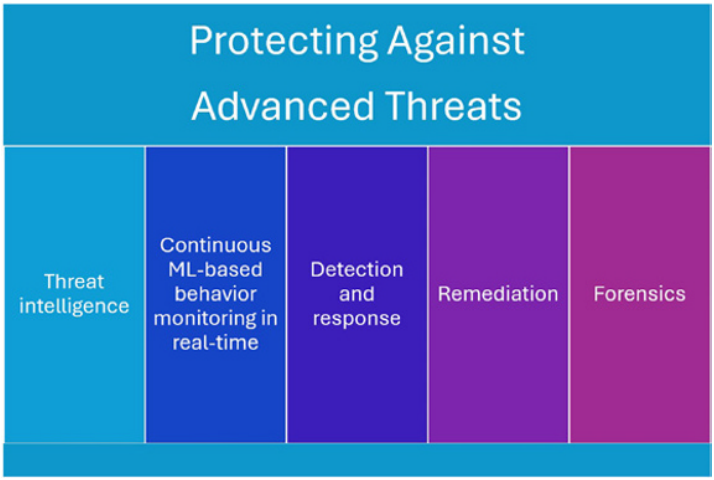

FIGURE 3-1: Protecting against advanced threats.

Banishing Malware and Ransomware

Banishing malware and ransomware requires many types of protection. Some measures are proactive; others are preemptive.

- **Proactive** measures are the actions you can take before a problem happens, such as ensuring you have current antivirus software.
- **Preemptive** actions are performed as an attack is happening, or at the beginning of the attack, to mitigate the damage the attack does.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Whether proactive or preemptive, both types require planning in advance and the right tools to be effective.

Flexing proactive muscles

In the cybersecurity world, you have several proactive actions to protect endpoints and precious data, including:

- **Risk assessment.** Inventory, classify, analyze, and protect sensitive data. Risk assessment can help with regulatory compliance and help you prevent loss of critical data.
- **Patch management.** Keep software, operating systems, and firmware updated to eliminate vulnerabilities.
- **Application safelisting.** Block end users from installing unapproved software. Allow only approved software to run on systems to prevent malicious executions.
- **USB and external media restrictions.** Control access to removable media to prevent malware infiltration.
- **Antivirus.** Ensure that your antivirus software is updated and running on all devices.

  
  REMEMBER

  Today's new generation antivirus isn't the antivirus of your ancestors. Modern antivirus leverages the power of AI and ML in a behavior-based approach rather than the file-based approach of old that relied on virus signatures. Antivirus can be both preemptive and proactive.
- **Firewalls.** Firewalls filter traffic at the entrance to your network and on each device attached to the network.
- **Backups.** If disaster strikes and there's no backup, all is lost. You must define your backup strategy long before you need it. Some ransomware attempts to erase or damage backups before the ransomware locks your system, so ensure that you have a backup in the cloud or are otherwise not connected to your network. When planning your strategy, remember that anything generated after your last backup will be lost. Create and follow your backup plan as if you will be attacked.
- **Business continuation.** Ensure you have a plan for business continuation if you're hit by ransomware or another disaster. What steps will you follow to get your company up and running? Update this plan at least annually.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Awareness training.** Train end users to recognize potential attacks and how to react to them. Have a procedure for them to follow and train on that as well. Repeat training at least annually and as a part of the onboarding process.
- **Testing end users.** Use a service or software that sends phishing emails to test how end users react. If they take the bait, they need further training in recognizing dangers.
- **Use virtual private networks (VPNs) in public places.** Configure VPNs and train employees to use them when connecting to your network in public places instead of their favorite coffee shop's wide-open Wi-Fi.
- **Limit user access.** Ensure that users have access only to what they need to do their work. If their login is compromised, you want the attacker's reach to be limited.
- **Browser choices.** Choose a browser for your organization that's secure and updated/patched appropriately, then enforce strict browsing policies.
- **Penetration testing.** You think you're all set with your security, so it's time to test it before someone else does. This enables you to identify and plug holes in your security.
- **Avoid admin logins.** Ensure that IT department employees have a standard user login and only elevate permissions to admin when required. Provide training.

Flexing preemptive muscles

Preemptive activities attempt to stop a malware attack as it's happening. Preemptive activities are most effective if employed when the attack first starts. Here are some examples of preemptive activities:

- **Endpoint detection and response (EDR) software.** EDR solutions go beyond what antivirus can do, using ML and AI to spot anomalies in behavior and even disable processes being used to perpetuate an attack. EDR can also provide detailed real-time alerts and analysis, enabling cybersecurity teams to take immediate action and to create comprehensive plans to avoid the threat in the future.
- **NGAV.** NGAV leverages AI and ML to detect and act upon previously unknown malware and zero day threats.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Threat hunting.** Threat hunting means actively seeking ongoing or previously unknown threats. Most cyber threats can lurk in a system for weeks or months before they're noticed, as attackers steal credentials and data.


TIP

Threat hunting is tricky as it demands speed, skill, and constant vigilance, which is why some organizations outsource the job to Managed Detection and Response (MDR) providers who specialize in detecting and neutralizing threats in real time.

Using AI to Counter AI Threats

As threat actors become more sophisticated and use AI tools, organizations must keep pace to protect their systems. In this section, you see why AI is like a two-edged sword.

AI's dark side

On the bad side, threat actors use AI to enhance their existing tools to create better phishing and social engineering attacks by quickly generating more realistic emails. Attackers also use AI to search for systems' vulnerabilities faster and to code new malware. AI takes impersonation schemes further by generating realistic audio and video to mimic family and coworkers to trick victims into providing credentials or personally identifiable information (PII), or even authorizing bank transactions to separate people from their money.


WARNING

According to the recent IBM Cost of a Data Breach Report 2024, the cost of a data breach was a whopping US$4.9 million on average, worldwide. Some organizations' losses were much higher, and losses in the United States tended to be double that amount.

AI's bright side


TIP

On the good side, organizations can leverage the power of AI in several ways to improve their security:

- **Speed.** The same speed advantage of AI that helps attackers wreak havoc on your systems can help you find malware and attack faster and automate reactions. For instance, NGAV uses AI to work based on behavior instead of using static signature files.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Prioritization.** AI can analyze and prioritize security alerts, freeing IT personnel to act on the alerts.
- **Reduce false positives.** Detailed response alerts from AI help reduce false positives. For instance, there may be a legitimate process or two in multiple incidents detected by an anti-malware solution.
- **Pattern and anomaly detection.** AI can quickly identify user activities or use patterns that deviate from a baseline, enabling preemptive responses to threats. This is especially useful in patch management, where AI can automate test group creation and block misaligned patches when there's a deviation from the baseline. This ensures maximum compliance in minimal time, preventing disruptions.
- **Attack path prediction.** AI can simulate potential attack chains, identifying which systems are likely to be targeted next. This allows security teams to proactively isolate high-risk endpoints, close lateral movement paths, and strengthen defenses before an attacker can exploit them.

The bottom line is that threat actors leverage the power of AI to configure their attacks, and without leveraging that power to defend your organization, you're more likely to become the next victim.

Measuring the effectiveness of AI-based endpoint security

Calculating the gains from implementing AI in your endpoint security stack can be a bit tricky and elusive. How do you measure the value of a corporation's reputation until it's damaged and the drop in sales is palpable? AI's impact lies in both tangible metrics and hard-to-quantify but critical benefits.

Key performance indicators (tangible benefits) include:

- **Mean time to detect (MTTD):** How quickly threats are identified.
- **Mean time to resolve (MTTR):** The speed at which incidents are mitigated (achieving patch compliance, for example).
- **Intrusion prevention metrics:** The volume of attempted attacks detected and blocked.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Beyond these, AI delivers intangible yet invaluable advantages, such as:

- **Proactive risk assessment:** Identifying vulnerabilities before they become crises.
- **Enhanced compliance and reporting:** Granular regulatory processes and audits.
- **Optimized IT workforce efficiency:** Allowing teams to focus on strategic tasks instead of firefighting threats.
- **Faster decision-making:** Prioritizing security incidents based on real-time AI-driven risk analysis.

For some companies, the cost of not leveraging AI in security could be catastrophic, from disruptions to financial loss. In an era where cyber threats evolve by the second, AI is no longer an advantage — it's an imperative.

REMEMBER

According to the IBM report Cost of a Data Breach Report 2024, using automation and AI tools extensively saved corporations US$2.2 million.

Safeguarding the Future

Cybersecurity is about protecting the future. Keep up with changing compliance rules as the security landscape alters, the tide of ransomware attacks rises, and shadow IT and shadow data increase.

Tooling for success

This chapter has identified some key preemptive tools that you can use to protect your data including NGAV and EDR. You certainly want to leverage the power of AI for cybersecurity because the bad actors are using it, and you don't want to be their next victim.

Practicing cyber-resiliency

Just like fire drills and emergency readiness drills, excellence in cybersecurity requires practice. First, ensure that your corporate culture is one of security awareness and resilience. Activities to that end are:

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Training end users annually on security awareness
- Practicing mock attacks and responses
- Sending employees fake phishing emails and providing retraining as indicated
- Ensuring that you have a response playbook and that those involved are trained in how to take action if an incident occurs
- Subscribing to cybersecurity feeds to keep up with trends
- Encouraging a "Security-First" mindset by emphasizing that security isn't just IT's responsibility, but should be embedded into corporate culture
- Investing in AI-based endpoint protection and attack prevention for faster detection and response
- Enforcing strong identity and access controls: Implement MFA and zero-trust principles for enhanced security

REMEMBER

Building a culture of cybersecurity benefits everyone: Your customers, your suppliers, your partners, and your organization.

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Leveraging the power of AI
- Analyzing behavior
- Monitoring privileges

Chapter 4
(More than) Ten Things to Look for When Choosing an Endpoint Security Tool

Here are some considerations and features to help you choose the right endpoint security tool for you:

- **Compatibility and coverage.** Consider choosing a tool that consolidates all your endpoint requirements and supports multiple platforms. This is crucial to avoid tools sprawl and compatibility issues, ensuring maximum return on investment (ROI) and streamlined endpoint security.
- **Artificial intelligence (AI).** Does the tool leverage the abilities of AI to detect and mitigate threats autonomously? You'll need one that does because cybercriminals are already using AI to create and streamline their attacks.
- **Pain points.** Take time to create a list of your greatest pain points. Is it unifying your ITOps and SecOps? Is it budget? Determine which features would provide the best security

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

while streamlining your work, addressing your pain points, and improving security posture.

- **Patch and update management.** Keeping systems patched is a pain point for many organizations. Does the security tool automatically apply patches and updates to operating systems, applications, and mobile devices? Does it improve efficiency and reduce administrative overhead?
- **Vulnerability remediation.** Look for a security tool that can help you remediate vulnerabilities by scanning, providing a detailed analysis and prioritizing them for you.
- **Data security and privacy compliance.** Does the system you're considering detect and encrypt sensitive data, and classify the data based on data rules that you can define? Does the solution comply with privacy regulations like GDPR, CCPA, HIPAA, and ISO 27001 to ensure secure data handling?
- **Asset management.** Look for a tool with real-time discovery of hardware and software attached to your network so you'll know if someone attaches an unauthorized device to your network. It should also track warranties and notify you when licenses are about to expire. Trust certificate management is a plus.
- **Next-generation antivirus (NGAV).** Look for an endpoint tool that uses AI-enhanced next-gen antivirus to analyze behavior rather than rely on malware signatures.
- **Applications and browsers.** Does the endpoint security tool you're considering enable you to set installation permissions and monitor privileges? It must also provide data encryption and ensure that data is safe at rest and in transit. The ability to lockdown browsers to only approved websites, apps, and extensions is a must to prevent web-based attacks and infiltration attempts.
- **References.** Who are existing customers of the solution provider that you're considering? How long have they been customers? Can the solution provider supply recommendations from those customers?
- **Incident forensics and reporting.** Does the solution offer detailed incident forensics that provide valuable insights into the attack vectors and timeline via process trees? Does it offer comprehensive reporting so that it can help with compliance audits and post-attack analysis?

Best wishes to you for future success and cyber safety!

These materials are © 2026 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

ManageEngine
Endpoint Central

One platform. Total endpoint control.

20 YEARS of Endpoint Central

Manage, secure, and streamline every endpoint from a single console.

Endpoints are where business gets done and where threats often begin. Apart from being a standard IT hygiene practice, managing and securing these endpoints is mission critical. Endpoint Central delivers a unified approach to keep every device visible, compliant, and protected while ensuring users stay productive and secure.

Endpoint Central highlights

- Centralized endpoint management
- Real-time asset intelligence
- Patching and vulnerability remediation
- Next-gen antivirus
- Ransomware response and mitigation
- Continuous compliance management

Trusted by the best

31K+
customers

20 years
in the industry

26M+
endpoints managed

Across 180+
countries

Learn more

mnge.it/endpoints

Secure every endpoint and build cyber-resilience

With cybercrime constantly in the news and on the rise, endpoint security has never been more critical. Cybercriminals are rapidly adapting to changes in technology, and businesses must too. But with an ever-evolving threat landscape, how can you stay ahead of the attackers and protect your organization?

Endpoint Security For Dummies is your must-read guide to implementing a comprehensive endpoint security program to enhance your organization's security posture, protect against advanced threats, and banish malware and ransomware. Arm yourself with the information in this book to stay streets ahead of cybercriminals and protect your assets.

Inside...

- Understand the evolving threat landscape
- Think like an attacker to defend better
- Follow the checklists for CISOs and IT admins
- Utilize layered endpoint security
- Leverage AI to curb AI-based attacks
- Adopt an advanced threat protection blueprint
- Be future-ready with endpoint security tools

ManageEngine
Endpoint Central

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-394-32908-3
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

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