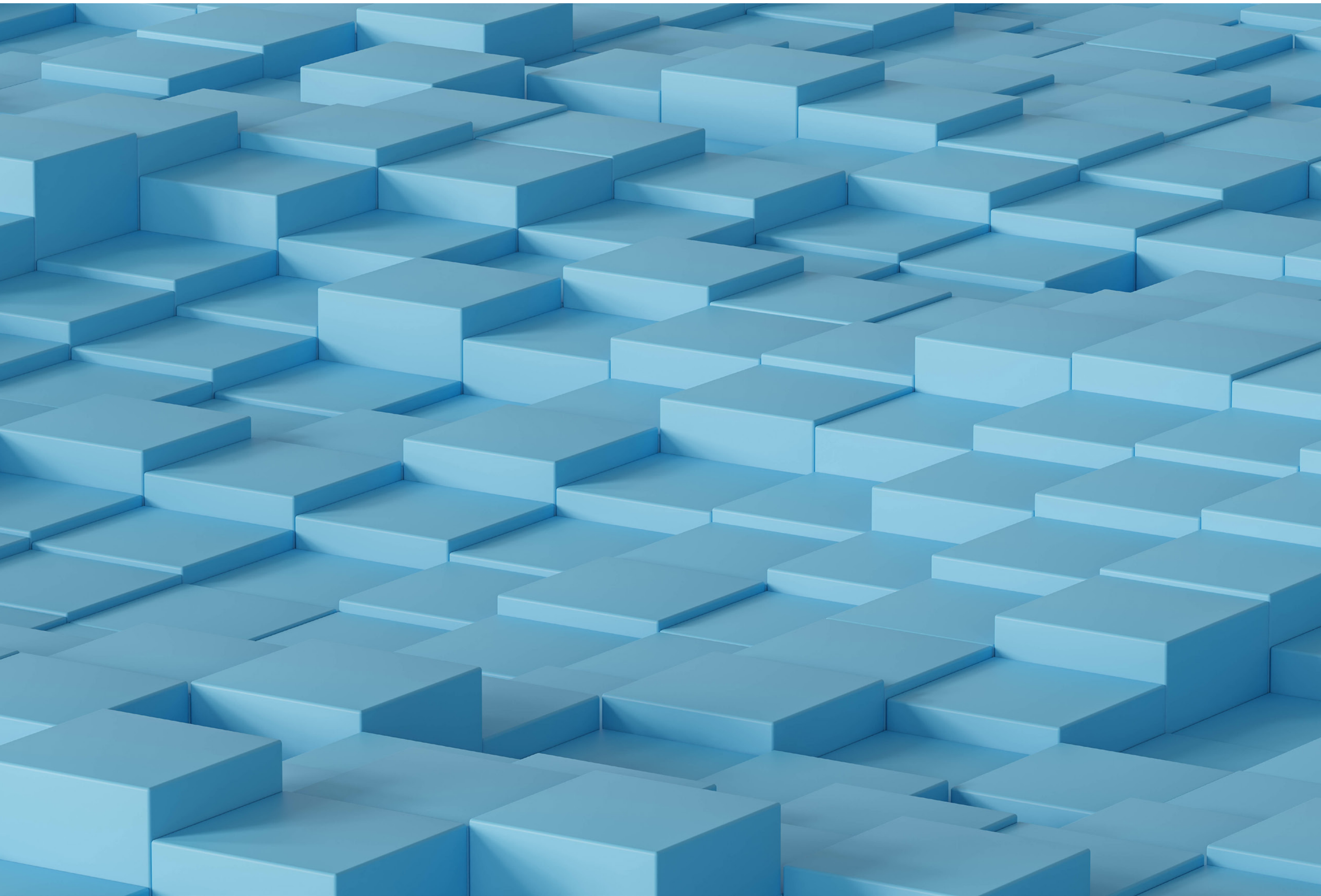
# Quick Start Guide to Endpoint Detection and Response

*Get up to speed with EDR and what it can do for your organization.*



# Protection in a world of endpoints

Over the past two decades, we have witnessed an exponential rise in the number of devices connecting to organizations' networks. From employee-owned smartphones to tablets to printers and smart TVs, these endpoints bring countless productivity benefits.

But they also introduce real danger.

All of these devices pose a threat to your organization's security. Every employee's personal devices, as well as company-issued tech and in-office equipment, are a potential 'backdoor' into your network.

And this is where Endpoint Detection and Response (EDR) comes in. The concept, which was first introduced in 2013 and is increasingly adopted by leading organizations, aims to address the risk that all these connected devices represent. It provides a variety of tools and techniques which help manage this proliferation in devices, and helps you adapt to the risks involved.

In this guide, you will learn **what EDR is** and **how to integrate it** into your wider cybersecurity posture.

## Internet of Things (IoT) Device Statistics at a Glance

**75 billion**
the estimated number of IoT devices connected to the web by 2025

**5.4 billion**
connected IoT devices from the consumer segment as of 2020

**3.17 billion**
China's connected IoT devices in 2020, leading all countries

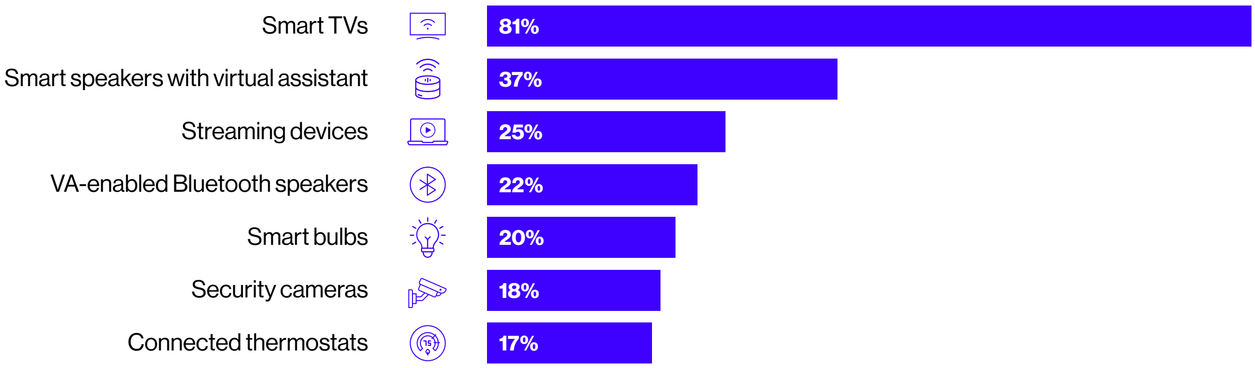
**127**
the number of new IoT devices connected to the web per second

**26.66 billion**
the number of active IoT devices worldwide as of 2020

**50%**
IoT platforms focused on industrial and manufacturing industries

**13.6 zettabytes**
data generated by IoT devices in 2019 alone

## Top Smart Home IoT Devices in the US, by Ownership



Original infographic source: Finances Online, 2021

# What is Endpoint Detection and Response?

Endpoint devices are frequently the primary target for cyber-attackers. According to a 2023 study[1], over three quarters of organizations have suffered at least one breach related to poor endpoint management.

To address this urgent need, the concept of an Endpoint Detection and Response (EDR) system has emerged. EDR aims to provide:

- A toolset to detect and prevent threats on network-connected devices.
- Deeper knowledge, insightful analytics, and superior protection.
- A pragmatic response to the reality that employees now use more devices than ever before.

EDR systems are engineered to monitor and respond to threats at the endpoint level. They do more than just detect threats; they actively analyze and investigate suspicious activities, offering a more proactive approach to cybersecurity.

## Key features of an EDR solution

- **Essential tasks:** Scanning, detecting, and removing malware.
- **Proactive tasks:** Blocking attacks and exploits against applications on devices.
- **Analysis:** Providing insights into threats with an overall analysis of the cause of the threat.
- **Search:** Quickly perform 'threat hunts' across the entire environment.

## How does EDR differ from traditional cybersecurity?

Endpoints are increasingly the primary method that cyber criminals exploit to enter their victims' systems. EDR therefore offers a pragmatic response to this reality. It differs from traditional anti-virus and firewall security postures in several ways:

- **Proactive:** Unlike traditional anti-virus technology, EDR proactively seeks out threats.
- **Detecting unknown threats:** Traditional anti-virus technology is only able to identify known threats. EDR uses a combination of machine learning and latest industry insight to identify unusual behavior on endpoints – including new types of malware.
- **Automation:** The most advanced EDR uses machine learning and automation. It not only alerts you to threats but can even neutralize them independently.

[1] Business Wire: More Than 75% of Organizations Have Experienced At least One Attack Related to Poor Endpoint Device Management, 2023

# Four key benefits of EDR

*Introducing EDR into your cybersecurity posture has several key benefits.*

1. **Confidently report the state of security at any time**
   EDR provides tools to help understand your organization's current security position. Using EDR:
   - Helps determine which machines have been affected by malware.
   - Helps identify areas that may be vulnerable to attack.
   - Helps administrators to determine the scale and severity of an attack.
   - Makes it easier to demonstrate that sensitive information is protected.
2. **Discover attacks that have gone undetected**
   EDR's threat detection capabilities let you identify potentially undetected incidents, meaning you can:
   - Detect attacks by searching for Indicators of Compromise (IOCs).
   - Provide a list of the most important suspicious events.
   - Analyze new scripts when it is not immediately obvious whether they are malicious or benign.
3. **Respond faster to potential incidents**
   Once incidents are detected, IT and security teams will want to address them fast. EDR can significantly accelerate this by:
   - Isolating compromised devices on demand.
   - Supporting the research process.
   - Offering guided incident response – EDR provides proposed next steps to help analysts. This includes the ability to isolate endpoints for immediate recovery, clean and block files, and take forensic snapshots.
4. **Understand how an attack took place to prevent new attacks**
   EDR also helps with investigation, so you can understand how the attackers entered your systems:
   - EDR systems provide a visual representation of the **entire attack chain**.
   - You get accurate reporting on how the attack began and where the attacker went.
   - EDR's use of machine learning streamlines the analysis of suspicious events – ranking their threat score so security teams can **efficiently prioritize** their response efforts.

## Advice for deploying an EDR

All EDR tools are designed to be 'generalist' - they could be deployed at many different kinds of organization. The challenge is to tailor a solution to your specific scenario. So how do you do this?

- **Strategy first:** EDR is most successful when it is deployed as part of a clear strategy. You need to define desired outcomes, then select an EDR platform that fits your strategy.
- **Risk appetite:** You can use EDR to create an almost impenetrable (but hard to use) device policy, or something much more flexible (but riskier) So, what is you risk appetite?
- **Continual review:** As an organization grows or enters new markets, its EDR policies will need to adapt and be reviewed regularly.
- **Integration:** EDR technology won't exist alone – it will need to integrate with your organization's other technology ecosystem.

# Supported EDR with Managed Detection & Response (MDR)

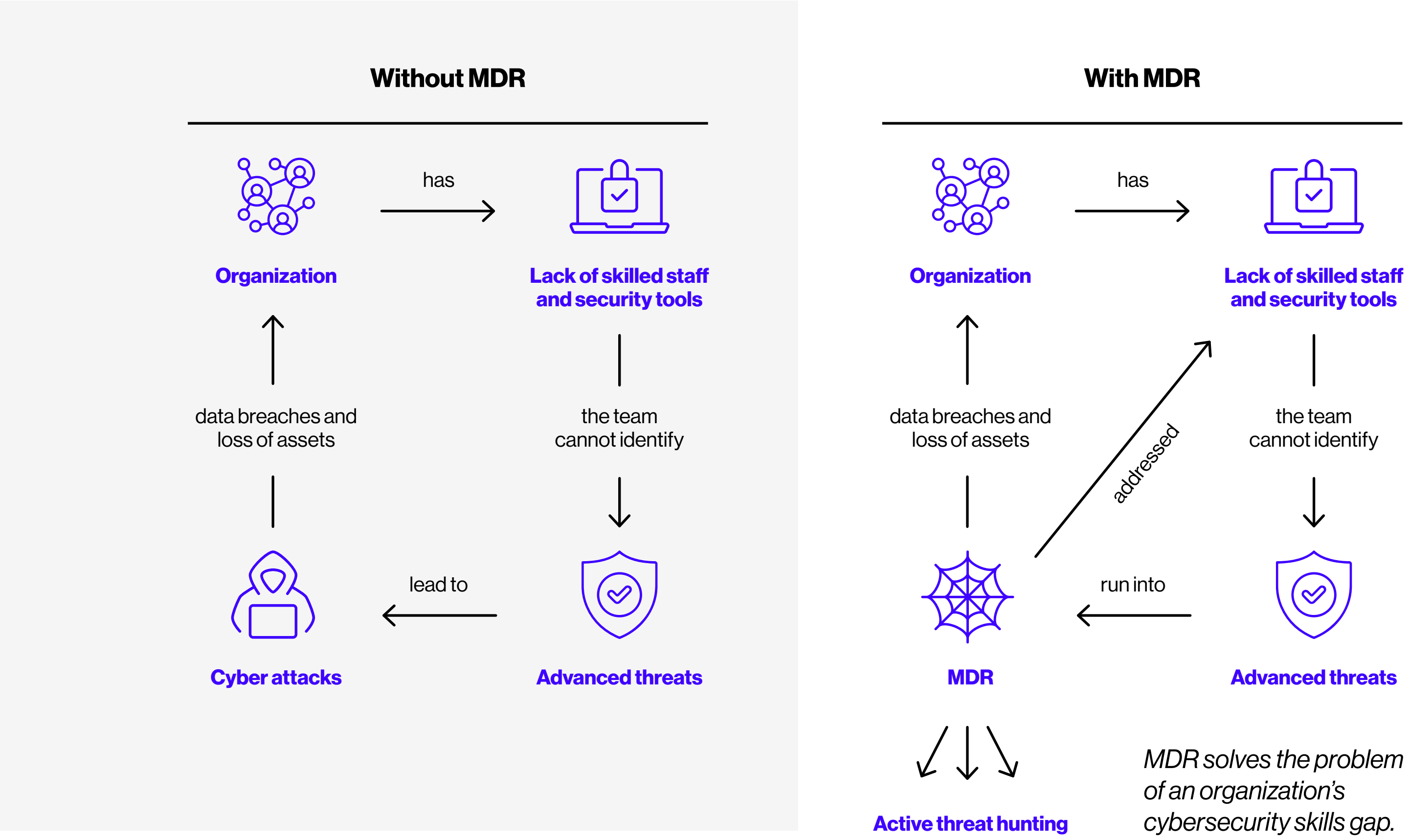
Since the emergence of the Endpoint Detection and Response concept in the 2010's, a wide variety of cybersecurity companies have introduced EDR tools of varying degrees of sophistication.

However, using EDR technology – particularly standalone solutions – can cause issues for time-pressed IT teams. Endpoint Detection and Response often **generates more alerts** for IT security experts to analyze. This requires **time and expertise** to investigate. In response, vendors have developed Managed Detection and Response (MDR).

## What is Managed Detection and Response?

With MDR, the most time-consuming tasks are taken out of IT teams' hands, with an external service provider managing and analyzing alerts for them. Indicators of Compromise (IoC's) are detected, analyzed and investigated. After this, advice will be given to the customer on how to remove a current threat or how to prevent it in the future.

MDR allows time-pressed businesses to get all the security **benefits** of EDR, **without the additional work** involved in managing the alerts an EDR system generates.



*MDR solves the problem of an organization's cybersecurity skills gap.*

Original infographic source: phoenixNAP, 2020

# Get started with EDR

SoftwareOne can help determine the requirements and needs for EDR solutions that fit your environment, budget, and context. We deliver, implement, and maintain the solution(s) throughout the software lifecycle, including through our Managed Detection and Response service for Microsoft Sentinel.

Microsoft Sentinel is the most complete solution for EDR on the market. It facilitates a comprehensive 24x7 threat protection solution delivering continual monitoring, detection, prevention, and response across your entire multi-platform, multi-cloud digital estate. SoftwareOne helps you to maximize Microsoft Sentinel and tailor it to you needs.

## Why partner with SoftwareOne for Managed Detection and Response?

1. **350+ pre-defined security uses cases:** We actively resolve incidents, reducing the workload for security professionals with both manual actions executed by SoftwareOne analysts as well as automated resolution driven by SoftwareOne's security library of pre-defined use cases.

2. **Azure DevOps integration:** Our Azure DevOps integration and solution deployment via C/CD pipelines enhances operational efficiency and strengthens your cybersecurity

3. **24x7 globally managed SOC:** This ensures continuous access to expert security monitoring worldwide, regardless of your location and time zone.

4. **Up-and-running in days:** Leveraging automation, intelligent data analytics tools and a library of pre-defined scenarios, alongside our streamlined onboarding process means we can help you to swiftly transition from setup to action.

5. **Expertise with EDR tools:** Our highly experienced teams help you to deploy advanced EDR solutions such as Microsoft Sentinel. We have years of experience configuring and deploying these kinds of platforms, so you are protected fast, while avoiding implementation pitfalls.

6. **Reduce costs:** Our expert teams add security without contributing to your staffing overheads. That means you lower your total cost of ownership, get started faster, reduce infrastructure and maintenance costs, and collect data at cloud scale.

**Contact us today for a Security envisioning workshop and begin your journey to a more proactive cybersecurity.**

## CONTACT US

Get in touch to find out more about our services.

**www.softwareone.com**

SoftwareOne, Inc.
T. +1 800 444 9890
E. connect.us@softwareone.com