

# What is threat detection and response (TDR)? Complete guide

September 2024

## **In this guide:**

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

Threat detection and response, or TDR, is the process of recognizing potential cyberthreats and reacting to them before harm can be done to an organization. It helps prevent data breaches, ransomware attacks and other security incidents, serving as an extra line of defense behind traditional security features, such as firewalls and antivirus software. With TDR, the goal is to act before a compromise becomes a breach or another type of cyberattack. This comprehensive guide to threat detection and response explores the technologies and practices that enable this layer of protection across a range of IT assets.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

# What is threat detection and response (TDR)? Complete guide

*PHIL SWEENEY, INDUSTRY EDITOR*

Threat detection and response, or TDR, is the process of recognizing potential cyberthreats and reacting to them before harm can be done to an organization. By identifying cybersecurity risks -- that either have been or could be exploited by intruders -- and then driving efforts to respond to the threats, TDR helps prevent data breaches, ransomware attacks and other security incidents.

Threat detection involves a mix of monitoring technologies, [threat intelligence](#) and human expertise. It serves as an extra line of defense behind traditional security features such as firewalls and antivirus software, seeking out vulnerabilities in endpoint devices, IT networks, applications and elsewhere. TDR offerings are sold as products as well [as managed services](#).

A key element in TDR is its ability to react to vulnerabilities through automated responses, which can, depending on the situation, correct, contain or otherwise counter the potential threat. With TDR, the goal is to act before a compromise becomes a breach or another type of cyberattack.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

Once alerted to a potential threat, TDR can initiate responses. For example, it will block a suspicious IP address, disable an account, isolate an infected device or temporarily shut down affected services.

A business trying to [implement an attack surface management program](#) knows how essential it is to monitor IT assets -- all of them, all the time. But being able to achieve that goal is the challenge.

This comprehensive guide to threat detection and response explores the technologies and practices that enable this layer of protection across a range of IT assets.

## WHY IS THREAT DETECTION AND RESPONSE IMPORTANT?

No matter how good an organization's cybersecurity defenses might be, intrusions into IT networks and systems are to be expected.

Inevitably, there will be an open port from a forgotten-about test server, a device running misconfigured security software, a malware-infected personal laptop that an employee uses to connect to a corporate network, or other security holes. It's TDR's job to spot and stop such vulnerabilities before attackers can take full advantage.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

As Dave Gruber, an analyst at TechTarget's Enterprise Strategy Group research and advisory division, put it: "The faster we can detect, the faster we can contain, then the faster we can stop bad guys from executing some really malicious, ugly thing."

The risks are many. Security events range from troublesome to highly destructive. For example, a business that is breached will lose data, suffer reputational damage and take a financial hit. A 2024 IBM/Ponemon Institute report estimated the average cost of a data breach at \$4.8 million, a 10% increase over the prior version of the annual report. The estimate was based on an analysis of breaches at 604 organizations worldwide between March 2023 and February 2024.

An organization trying to protect itself must deal with both the variety of cyberthreats and the endless cat-and-mouse maneuvering between attacker and defender. Forrester Research analyst Allie Mellen said the changing nature of IT threats ranks alongside IT complexity as the top frustrations the consulting firm hears year after year from its clients.

Ransomware, additional types of malware, phishing attacks and other cyberthreats are among the tactics bad actors use against businesses, schools, governments and healthcare providers. The reason these techniques are used so commonly is because they are effective. TDR is a key component of [cybersecurity strategies](#) that aim to block them.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

# The value—and challenge—of TDR



**DAVE GRUBER**

Analyst, TechTarget's Enterprise Strategy Group

“Our IT infrastructure is growing and changing so fast, and we have supply chains and partners that are into our systems, and contractors, it's almost impossible for us to close all the windows and lock all the doors. So, we need something that watches inside of our world, which is this detection and response idea, for (threats) that make it through prevention.”



**ALLIE MELLEN**

Analyst, Forrester Research

“If you're going to go out there and bring in a bunch of threat intel feeds and not do any curation or decision-making about how long you're keeping the threat intel or what you're using it for, you're not going to have a good time. ... You need people to support that. You need the processes in place to go back and make sure that any stale threat intel is being deprecated. All of those aspects have to come together.”



**JEFF POLLARD**

Analyst, Forrester Research

“These tools don't necessarily talk to each other. There's lack of integration, there's not a ton of automation. And if there is automation, you have to build it yourself. ... You can work with vendors that do some of it but not all of it, so it winds up being these massive projects that require five, six, seven, eight, nine different technologies from three, four, five, six, seven vendors with different capabilities. It's daunting.”

©2024 TECHTARGET. ALL RIGHTS RESERVED. TechTarget

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

## HOW DOES THREAT DETECTION AND RESPONSE WORK?

Because preventive measures can't stop every cybersecurity threat, organizations need to discover what they've missed. Threat detection aids in this process by monitoring networks, endpoints, applications, user activity and data to uncover indicators of compromise ([IOCs](#)), which might reveal malicious activity. Threat detection products analyze traffic patterns, system logs, suspicious files, access attempts and other data for anomalous patterns and behaviors.

To meet the demand for additional protection, security vendors have positioned their products into a growing number of segments within the threat detection and response category, including the following:

- **Cloud detection and response.** [CDR](#) focuses on protecting cloud resources. This includes tighter control over who is granted access to particular cloud services.
- **Data detection and response.** [DDR](#) provides capabilities to secure and identify risks to an organization's proprietary data. Proactive threat detection can help keep data from falling into the wrong hands.
- **Endpoint detection and response.** [EDR](#) provides continuous monitoring and response capabilities for desktops, laptops, mobile devices, IoT gear, servers, workstations and other devices. It collects and analyzes data about each endpoint, and some EDR systems will automatically quarantine a compromised device.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

- **Extended detection and response.** [XDR](#) provides greater visibility than EDR by integrating telemetry from networks, cloud environments, endpoints and additional sources. Having data from various security tools in one place rather than in many makes that information much more useful to a security team.
- **Identity threat detection and response.** Stolen passwords and compromised user accounts provide attackers with prime entry points. [ITDR](#) delivers capabilities to improve detection and response of threats to identity management systems.
- **Managed detection and response.** [MDR](#) services from third-party providers offer outsourced monitoring and threat response. These services assist organizations that might not have necessary security expertise on staff or global enterprises that need help keeping up with the volume of threats they face.
- **Managed extended detection and response.** [MXDR](#) is an outsourced version of XDR. This service provides customers with wide visibility into their systems, threat response capabilities and human expertise.
- **Network detection and response.** [NDR](#) uses advanced monitoring and machine learning to create a baseline of normal behavior on an organization's network. It then looks for deviations from that baseline to identify and potentially stop malicious traffic.



## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

## WHAT THREATS DOES TDR IDENTIFY AND PREVENT?

Security teams have always devoted attention to network and [endpoint security](#), but their methods needed to adapt as threats grew in complexity and quantity.

TDR tools offer visibility into stealthy attacks to enable faster responses and reduce business disruption and risk. They detect and mitigate many threats, including the following:

- **Malware.** [Malware](#) is any form of malicious software, including spyware and Trojans, designed to infect systems and networks and steal data.
- **Ransomware.** Threat actors use [ransomware](#) -- now the most prominent form of malware -- to encrypt and exfiltrate business-critical data. They then demand the victim pay to decrypt the data and prevent the attackers from selling or publicly disclosing it.
- **Phishing.** The most popular form of social engineering, [phishing](#) attacks trick users into giving up sensitive information and account credentials, which attackers then use to install malware or infiltrate systems.
- **Distributed denial-of-service (DDoS) attacks.** [DDoS](#) attacks flood systems with traffic to overwhelm computing services and disable servers.
- **Botnets.** A [botnet](#) is a network of malware-infected devices that attackers use to conduct additional actions, such as send spam emails, conduct DDoS attacks, steal data or money, or perform cryptojacking.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

- **Advanced persistent threats.** [APTs](#) are cyberattacks in which malicious actors gain access to an organization's network to steal data over a prolonged period of time.
- **Zero-day threats.** A [zero-day vulnerability](#) is a security flaw in software, hardware or firmware that developers are unaware of and, therefore, have not patched.
- **Living-off-the-land attacks.** Living-off-the-land attacks involve malicious actors abusing legitimate tools present in a network to compromise an organization.

Damage can be done -- and done quickly. A key security metric is breakout time, which measures how long it takes an attacker to achieve lateral movement between systems within a targeted organization after making an initial intrusion. In its three most recent annual threat reports, security company CrowdStrike showed average breakout times dropped from 98 minutes to 84 minutes to 62 minutes.

With capable hackers positioned to exploit systems so quickly, security teams face pressure to respond. That's where the many varieties of TDR come into play.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

# Types of threat detection and response

Threat detection and response offerings are available in an array of options—and the list is expanding.

**Cloud detection and response (CDR).** CDR focuses on protecting cloud resources and controls from cyberthreats.

**Data detection and response (DDR).** DDR provides capabilities to secure and identify data risks.

**Endpoint detection and response (EDR).** EDR provides continuous monitoring and response capabilities for endpoint devices, including desktops, laptops, mobile devices, IoT devices, servers and workstations.

**Extended detection and response (XDR).** XDR provides enhanced capabilities beyond traditional EDR tools, offering greater visibility and context than EDR by integrating telemetry from additional cloud-based and on-premises sources.

**Identity threat detection and response (ITDR).** ITDR improves detection and response capabilities for identity management systems.

**Managed detection and response (MDR).** MDR services from third-party providers offer outsourced monitoring and threat response.

**Network detection and response (NDR).** NDR focuses on detection and response for network activity, such as anomalous or malicious traffic.




ILLUSTRATION: VISUAL GENERATION/GETTY IMAGES

©2021 TECHTARGET. ALL RIGHTS RESERVED. TechTarget

## THREAT DETECTION AND RESPONSE FEATURES AND CAPABILITIES

Threat detection and response can cause confusion to those unfamiliar with it -- and not just because of the way its terminology has infiltrated the alphabet. It handles a variety of tasks in a variety of ways, and it's not always easy to know [where one type of TDR begins and another ends](#).

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

Certain forms of TDR, such as [EDR, XDR and MDR](#), perform similar yet different functions. XDR comes in separate [open and native deployments](#). Vendors make several types of threat detection, such as EDR, NDR and XDR, available to their customers both as products and outsourced services. There might be valuable [use cases for CDR](#) beyond what an individual cloud provider offers.

Endpoint protection provides a good example of the multitude of security options. Organizations long ago realized the value of endpoint security to protect servers, laptops, mobile phones and even printers against malware and similar threats.

EDR and XDR add depth to those device protection efforts by monitoring every device in an organization -- regardless of where the devices are located. This level of protection is far [more advanced than antivirus software](#), which scans endpoints only for known threats. EDR actively seeks out potential threats through a variety of methods, such as tracking IP addresses of devices that connect to an organization's systems or when someone attempts to change a password. It can identify intrusions that might have eluded an [endpoint protection platform](#) (EPP) at the security perimeter. This is helpful, since traditional understandings of that perimeter continue to be stretched by remote work, IoT and the ubiquity of mobile devices.

With more devices from more locations accessing an organization's network, security teams must juggle [multiple types of endpoint security](#). These efforts, when well

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

coordinated, should mitigate risks presented by malware, unpatched software and unencrypted data. A business, for instance, should view [EPP and EDR as complementary technologies](#) that promote the idea of a layered defense against cyberthreats rather than different options to accomplish the same tasks.

Redundancy questions might also arise over whether EDR should be deployed alongside a security information and event management ([SIEM](#)) platform. Both aggregate telemetry, but a closer look shows [SIEM and EDR protect endpoints differently](#). While a capable SIEM system will identify threats, EDR can recommend fixes to vulnerabilities and possibly contain a threat before a breach results in data loss.

SIEM technology plays a key role, though, in organizing a company's security efforts. It pulls log data from security devices, firewalls and applications. SIEM sorts that data and generates helpful alerts in ways that alleviate the common complaint from security admins about the number of unnecessary or low-priority alerts they encounter.

When a security operations center is routinely deluged with false positives, staff can overlook important signals of an attack underway. One of the most high-profile -- and costly -- examples of this is the 2013 Target breach, an incident that compromised an estimated 40 million customer card accounts and was blamed, in part, on staff being afflicted with [alert fatigue](#).

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

## BEST PRACTICES IN TDR AND THREAT MANAGEMENT

The following are some best practices to help ensure TDR efforts and broader threat management initiatives are successful.

### EFFECTIVE INFORMATION MANAGEMENT

Access to large amounts of security information might at first seem to be only a good thing. In practice, the abundance of security telemetry and details about cyberthreats can also be a burden.

In many respects, threat management is information management. Knowing which data points matter from a security standpoint is crucial -- but, given the volume of information security tools absorb, it is impossible to make all the necessary assessments manually. Technology and automation are essential.

Different approaches to managing threat information might involve the use of [SIEM, XDR or security orchestration, automation and response](#) (SOAR) tools. A SIEM tool will likely provide detailed information about a security event, while a SOAR system is useful in taking data and initiating an automated response to an attack. Their capabilities work in tandem. XDR uses SIEM data too, but its response capabilities are much more far-reaching than SOAR's.

## In this guide:

[Why is threat detection and response important?](#)

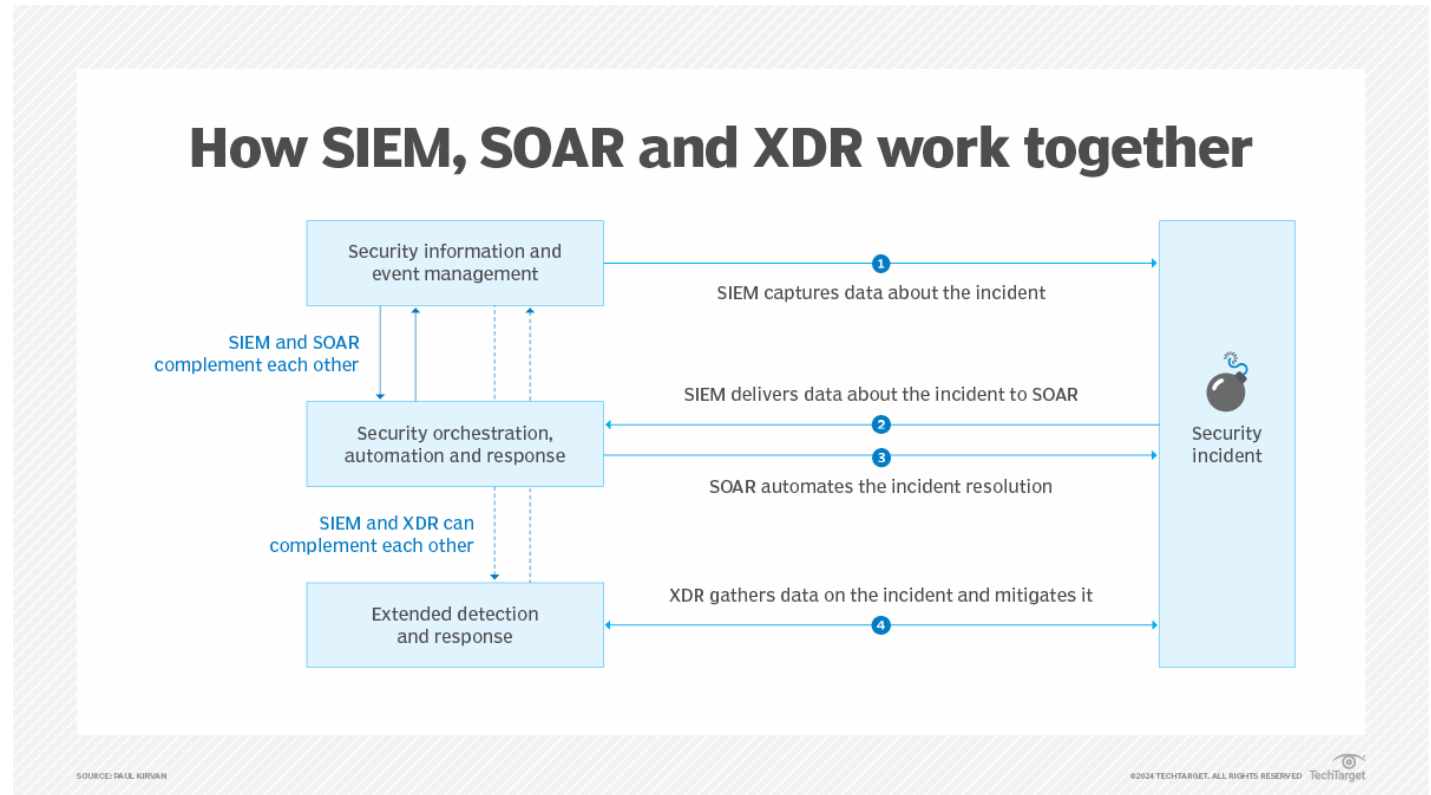
[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)



## THREAT INTELLIGENCE

Any serious effort to interrupt cyberthreats should incorporate threat intelligence. This is important information about attacks and potential attacks, such as which external threats are prevalent at any given moment, the tactics being used by particular threat actors and so on. An example of relevant threat intelligence would be the appearance of a zero-day vulnerability; until organizations are aware of the exploit, they won't be able to prevent attackers from deploying it against them.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

## THREAT HUNTING

While threat intelligence relates to threat hunting, they describe different things. Threat hunting is the act of seeking out threats that might already be inside an organization's systems. Threat hunters will use the specific information available to them via a [threat intelligence feed](#) to inform their work, but the two terms are not interchangeable.

When a security team begins threat hunting, it is actively looking through systems for clues that an attacker has been present. There are several [strategies and steps](#) they can use in this work to bolster their chances of success:

- Structured threat hunting, which looks for evidence of techniques known to have been used by attackers.
- Unstructured threat hunting, which searches for IOCs.
- Situational threat hunting, which concentrates threat hunting on those IT assets believed to be most at risk.

Threat hunters should also review [key threat hunting frameworks](#). Methodologies such as Sqrrl and Peak can help security admins develop some structure around their hunting activity.



## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)



## USE OF EXTERNAL THREAT RESOURCES

Another useful resource in threat hunting and threat detection is the [Mitre ATT&CK framework](#), an open-to-all collection of information on tactics and threats. Operated by a nonprofit research organization, the Mitre knowledge base is widely used to analyze the [behavior and techniques of adversaries](#) during a cyberattack. By sharing this type of information, organizations and security vendors can be better informed about -- and perhaps better prepared for -- the latest cyberthreats.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

In an attempt to improve information sharing, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) [created a portal](#) in 2024 specifically for users to voluntarily report security incidents. CISA leaders said they hoped that making details of a particular security event widely known would prevent attackers from using the same tactics on multiple targets.

## AI, TDR AND THE FUTURE

Threat detection and threat management continue to grow in sophistication. Organizations have options available that range from [unified threat management](#) products to fully outsourced XDR services. But these security technologies won't promise to solve every information problem or eliminate every risk -- because they can't. What they can do is make an organization more ready for the threats that are bound to come.

As with most everything, [AI will play a larger role](#) in information security as a whole and TDR in particular. The exact shape of that is far from clear, but experts anticipate AI will be used as both a shield and a weapon. As more organizations experiment with and implement AI systems, they should [engage in threat modeling](#). This work could help them to spot potential security threats as well as to be prepared for when something in an AI deployment goes wrong.

## In this guide:

[Why is threat detection and response important?](#)

[How does threat detection and response work?](#)

[What threats does TDR identify and prevent?](#)

[Threat detection and response features and capabilities](#)

[Best practices in TDR and threat management](#)

[AI, TDR and the future](#)

TDR vendors have for years touted the power of AI and machine learning, pointing to these technologies as the reasons their products can detect threats more effectively and efficiently than humans. Skilled admins might know their networks from east to west and north to south, but they simply cannot learn traffic patterns and recognize anomalies as quickly as an NDR product running advanced machine learning algorithms.

Another ongoing development in threat detection and response is wider use of outsourced services. Gartner predicts that by 2025 as many as 50% of businesses will use a third party for at least parts of their TDR work. When [selecting a managed security service](#), organizations should carefully consider a provider's strengths, ask about global coverage and determine which reporting metrics will be furnished.

*Phil Sweeney is an industry editor and writer focused on information security topics. Sean Michael Kerner, an IT consultant and technology writer, contributed to this article.*



## CONTINUE READING

- [What is threat hunting? Key strategies explained](#)
- [EDR vs. MDR vs. XDR: Key differences](#)
- [How AI could change threat detection](#)