Digital Security
Progress. Protected.

XDR'S ROLE IN MAINTAINING A PROACTIVE DEFENSE

XDR's Role in Maintaining a Proactive Defense

INTRODUCTION

Extended detection and response (XDR) and its predecessor, endpoint detection and response (EDR) can be thought of as reactive security tools. After all, they are designed primarily to detect anomalous activity — signs that an intrusion into the environment has succeeded — and they also include tools for investigation, incident response and remediation.

In this guide, we'll explain how, in the right hands, XDR has a role in prevention as well.

WHAT'S THE DIFFERENCE BETWEEN EDR AND XDR?

EDR ingests data gathered from endpoints and analyzes system, process and user activity to detect security threats. It provides remedial guidance for threats that bypass prevention controls and enables endpoint threat investigations. EDR capabilities are often included in endpoint protection platforms and delivered as software agents connected to centralized cloud-based security analytics and management software.[1]

XDR is a loosely defined term, and there are as many different understandings of what XDR is as there are companies that offer these solutions. Here's one thing everyone seems to agree on: XDR is "extended" because it goes beyond the endpoints by ingesting threat intelligence and telemetry from other sources. Here's what Gartner says: "XDR delivers security incident detection and automated response capabilities for security infrastructure. XDR integrates threat intelligence and telemetry data from multiple sources with security analytics to provide contextualization and correlation of security alerts."[2]

1 Gartner, *Hype Cycle for Endpoint Security*, **Franz Hinner, Satarupa Patnaik, Eric Grenier, Nikul Patel, August 1, 2023**
2 Gartner, *Market Guide for Extended Detection and Response*, Thomas Lintemut, August 17, 2023

UNCOVERING UNRECOGNIZED VULNERABILITIES

An ounce of prevention is worth a pound of cure, and this saying has never been more applicable to cybersecurity. Although there has been considerable focus recently on enhancing detections, prevention should remain the first line of defense.

As Forrester explains, "When an attack is prevented by the endpoint protection platform, analysts can spend time investigating how the threat penetrated their other lines of defense instead of cleaning up a mess at the endpoint."[3]

PREVENTION AS WELL AS REMEDIATION

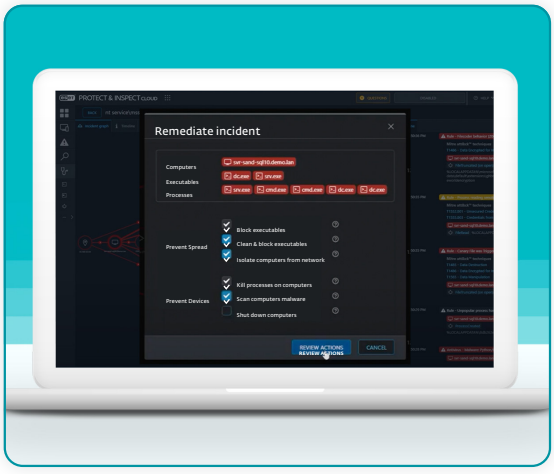
Here's where XDR serves as part of the first line of defense

Beyond remediation, XDR can support a prevention-first approach. As good as modern endpoint protection can be, it doesn't stop 100% of threats. According to one source, compromised usernames and passwords and phishing attacks are the most commonly used initial attack vectors,[4] and these involve the human element. Insider threats and supply chain attacks carried out via trusted third-party software vendors are other examples of attacks that can evade traditional endpoint security. Also consider that if threat actors do succeed in accessing one or more networked assets, they often embed the evasive, malicious payload but wait for months before launching the real attack.

Organizations using XDR for the first time may be surprised by all the events that trigger detections, revealing a host of poorly configured systems, unpatched vulnerabilities and latent threats. The initial deployment of XDR can deliver immediate benefit by uncovering poor cyber-hygiene practices and revealing threats lurking in the network.

STOPPING ATTACKERS IN THEIR TRACKS

XDR provides visibility into low-level events and also provides the context to determine if seemingly innocuous activity is actually malicious. Detection rules, indicators of compromise and search capability allow an in-depth review of executables across the network that identifies anything suspicious. An event or series of events determined by behavioral analysis to be a potential sign of attack triggers an alert allowing immediate investigation.



An XDR solution that maps to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework provides comprehensive information about even the most complex threats, serving as a set of signposts that an attack is underway and also what the next action should be. The XDR itself may also recommend investigation steps or remediation actions or may trigger an automated response. Security analysts can access the full suite of investigation and remediation options available through PowerShell via the XDR but also can draw XDR-furnished one-click response options, such as rebooting and shutting down an endpoint, isolating endpoints from the rest of the network, forcing a logout, running an on-demand scan, killing any running processes, and blocking applications from executing or DLL code libraries from loading.

3 The Forrester Wave™: Endpoint Security, Q4, 2023, Forrester Research, Inc., October 19, 2023
4 Ponemon Institute, Cost of a Data Breach Report 2023.

DETECTING UNKNOWN APPLICATIONS AND RISKY BEHAVIORS

XDR monitors actions carried out by an executable and quickly assesses if executed processes are safe or suspicious. It is able to block malicious modules from being executed on any computer in the network and detects violations of policies that apply to use of specific software, such as torrent applications, cloud storage, Tor browsing or other unwanted software. It then notifies users and uninstalls the violating software. XDR is also able to detect and block portable applications that do not actually install and block their unauthorized scripts from running.

Monitoring anomalous user-related incidents is possible due to specific rules written to be triggered by behavior, and in addition, grouping of computers by user or department allows security teams to identify if the user is entitled to perform a specific action or not. If specific users are repeatedly involved with malware incidents, XDR allows security analysts to quickly complete a root-cause analysis to determine the source of the infections so that any risky behaviors may be corrected.

The tools used by IT admins have functionalities that, in the wrong hands, can be abused to download malware, reconfigure systems, disable security settings, perform reconnaissance and even destroy data. Since these tools are legitimate, endpoint security software is limited in its ability to differentiate between fair use and abuse. However, XDR makes it possible to monitor how IT admin tools are being used and alert defenders to actions that are not typical for admins or are potentially dangerous.

ENABLING PROACTIVE THREAT HUNTING

Threat hunting can significantly reduce adversary dwell time in the network. XDR gives defenders visibility into the earliest stages of an attack, before any deployment of destructive malware, such as ransomware or a data wiper.

A query-based search of indicators of compromise and filters applied to raw data allow for sorting based on file popularity, reputation, digital signature, behavior or other contextual information. Setting up multiple filters allows automated threat hunting and incident response, including the ability to detect and stop advanced persistent threats and targeted attacks.

The security news cycle often reveals ongoing attacks, sometimes happening on a mass scale, resulting in defenders running to their consoles to monitor for the newly reported attacks and fine-tune defenses. XDR provides the ability to write threat-hunting rules that can search the database of events, looking for potential signs of compromise so any infiltration can be quickly shut down.

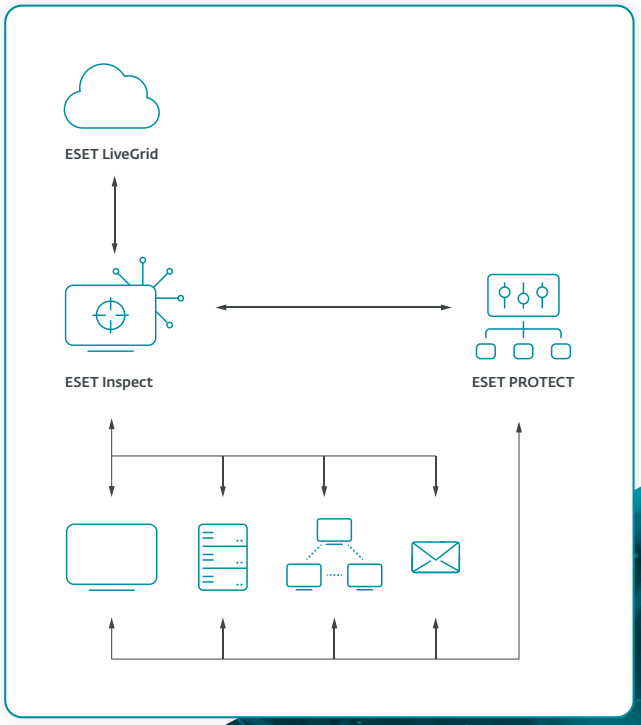
ESET INSPECT: A PROACTIVE, XDR-ENABLING SOLUTION

ESET Inspect allows risk managers and incident responders to perform fast and in-depth root-cause analysis and immediately respond to incidents. Paired with the time-tested preventive power of ESET's endpoint protection products, ESET Inspect is a cloud-delivered solution that can:

- Detect advanced persistent threats
- Stop fileless attacks
- Block zero-day threats
- Protect against ransomware
- Prevent company policy violations

ESET's approach to XDR is tightly connected to its multi-award-winning prevention products that apply behavioral analytics across the endpoint, network, cloud, email and other layers. With this tightly integrated, underlying multilayered security, every single layer sends data to ESET Inspect, which analyzes vast amounts of data in real time to detect threats.

ESET Inspect enables quick analysis and remediation of any security issue in the network, spotting suspicious activity and stopping attackers before they can make an impact.



About ESET

AI-NATIVE PREVENTION FOR TOMORROW'S THREATS

Stay one step ahead of known and emerging cyber threats with our **AI-native, prevention-first approach**. ESET combines the power of AI and human expertise to make protection easy and effective.

Developed over 30 years, ESET's best-in-class protection is powered by our **in-house global cyber threat intelligence**, including our **extensive R&D network** led by industry-acclaimed researchers.

ESET PROTECT, our scalable, cloud-first XDR cybersecurity platform combines next-gen prevention, detection and proactive threat-hunting capabilities with a wide range of security services, including **managed detection and response** (MDR). Our highly customizable, integration-ready solutions support all deployment methods, include local support and have minimal impact on performance. They identify and neutralize known and emerging threats before they can be executed, support business continuity, and reduce the cost of implementation and management.

Our mission isn't just to stop attacks in their tracks; it's to prevent them from ever happening. ESET protects your business so you can unlock the full potential of technology.

Digital Security
Progress. Protected.