Show me the value:

MDR reporting for manufacturing execs

Cybersecurity
Progress. Protected.

From IT to the C-Suite: Cybersecurity Becomes a Business Priority

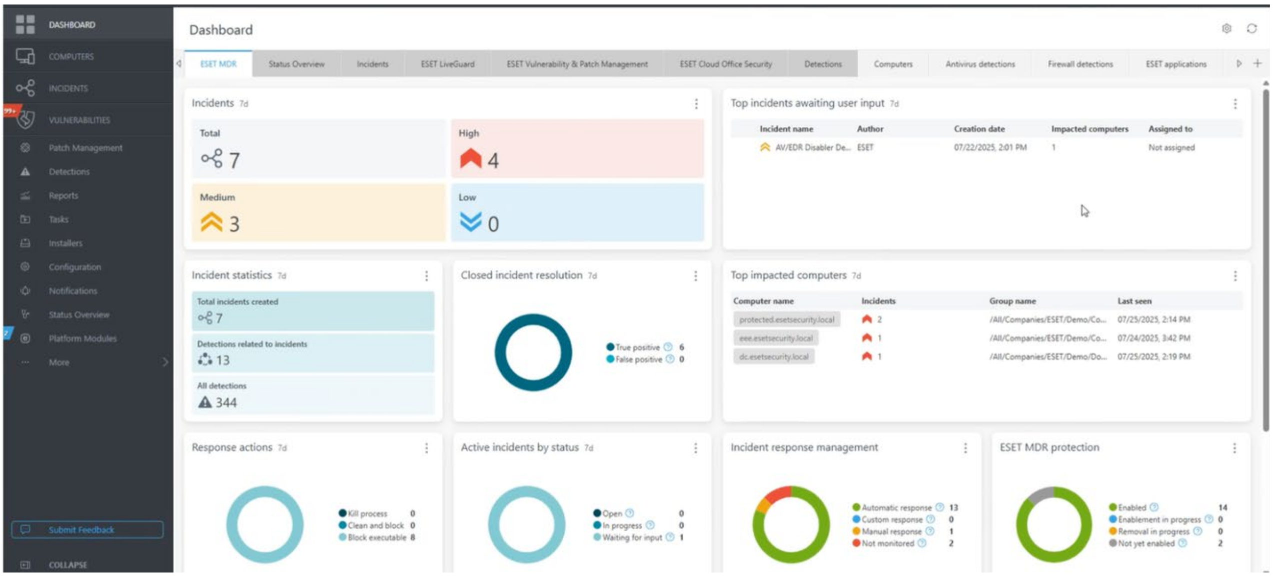
The risk of cyberincidents is a concern that has moved out of the IT or security departments and is top-of-mind with corporate leadership. A survey by IDC found that more than half of boards are concerned with the costs of productivity loss from incidents, cyberinsurance, and the potential for regulatory fines.

As the most-targeted business sector according to the 2025 Verizon Data Breach Investigations Report, manufacturers have an even more urgent need to demonstrate to their leadership that cybersecurity is being effectively maintained.

ESET Managed Detection and Response is a 24x7 cybersecurity service that continuously monitors the network environment for threats, blocks and contains them before they can execute malicious behavior, and removes and remediates them.

The security consoles are manned by experienced security analysts who keep abreast of the tactics and techniques used by threat actors. The service is fully transparent—if you're using ESET MDR, your internal IT and security teams have access to the same console that our security analysts use.

The top-level dashboard view (below) provides a high level overview of the current state of security. The drill-down capability allows you to view at a higher level of detail, but with this top-level view, non-IT executives can quickly gain a picture of the service level, responses and actions taken, and be reassured that the security of the organization is in effective hands.



Top incidents awaiting user input 7d

Incident name	Author	Creation date	Impacted computers	Assigned to
AV/EDR Disabler De...	ESET	07/22/2025, 2:01 PM	1	Not assigned

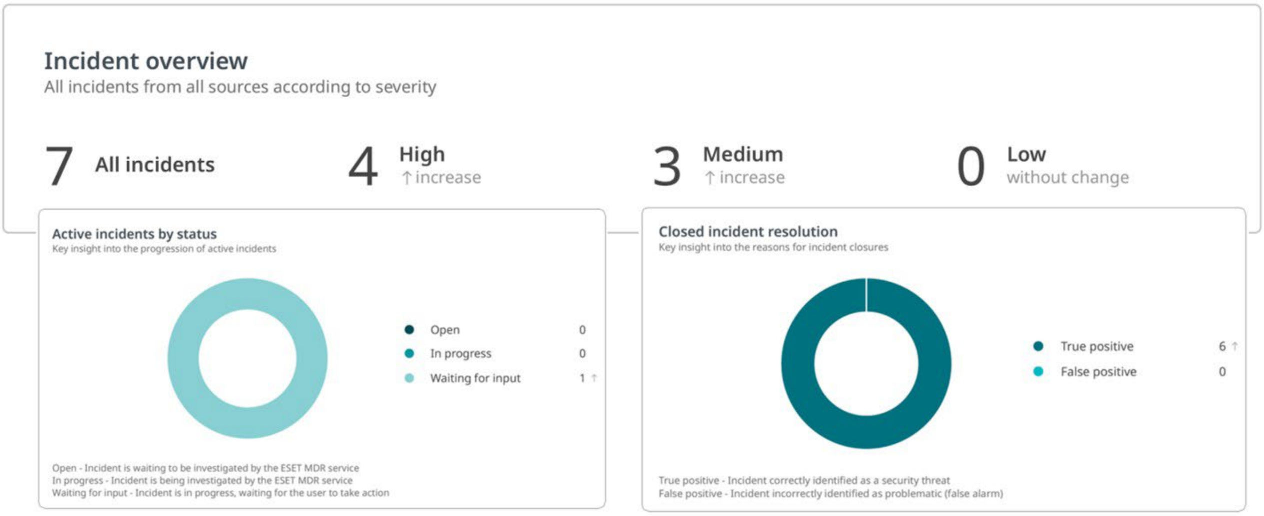
Top impacted computers 7d

Computer name	Incidents	Group name	Last seen
protected.esetsecurity.local	2	/All/Companies/ESET/Demo/Co...	07/25/2025, 2:14 PM
eee.esetsecurity.local	1	/All/Companies/ESET/Demo/Co...	07/24/2025, 3:42 PM
dc.esetsecurity.local	1	/All/Companies/ESET/Demo/Do...	07/25/2025, 2:19 PM

Moreover, if there is an active incident, understanding the severity of the situation, the risk presented by the incident and the computers affected allows IT and the business to make some “in the moment” decisions.

Note that at this level of detail, the focus is on cyberincidents—not the noise of thousands of alerts that is typical of some security tools. With the MDR service, artificial intelligence filters the noise, triages the most critical alerts, identifies patterns of alerts that indicate an attack is in progress, and packages the attack as an incident for priority investigation by human analysts.

If an executive has any questions about an incident and how it was handled, you can use the drill-down capability to satisfy their curiosity.



Incident overview
All incidents from all sources according to severity

7 All incidents

4 High
↑ increase

3 Medium
↑ increase

0 Low
without change

Active incidents by status
Key insight into the progression of active incidents

●	Open	0
●	In progress	0
●	Waiting for input	1 ↑

Open - Incident is waiting to be investigated by the ESET MDR service
In progress - Incident is being investigated by the ESET MDR service
Waiting for input - Incident is in progress, waiting for the user to take action

Closed incident resolution
Key insight into the reasons for incident closures

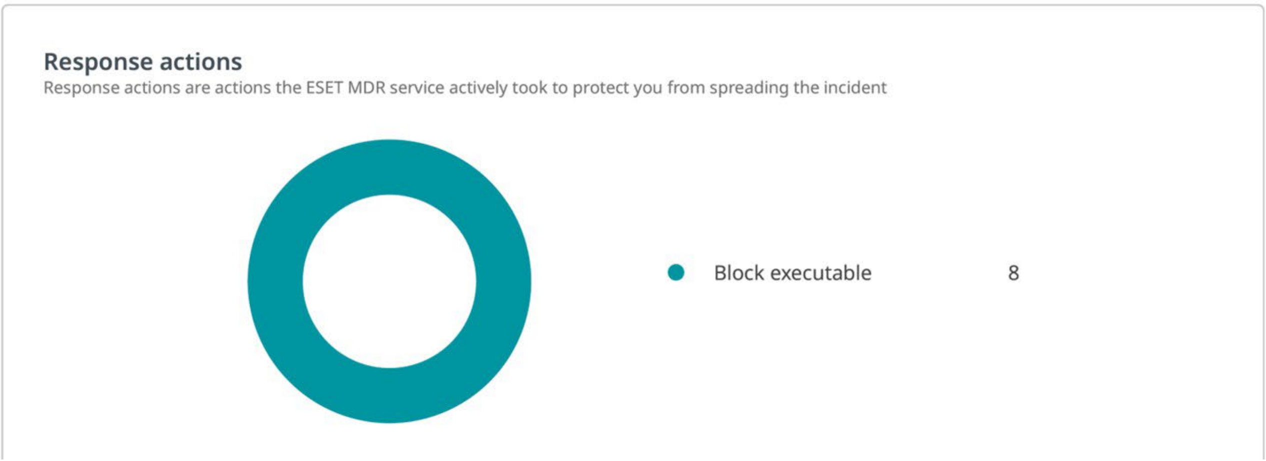
●	True positive	6 ↑
●	False positive	0

True positive - Incident correctly identified as a security threat
False positive - Incident incorrectly identified as problematic (false alarm)

As part of the MDR service, ESET furnishes weekly and monthly reports, delivered in .pdf form, that summarize the state of security, threats detected and actions taken.

At the time the report above was generated, there was one incident awaiting input (in this case, opened by a human ESET analyst) where suspicious, unusual, but not immediately threatening behavior might have been legitimate activity and therefore confirmation from local IT was needed.

ESET MDR is an active, hands-on, interventional service. Because it works in conjunction with ESET Endpoint Protection, ESET security analysts are able to exercise control over ESET endpoints when warranted and prevent attacks by killing processes or blocking them. While simple, this view of the data underscores that your MDR service is not just monitoring, but stopping attackers in their tracks by interrupting the attack chain.



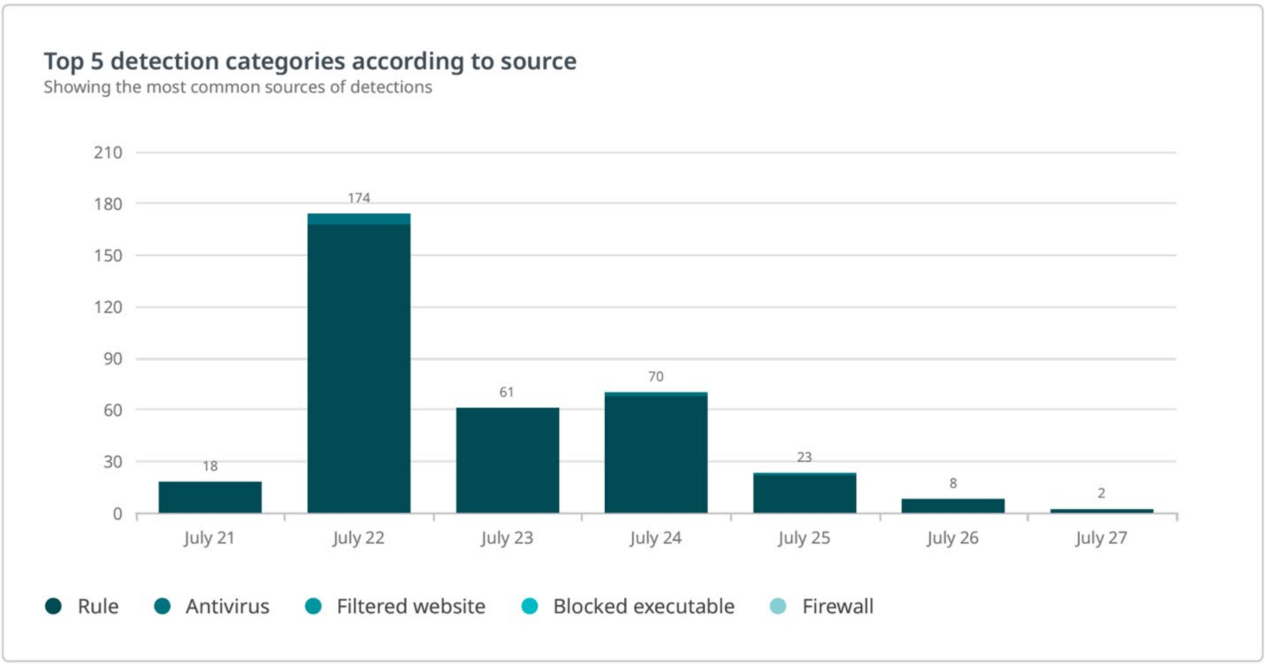
Response actions

Response actions are actions the ESET MDR service actively took to protect you from spreading the incident

The ESET MDR service is able to detect, block, prevent further execution and remediate/ recover from an attempted attack in an average time of six minutes.

This is accomplished through the 17 layers of security built into ESET Endpoint Protection, the ESET Inspect EDR console, and the MDR service. All work in concert and all are included in the ESET PROTECT MDR product tier.

Because the MDR service works alongside ESET Endpoint Protection, the MDR service leverages threat detection and data collected from ESET security tools running on endpoint devices. As shown below, most of the detections of suspicious behaviors were triggered by rules in the MDR console.

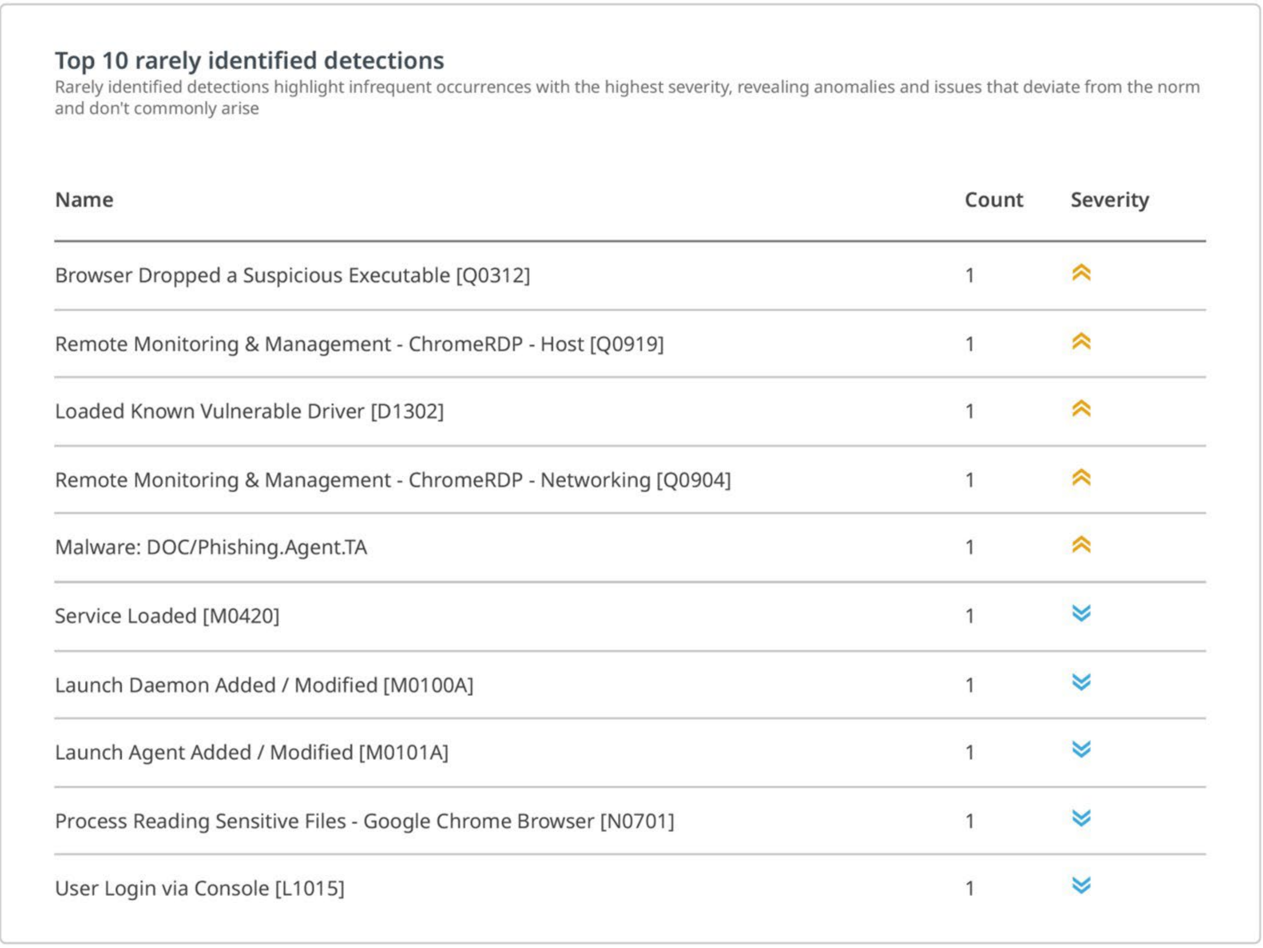


Top 5 detection categories according to source

Showing the most common sources of detections

This is evidence that ESET Endpoint Protection is doing its job—protecting the endpoints with its 99.6% detection rate and zero false positives.

Execs who are especially tech- and security-savvy might be interested in the view below. By way of introduction, a lot of the activity that gets flagged for detection is suspicious but not malicious. It's activity by employees that also happens to mimic some of the techniques used by threat actors, who often use legitimate tools for illegitimate purposes (and there's a separate view for that, too).



Top 10 rarely identified detections

Rarely identified detections highlight infrequent occurrences with the highest severity, revealing anomalies and issues that deviate from the norm and don't commonly arise

Name	Count	Severity
Browser Dropped a Suspicious Executable [Q0312]	1	⇈
Remote Monitoring & Management - ChromeRDP - Host [Q0919]	1	⇈
Loaded Known Vulnerable Driver [D1302]	1	⇈
Remote Monitoring & Management - ChromeRDP - Networking [Q0904]	1	⇈
Malware: DOC/Phishing.Agent.TA	1	⇈
Service Loaded [M0420]	1	⇊
Launch Daemon Added / Modified [M0100A]	1	⇊
Launch Agent Added / Modified [M0101A]	1	⇊
Process Reading Sensitive Files - Google Chrome Browser [N0701]	1	⇊
User Login via Console [L1015]	1	⇊

This is the opposite—it's the stuff that really sticks out, especially the ones marked as high severity. These are "one-off" actions that really grab the attention of our artificial intelligence-driven tools and instantly engage our security analysts. With the ESET MDR service, artificial intelligence filters the noise and automates detections, while human analysts validate the alerts, contextualize them, and respond as necessary.

Cybersecurity in general and MDR specifically are business investments in protecting bottom-line health. In the manufacturing sector especially, the stakes are especially high because it's a tempting target for threat actors because of the imperative to keep the production lines running. For business leaders that aren't IT or security specialists, reporting that speaks to their level of understanding is key for them to be able to justify their investments. That, in turn, secures their support and your continued access to the resources you need to do your job and protect the business.

Two Tiers of MDR Service

Choose the one that's right for your organization.

MDR

The base tier of MDR is designed to be affordable for smaller manufacturers with as few as 25 seats. ESET experts immediately contain the threat, take action by blocking files and processes, and then notify you of the actions taken and any additional steps you need to take.

- Notification of incidents and actions taken
- Optimization of the ESET Inspect MDR console at the backend level
- Continuous threat hunting
- Feedback to incidents
- Weekly & monthly reports

MDR Ultimate

Larger manufacturers at the enterprise level tend to have dedicated IT security admins who want to work with our analysts through an incident. ESET MDR Ultimate works as a seamless extension of your IT function. We contain the threat and then interact with your internal security personnel on complete remediation.

- Joint response to incidents with remediation guidance
- Optimized ESET Inspect console for your environment
- Continuous and on-demand threat hunting
- 24/7 availability to analysts
- Periodical reports with human interpretation

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

Cybersecurity
Progress. Protected.