Three common misconceptions about EDR software

The capabilities of EDR tools are often misunderstood. Get a clear picture of how to protect your organization from known *and unknown* threats.

Endpoint detection and response (EDR) tools are designed to detect known bad activity. But without the support of a Converged Endpoint Management (XEM) solution, like Tanium, they can't find where attackers are hiding, investigate what they did, or remove them from your environment.

An endpoint threat explosion

The endpoint is where global organizations now do business. It's also where they're most likely to be targeted by malicious third parties out to steal sensitive data, extort money from encrypted systems, and much more.

Over two-thirds (68 percent) of organizations experienced an endpoint attack that resulted in compromised data or IT systems over the previous 12 months, according to one 2020 report.

The shift to mass remote working over the last two years created an explosion in corporate endpoints that only increased the enterprise cyberattack surface. Some 90 percent of CXOs we spoke to said they experienced a surge in breaches.

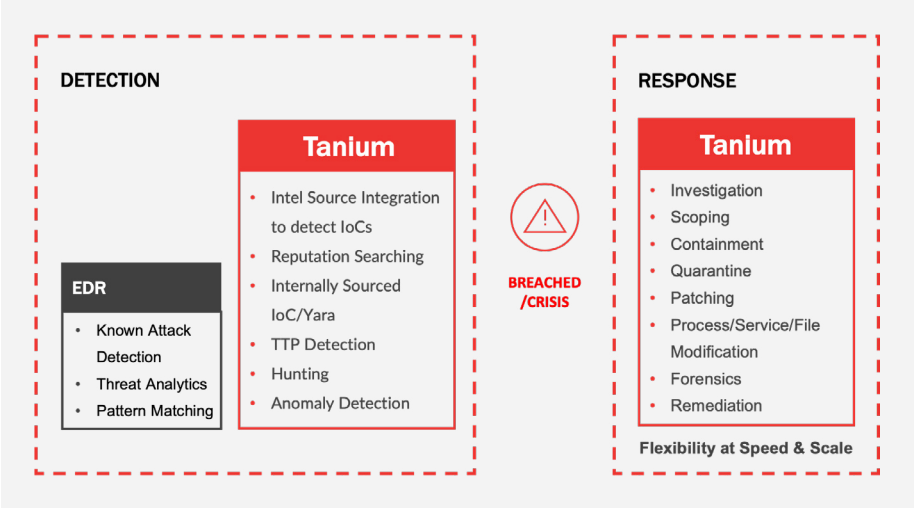
All of which makes EDR a no-brainer for many cybersecurity leaders today. Yet, it's also important to understand where the limits of the technology lie, and where additional tooling may be required.

90%
of CXOs report a surge in breaches

68%
of organizations report an endpoint attack in the past 12 months

Learn more

Watch this interview with Nir Yosha, Technical Solutions Engineer at Tanium, to learn more about how Tanium can fill critical gaps left by EDR tools. Or visit tanium.com to learn more about our threat hunting solutions.



Three misconceptions of EDR

Misconception #1: EDR software is a great tool for proactive threat hunting

EDR software products are built to detect suspicious system behavior, provide contextual information and block malicious activity. But they do so only for known malware (via signatures) and bad behavior (via heuristics).

EDR software alone is not equipped to detect:

- Memory-based attacks
- Fileless attacks
- Living off-the-land (LotL) attacks
- Other techniques used by threat actors to stay hidden

It's these that you need to focus on in threat hunting.

Misconception #2: EDR tools reduce the workload for Security Operations Center (SOC) analysts

It's true that EDR tools can automate the protection and blocking of some malicious activities, which can free up some analyst time. However, rather than reduce the SOC workload, they add to it.

EDR tools increase SOC workload in multiple ways:

- Each EDR tool generates thousands of alerts each day
- EDR alerts lack context, so analysts depend on additional tools
- While analysts are busy with multiple EDR tools, some threats will sneak through, leading to analysts chasing false positives and dead ends

Misconception #3: EDR provides capabilities for full response and remediation

EDR can help with some incident response activities, but it is certainly not a go-to tool.

EDR tools don't provide:

- Behavioral analysis to help scope an attack in progress
- Historical data for investigation and analysis
- Records of activities across all hosts

That means incident responders must find alternative tools to deliver real-time scoping, isolation and forensics.

How can Tanium help?

Security teams should instead look to complement their EDR capabilities with the Tanium platform. Tanium allows customers to:

- Ask the right questions to rapidly discover advanced malicious activity not detected by EDR
- Gain visibility into how far attacks have spread, and if data has been exfiltrated
- Help isolate any threats in real-time and at scale
- Understand what happened post-incident, what the damage is and how the organization can improve before the next attack
- Tanium and EDR work hand-in-hand to minimize cyber risk and make your organization safer, more secure and resilient

Get started on the path to a more secure IT environment. Begin your free trial of Tanium today.

Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud, and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete, and up-to-date endpoint data — giving IT operations, security, and risk teams confidence to quickly manage, secure, and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.