WatchGuard

Three Things You Need to Know About MITRE ATT&CK Evaluation ER7

> Get real about what matters when measuring endpoint security protection, noise, and efficiency.

Introduction

The seventh round of MITRE ATT&CK Evaluations is out, and because MITRE only releases raw data, you're about to see plenty of different takes. Don't get me wrong – WatchGuard has ours too, and we'll walk you through it in this eBook.

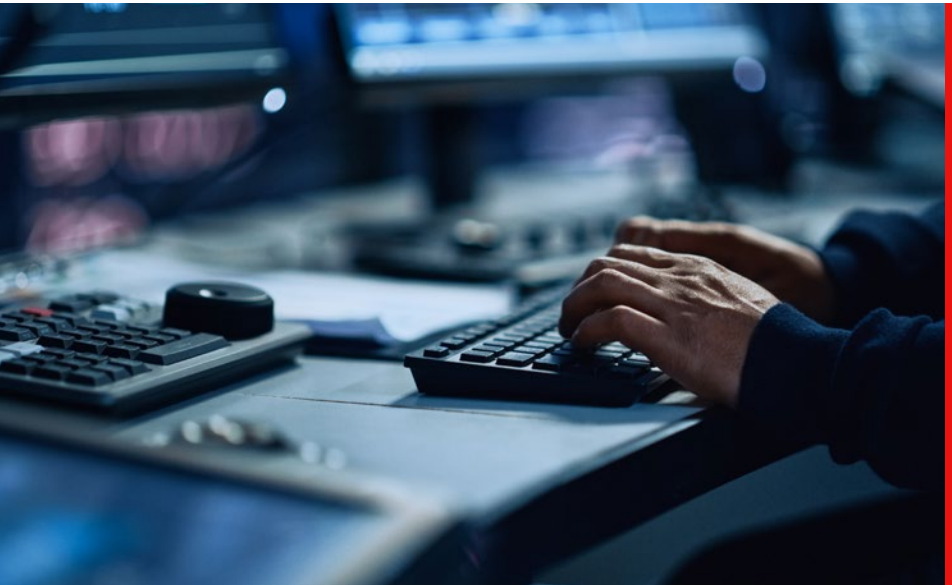
First, we'll give you an insider's view so you can decide for yourself what really matters in MITRE ER7.

01 What the MITRE ATT&CK Evaluation ER7 Actually Measures

MITRE ATT&CK Evaluations don't hand out rankings or trophies – they're technical exercises. MITRE runs a realistic, multi-step attack in a controlled environment and simply records how each product reacts. When the evaluation concludes, MITRE publishes the same raw data for every vendor – detections by attack step, config-change deltas, noise (false positives), alerts, and more.

> In this year's ER7 Evaluation, MITRE:

- Simulated a full Mustang Panda "Hermes" campaign on Windows.
- Tracked which attack steps were detected and how much analytic detail each detection included.
- Measured how much of the attack was actually prevented and at what point in the kill chain.
- Distinguished between out-of-the-box behavior and results that require configuration changes or human review.
- Mixed in legitimate activity to see which products flagged or blocked benign activity.



> MITRE shares raw data; after that, it's on you to make sense of it.

> Look at results through these three lenses:

Attack Visibility:

How much of the attack the product actually sees.

Threat Prevention:

How well – and how early – it stops the attacker.

Operational Burden:

How much noise, alerting, or extra work it creates for your team.

Action Category	Key MITRE Insights	How It's Measured	Real World Interpretation
Attack Visibility	Attack Detection	Percentage of "steps" or "techniques" detected. A step corresponds to a major adversary action and may contain one or more ATT&CK techniques or sub-techniques.	A "step" represents what the adversary is doing in the kill chain (e.g. adversary-in-the-middle technique). Steps detected can prohibit damaging impacts.
	Substep Detection Coverage	Percentages of "substeps"or "subtechniques" detected. Substeps reflect the detailed behaviors that make up a step.	"Substeps" are how the attacker completes a "step." (e.g. substeps to 'AiTM' include obfuscated files, reflective code loading). EDR solutions are capable of blocking attacks without detecting every substep.
Threat Prevention	Prevention Coverage	Percentage of steps in an attack that the product blocked.	Does the product stop the attack, rather than merely detect it.
Operational Burden	Alert Volume and False Positive	Number of alerts generated. Number of false positives flagged or blocked. Number of legitimate actions blocked.	Excessive and nuisance alerting creates operational friction. Every alert requires attention, and high volumes strain staff, leading to slower responses to critical cases.

> Interpreting correctly puts the power of MITRE results back in your hands.

02 How Endpoint Security Vendors Manipulate MITRE Results

Strictly speaking, you can't "game" the MITRE results. The data is the data. But it is on you to make sure vendors aren't using test-only settings that would be a nightmare in a real environment.

> Some products can hit 100% detection simply by cranking up sensitivity and logging. Great for the chart, terrible for security teams who'd drown in noise and low-value alerts.

And vendors without a Zero Trust Application Service* often rely on aggressive "suspiciousness" tuning: lower the threshold, boost prevention, and accidentally label normal activity as malicious. That may look impressive on paper but hides real-world costs, false positives, and workflow headaches.

**WatchGuard's Zero Trust Application Service combines AI and expert SOC analysis to verify every unknown file and let only trusted, safe applications run.*

> Ensure results reflect real-world settings, not test-tuned configurations. What looks good on paper can be a nightmare in your environment.

> What to consider when reviewing each participant's results:

- Does the product see the full attack path, or are there stages with no visibility?
- Does it improve with a configuration change without causing more noise or extra detections on legitimate activity?
- How often does it detect or block benign actions that should be left alone?
- How many alerts does it generate for a full scenario, and are those alerts meaningful and correlated?
- Does prevention stop attacks early without disrupting normal business operations?

> Look for strong protection with zero operational friction. Here's how ideal MITRE results would look:

100% of attack steps detected:
Every solution should catch the major malicious actions in an attack.

90%+ of substeps detected:
You don't need every substep, but you do want broad coverage without piling on noisy alerts.

100% threat prevention:
If the product can see the attack, it should stop it – otherwise, why deploy it?

Zero legitimate activity blocked:
Real world configurations may allow a very small number of false positive alerts in the interest of detecting more threats, but it should never block legitimate activity and impact productivity.

Zero nuisance alerts:
Alerts that point to normal activity waste time, so pay close attention to the volume and quality of alerts in MITRE's data.

The payoff?

Solutions that deliver these kinds of results give you a quieter, more efficient security operation – much less noise, far fewer manual tasks, faster responses, and more systems protected with less effort and lower cost.

03 Where To Find a No Compromise Solution With Top Performance AND Operational Efficiency

Most EDR and XDR tools still force a tradeoff between detection, prevention, and day-to-day usability, often resulting in noise, disruptions, or analyst burnout. ER7 shows that WatchGuard breaks that cycle with clean detection, strong prevention, and low alert volume, keeping teams fast and focused.

We are proud to share WatchGuard's MITRE ATT&CK ER7 results.

100% Attack Visibility	100% Threat Protection	ZERO Operational Friction
MITRE ER7 Results		
100% step detection[1]	100% malicious actions blocked in the early stage[3]	Zero legitimate activity blocked
96.5% substep detection (27/28 covered)[2]		Only 3 high-fidelity alerts needed
The attack is fully visible as it unfolds. No blind spots. No surprises.	**Attacks don't just get detected; they get stopped at they early stage before they can progress.**	**No gaming the system, no clutter, no wasted time, just real-world security that works for you, not against you.**

1 Result from MITRE Detection Evaluations, in both the initial and configuration change runs in the Windows scenario
2 Result from MITRE Detection Evaluations with configuration changes in the Windows scenario
3 Result from the MITRE Protection Evaluations

> ***MITRE ER7 simply confirms what we already knew:*** *WatchGuard turns EDR from reactive to proactive. Anything unknown is untrusted. No guesswork. Just better protection.*

~ Neil Holme, Founder and CEO, Impact Business Technology

> Persistant Progress, Mighty Benefits

Hitting top results with a realistic, manageable configuration takes work. Our teams have learned from every past test cycle, improving not just detection and prevention, but how efficiently we protect customers with less noise and less effort. That's why we keep participating – because it makes our products better, and it's something vendors miss when they sit it out.

These results highlight clear advantages for companies using WatchGuard Endpoint Security, including:

- **Full protection without extra workload**
- **Less noise, fewer manual tasks, and faster responses**
- **Security teams that stay focused, in control, and able to protect more with less effort and lower cost**

BONUS Quick Reference Table:

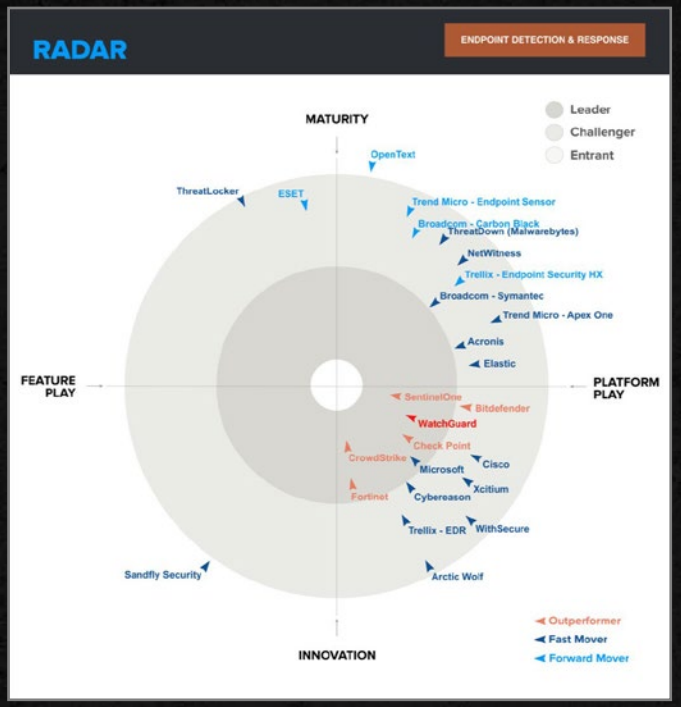
Translating MITRE ATT&CK E7 Insights into Real World Benefits

Category	Description	Operational Impacts	WatchGuard Outcome
Detection Coverage	Attack steps and substeps across the kill chain (initial access → exfiltration).	• Fewer blind spots • Clearer incident narratives • Better tuning and playbook design	100% malicious attack-step detection with deep substep visibility (86% init. run, 96.5% in configuration change).
Noise From Alert Volume and Detections on Legitimate Activity	Number and quality of alerts generated during the scenario runs. Legitimate business activity incorrectly flagged.	• Lower noise = fewer false alarms • Fewer, high-quality alerts = faster triage • High alert volume = noise and chaos, slow response, higher costs	Three high-fidelity alerts for the full Windows scenario, with the threat actor's security signals correlated automatically, describing the attack path. Stable even after tuning.
Out-of-the-Box vs. Configuration Change	Comparison of default performance vs. tuned performance.	• Initial run shows baseline effort to get value • Configuration change shows adaptability • Heavy tuning leads to disruption and cost	Improved malicious substep visibility without increasing benign detections or alert volume. No heavy tuning required.
Prevention & Legitimate Activity Blocked	Ability to stop malicious activity without disrupting good activity.	• Early prevention avoids costly investigations • False blocks create tickets, exceptions, and trust issues	100% prevention with zero legitimate activity blocked.

WatchGuard Endpoint Security: Ultimate Protection. Zero Stress

A Leader and an Outperformer in the 2025 GigaOm Radar Report for Endpoint Detection and Response (EDR)

WatchGuard stood out as a Top Innovator and was ranked highly for unifying zero trust prevention, AI-driven behavioral analytics, and efficient investigations in one easy-to-use endpoint platform.



Find Out More

For more details, check out the **WatchGuard MITRE ATT&CK ER7** web page and the table below connecting MITRE insights to real-world benefits.

WatchGuard Endpoint Security blocks ransomware, zero-day, and fileless attacks that evade traditional controls while cutting alert noise. It scales with add-ons for visibility, patching, full-disk encryption, and SecOps tools, as part of WatchGuard's Unified Security Platform for unified management across networks, endpoints, Wi-Fi, and identities.

About WatchGuard

WatchGuard® Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers. Unlike others, WatchGuard delivers *Real Security for Real World* environments through its Unified Security Platform®, bringing networks, endpoints, and identities together with AI and zero trust advances for strong protection that scales. Trusted by more than 17,000 security resellers and managed service providers protecting over 250,000 companies, WatchGuard helps partners grow fast, eliminate operational drag, and deliver strong outcomes – without added vendors, consoles, or complexity. WatchGuard is headquartered in Seattle, Washington, with offices worldwide. Learn more at WatchGuard.com

NORTH AMERICA SALES 1.800.734.9905 INTERNATIONAL SALES 1.206.613.0895 WEB www.watchguard.com