Qualys.

Essential EDR Must-Haves: A Selection Guide for Advanced Endpoint Detection and Response Solutions

The volume and complexity of attacks targeting the enterprise, large and small, is growing faster than the capabilities of conventional Endpoint Detection and Response (EDR) solutions to keep up. This has led to upstart vendors claiming that EDR is obsolete. The truth of the matter is that endpoints continue remain as the front-line of the attack surface and protecting them continues to be a challenge balancing the usability needs of the end-user vs. the strict controls that are needed to detect and prevent threats.

EDR solutions should be assessed using 5 basic capability metrics:

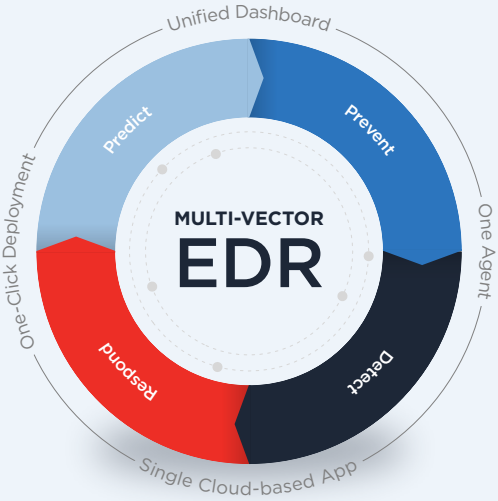
1 Zero-Day Detection

Legacy endpoint protection platforms (EPP), while outdated, are still the choice endpoint solution for many IT security teams. The reasons for this are often due to budget limitations, apathy, or a combination of both. The issue here more than anything else is that EPP solutions do not protect companies from unknown zero-day threats — a must in today's threat landscape.

How we do it

With **Qualys Multi-Vector EDR**, security professionals identify indicators of compromise (IoCs) utilizing the industry's most comprehensive behavioral detection, integrated threat intelligence, and machine learning. Telemetry that is collected by endpoints is correlated and mapped directly to **MITRE ATT&CK** Tactics and Techniques provide rich contextual analysis and meaningful insight into suspicious and malicious activities associated with an attack to not only protect from known threats, but unknown zero-day threats as well.

Qualys Multi-Vector EDR:
Endpoint Security Redefined



Qualys Multi-Vector EDR is a dynamic detection and response solution powered by the Qualys Cloud Platform. The Qualys EDR solution unifies multiple context vectors like asset management, vulnerability detection, policy compliance, patch management, and file integrity monitoring capabilities — all delivered with a single agent and cloud-based app.

2 Integration with Asset Management and Inventory Platforms

You cannot secure what you cannot see. Mapping malware to devices that they could exploit is the best way of hardening a hybrid network environment composed of both on-premises and remote endpoints. As mentioned, EDR is a critical component of an advanced security stack, but it is merely one component. Therefore, EDR solutions must not be evaluated as self-standing solutions, but as part of an orchestrated system that includes asset management, vulnerability management, and policy compliance as well. Before making a buying decision, protect your existing technology investments by assessing the integration and user experience of every EDR solution alongside these adjacent tools and platforms.

How we do it

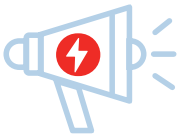
Multi-Vector EDR is the only solution in the industry integrated with the **Qualys Cloud Platform**, unifying multiple context vectors around asset criticality, high priority vulnerabilities and system misconfigurations associated with threats, as well as recommended patches to reduce your organization's mean-time-to-respond (MTTR). With a single and unified dashboard, Qualys solutions such as Cybersecurity Asset Management (**CSAM**) and Vulnerability Management, Detection and Response (**VMDR**) can be leveraged at the endpoint by users.

3 Vulnerability and Patching Support

Prevention is an overlooked capability not associated with traditional EDR solutions. However, unpatched vulnerabilities leave the door open for malware to successfully infect an endpoint and carry out its malicious objectives. Do not compromise when evaluating endpoint solutions and make sure they support your patching and prevention needs.

How we do it

Multi-Vector EDR is natively integrated with **Qualys VMDR**, allowing you to take a single malware incident, immediately pivot to identify all assets susceptible to the same exploit, and patch them all using **Qualys Patch Management**.



4 Alert Prioritization

As tools expand and alert volumes grow, more alerts do not always equate to superior detection and response. Prioritizing your response according to an incident's urgency and potential business impact is paramount for security teams looking to reduce false positives and optimize remediation efforts.

How we do it

Multi-Vector EDR leverages the **asset criticality score** tagged using **Qualys CSAM** to help your incident response teams prioritize resources and reduce alert fatigue. Like a microscope, Multi-Vector EDR provides deep insight into an endpoint to find the root cause of an infection. Then its findings from endpoints are shared with **Qualys Context XDR**, which acts as a wide-angle lens to provide a big picture view of an attack that spans multiple devices. The result is that threats that could have the biggest negative impact on your business are prioritized first for remediation.

5 ROI (return on investment)

EDR is part of a comprehensive security stack. Make sure that the vendor you select is invested in ongoing research and development of their EDR solution. Make sure it can leverage adjacent tools within your security portfolio. Most EDR solutions claim to have a light footprint, have an open API, or support seamless integration with other tools. However, this is not always the case. Furthermore, these integrations and upgrades always result in upcharges and more agents. Put EDR vendors to the test. Make sure that your chosen solution is one that scales with your organization as it grows at a cost that is competitive.

How we do it

Since **Multi-Vector EDR** is an extension of the **Qualys Cloud Platform**, security practitioners benefit from native integrations with **CSAM**, **VMDR**, **Policy Compliance** and **Patch Management**. With Qualys Multi-Vector EDR, security practitioners achieve advanced endpoint threat protection, improved threat context, and alert prioritization at a lower total cost of ownership compared to traditional EDR.

To learn more about Qualys Muli-Vector EDR and how we are helping customers reduce the risk of compromise by integrating vulnerability management with endpoint threat detection & remediation go to **www.qualys.com/apps/endpoint-detection-response/**

v220418