

EDR

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 This has led to upstart vendors claiming that EDR is obsolete.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Legacy endpoint protection platforms (EPP), while outdated, are still the choice endpoint solution for many IT security teams. Yet, EPP solutions do not protect companies from unknown zero-day threats — a must in today's threat landscape. When assessing an endpoint security solution, always test unknown and unknown threat detection capabilities.



2 Integration with Asset Management and Inventory Platforms

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.



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.



4 Alert Prioritization

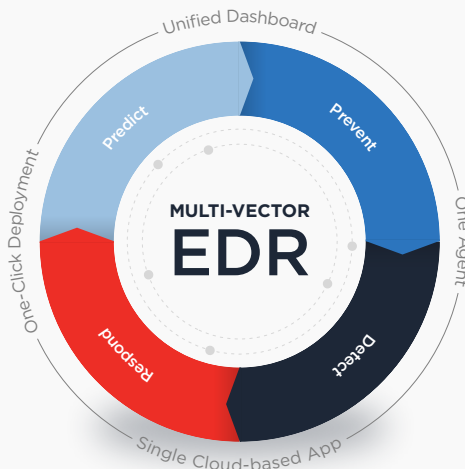
As tools expand and alert volumes grow, more alerts do not always equate to superior detection and response. Prioritizing your response according to an incident's urgency and potential business impact is paramount for security teams looking to reduce false positives and optimize remediation efforts.

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.



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.

To learn more about the Qualys approach to EDR is reducing the risk of compromise for our customers by integrating vulnerability management with endpoint threat detection & remediation go to

www.qualys.com/apps/endpoint-detection-response/

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.



For more information, please visit qualys.com