SOLUTION BRIEF

Boost Endpoint Security With Real-time, Automated Incident Response

Since January 1, 2016, more than 4,000 ransomware attacks have occurred daily on average.[1]

Executive Summary

Today's attacks, including ransomware, can take just minutes, sometimes even seconds, to compromise endpoints. Traditional endpoint protection platforms (EPPs) and even first-generation endpoint detection and response (EDR) tools simply cannot keep pace. In the case of EPP, solutions fail to detect frequent variants and newer fileless attacks. First-generation EDR tools require manual triage and responses that are not only too slow but also generate many alerts. Both of these types of solutions leave organizations exposed to cyber criminals, drive up the cost of security operations, and slow incident response processes, causing production shutdowns and disrupting system users.

FortiEDR addresses these deficiencies with advanced, real-time threat protection for endpoints both pre- and post-infection. FortiEDR proactively reduces the attack surface, prevents malware infection, and detects and defuses potential threats in real time. FortiEDR stops breaches and ransomware damage automatically and efficiently, streamlining security operations, and keeping users and production equipment online and working.

How FortiEDR Post-infection Protection Works

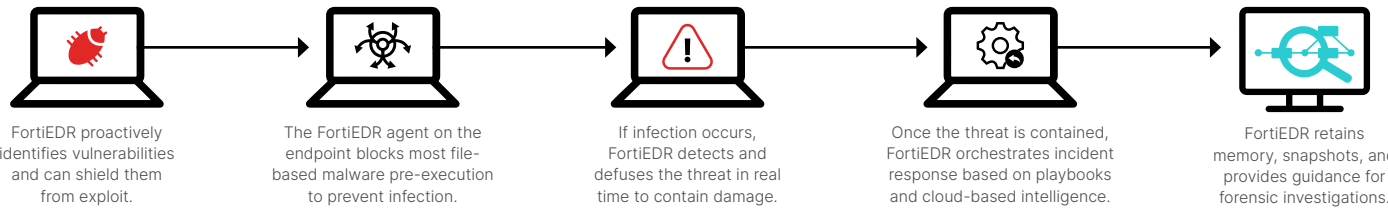

Figure 1: FortiEDR in action.

How FortiEDR Bolsters Endpoint Security

FortiEDR is a modern endpoint security solution that packs a broad set of prevention, detection, and response capabilities into a lightweight footprint that is easy to deploy, even on devices with limited system resources. The key capabilities of FortiEDR include proactive discovery and risk mitigation, next-generation antivirus (NGAV), behavior-based detection, real-time blocking, automated incident response, forensic investigation, threat hunting, and virtual patching capabilities (Figure 1). FortiEDR is part of the Fortinet Security Fabric architecture and integrates with Security Fabric components such as FortiGate, FortiNAC, FortiSandbox, and FortiSIEM.

Proactive risk mitigation

FortiEDR continuously identifies unmanaged devices and applications using FortiEDR collectors installed on existing endpoints, providing security teams with full visibility. Analysts can assign communication control policies based on application ratings, vulnerabilities, and real-time threat intelligence. This proactive risk mitigation minimizes the number of vulnerable endpoints and reduces the attack surface.

Real-time prevention

FortiEDR incorporates a machine learning (ML)-based antivirus (AV) engine along with FortiGuard threat intelligence to protect against file-based malware. FortiEDR protects endpoints even when they are not connected to the internet. With a small footprint and broad operating system support, FortiEDR can be deployed on devices with limited resources such as point-of-sale (POS) terminals running real-time operation systems and process controllers in manufacturing operations.

Automated detection and blocking

FortiEDR uses behavior-based detection to identify and defuse potential threats automatically. This approach is particularly effective against fileless malware, which easily evades traditional AV defenses by hiding in memory and never touching the disk. Fileless threats make use of legitimate system resources (also called living off the land) and execute attacks entirely in memory or deliver other attack vectors such as ransomware to accomplish their malicious goals.

FortiEDR also includes patented ransomware protection that dynamically re-routes write requests to a copy of the original file in order to compare entropy before blocking or allowing the change.

When suspicious behavior occurs, FortiEDR immediately thwarts the attacks by blocking all requested outbound communications or access to the file system. At the same time, the FortiEDR cloud-based analytics continuously classify (and reclassify) the threats for appropriate response actions and eliminate noise to streamline security analysis and operations.

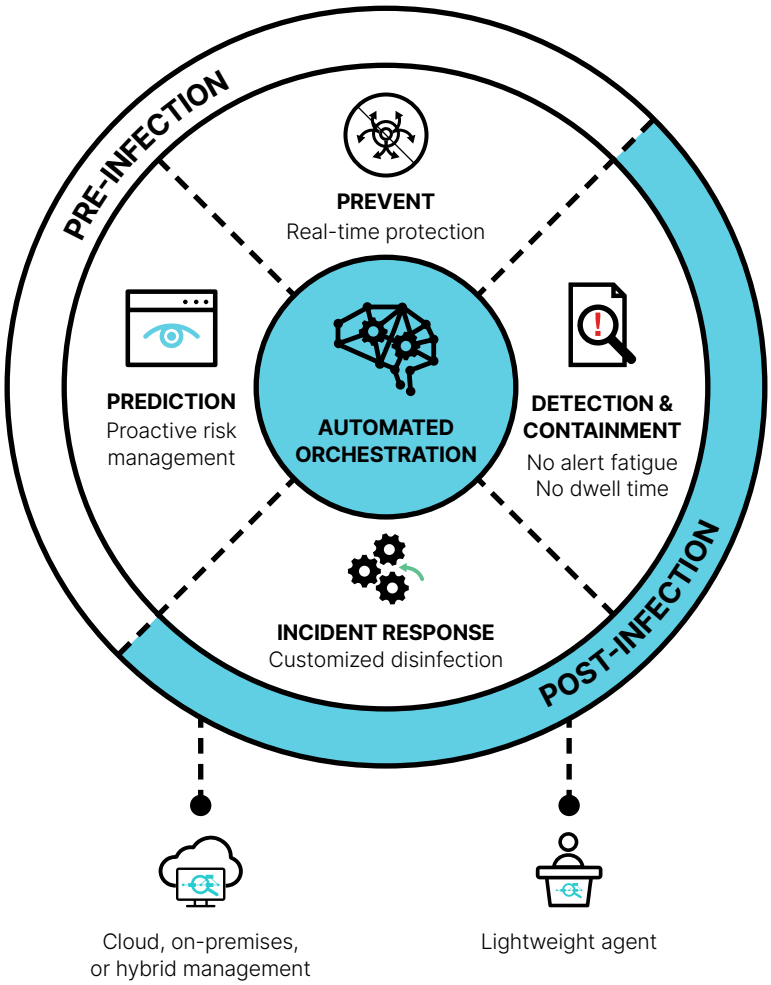

Figure 2: FortiEDR offers pre- and post-infection features to improve endpoint protection, detection, and response.

Orchestrated incident response

FortiEDR comes with an intuitive framework to predefine common response actions to enable orchestrated and automated incident response and remediation. Typical automated actions include terminating malicious processes, removing files, cleaning up persistency, rolling back malicious changes, notifying users, isolating applications and devices, and opening tickets.

Not all endpoints have the same risk tolerance. For example, the controller system on the manufacturing floor requires high availability and therefore has a lower risk tolerance than an employee's laptop. With playbooks, security teams can design a context-based incident response that initiates the appropriate actions based on threat classification and the endpoint group. This approach ensures a consistent incident response, reduces the time security teams spend on routine tasks, and helps organizations align their endpoint security policies with risk tolerance.

Forensic investigation

FortiEDR features a unique guided interface that offers clear explanation for alerts and suggests logical next steps for the forensic investigation. FortiEDR automatically enriches data with detailed information on attack techniques from trusted sources such as the MITRE ATT&CK database. Patented code-tracing technology gives security teams full visibility across the cyberattack chain. FortiEDR also reserves memory snapshots of attacks to aid investigation.

Business Benefits

FortiEDR delivers significant business value in the areas of endpoint protection, incident response, security operations, and business continuity.

Improve security with real-time protection

Working in real time and leveraging ML, FortiEDR stops breaches and prevents data loss and ransomware damage in real time, eliminating the time gap between detection and response. FortiEDR not only improves the organization's endpoint protection but also minimizes the impact of threats that manage to bypass the prevention stack.

Optimize security operations

FortiEDR optimizes security workflows with customizable, standardized incident response processes. FortiEDR frees staff time and reduces alert fatigue by automating repetitive tasks and minimizing false positives. By automatically combining alerts, linking events, and presenting a coherent attack graph, FortiEDR streamlines incident response and forensic investigations.

Ensure business continuity

FortiEDR enables response and remediation on running systems, which prevents production disruptions and maintains user productivity. FortiEDR supports legacy equipment with limited system resources, extending their useful life. Security teams can use FortiEDR to roll back malicious damage and avoid costly system reimaging.

Typical Use Cases for FortiEDR

FortiEDR prevents, detects, and defuses threats in operational technology (OT) environments while keeping machines online to avoid production shutdowns. It discovers vulnerabilities and delivers mitigation controls such as virtual patching to protect systems from exploits until the next available maintenance window. Featuring a small footprint, FortiEDR supports legacy equipment and air-gapped systems without affecting device performance.

FortiEDR protects credit card information at point of sale (POS), stopping attacks at the source. Payment Card Industry Data Security Standard (PCI DSS) certified, FortiEDR prevents data exfiltration in the event of system compromise. FortiEDR delivers virtual patching to shield POS systems from vulnerabilities. It offers embedded OS support with a small footprint that is suitable for legacy POS equipment.

FortiEDR Feature Summary

Pre-infection		Post-infection			
Discover and Protect	**Prevent**	**Detect**	**Defuse**	**Respond and Investigate**	**Remediate and Roll Back**
Proactive risk mitigation	**Pre-execution protection**	**Detect threats in real time**	**Stop breach and data loss**	**Full attack visibility**	**Disinfection**
■ Discover rogue devices and IoT ■ Application and reputation ■ Vulnerabilities ■ Risk-based policies reduce attack surface ■ Virtual patching	■ Kernel-level ■ Machine learning and signatureless ■ Application communication control ■ Eliminate data tampering and exfiltration ■ Applications communication control	■ No alert fatigue ■ Provide malware classification ■ Display IOCs ■ Deliver full attack chain	■ First and only real-time post-infection blocking ■ Block outbound communications ■ Prevent file encryption by ransomware	■ Customizable incident response playbooks ■ Eliminate dwell time ■ Capturing forensic data ■ Memory snapshot for fileless attack ■ Conduct threat hunting in your time	■ Roll back malicious changes ■ Remove bad files ■ Clean up persistency ■ Eliminate reimage/rebuild ■ Ensure business continuity ■ REST API output for external remediation tools

Fortinet Deployment and MDR Services

- Fortinet Professional Services provides expert assistance for architecture planning, configuration, playbook setup and customization, and training.
- FortiResponder is the Fortinet Managed Detection and Response (MDR) Service, which offers 24×7 threat monitoring, alert triage, and remote remediation services for peace of mind.
- FortiGuard Incident Readiness Service will assess an organization's plan and posture to handle ransomware, provide training, conduct tabletop exercises, and more.
- FortiGuard Incident Response Service is available to handle forensic investigation, determine incident scope, speed remediation, and support a return to safe operation.
- Certified Fortinet managed security service provider (MSSP) partners deliver MDR services, including fully managed security operations centers.

Conclusion

With the steady increase in the number and sophistication of advanced threats and ransomware, organizations must increase their security measures across the board, including their endpoints. FortiEDR offers next-generation endpoint protection, including the addition of a patented defuse capability: detection and response that is lightweight and easy to deploy. With FortiEDR, security teams can boost endpoint security, thereby speeding up incident response, streamlining security operations, and avoiding costly disruptions to production lines and knowledge workers. Optional MDR, assessment, and forensics services are available to augment in-house security staff and skills.

[1] "How to Protect Your Networks from Ransomware," U.S. Federal Bureau of Investigation, accessed November 6, 2021.

FORTINET®

www.fortinet.com

November 20, 2021 1:00 AM
580266-B-0-EN