SOLUTION BRIEF

Automated Endpoint Security Prevents Unplanned Downtime From Ransomware Attacks

Executive Summary

Given recent headlines, senior enterprise leaders are more aware of the risks and cyber threats to operational technology (OT) and industrial control system (ICS) environments. These threats can traverse the network from IT and cause disruption to OT endpoints or they can be a direct attack to OT endpoints.

According to a recent study based on a survey of respondents running OT systems, ransomware was their top concern (54.2%), followed by nation-state cyberattacks (43.1%), and non-intentional threat vectors caused by unapproved devices that can't defend themselves (34.5%).[1]

CISOs face several challenges in fulfilling these expectations, including securing OT endpoints. FortiEDR provides a robust solution for OT endpoint security by offering real-time threat protection, both pre- and post-infection. Organizations that deploy FortiEDR on their OT endpoints benefit from faster threat responses, automated actions, and fewer disruptions to production activities.

Cyberattacks on critical infrastructure are on the rise. A recent survey found that 9 out of 10 OT organizations experienced at least one intrusion in the past year.[2]

Vulnerable OT Endpoints

OT infrastructures in manufacturing, transportation, utilities, oil and gas, and other industries are increasingly becoming the targets of sophisticated cyberattacks. The weapon of choice is ransomware, which takes just seconds to encrypt crucial ICS components. Cryptoware can disrupt or even shut down the engineering workstations and supervisory control and data acquisition (SCADA) servers and historians essential to operating production lines and safety systems. The motivations for these types of attacks vary. Some bad actors seek financial gain via ransom payments, while others aim to disable critical infrastructure and cause havoc in the community and beyond.

FortiEDR provides superior endpoint protection features for production environments, including:

- Real-time ransomware protection
- Support for legacy systems, including Windows XP Service Pack 2, Windows Server 2003, and 15-year-old Linux systems
- USB port protection with device control
- Secure remote remediation
- Virtual patching and application control
- Lightweight agent
- Automated response playbooks

In the past, many OT infrastructures were self-contained and isolated (or "air gapped") from unsecured networks, such as the public internet. Hence, they were relatively safe from internet-based threats. Now that OT and IT systems are converging, outdated and unpatched OT endpoints represent a tempting entry point for attackers. Compounding the problem, OT devices often run on legacy operating systems with limited system resources, making them difficult to protect with traditional endpoint security solutions.

To address these security challenges, many organizations have added a broad selection of point security products to cover each new risk exposure. However, this approach introduces complexity and leaves security gaps. Complexity has driven cyber risks and costs to dangerous new heights. Additionally, isolated and fragmented systems are a significant challenge in managing OT security. To learn more, see Simplifying Cybersecurity by PWC.

FortiEDR for OT Environments

FortiEDR addresses these problems with advanced, real-time threat protection—both pre- and post-infection—for the full range of OT endpoints. FortiEDR is a modern endpoint security solution with a broad set of endpoint detection and response (EDR) capabilities in a lightweight footprint that is easy to deploy, even on legacy OT systems with limited system resources.

FortiEDR includes next-generation antivirus (NGAV), application and communication control, automated EDR, real-time behavior-based blocking, threat hunting, incident response, and virtual patching capabilities (see Figure 1). FortiEDR leverages the Fortinet Security Fabric architecture and integrates with Security Fabric components, such as FortiGate, FortiNAC, FortiSandbox, FortiSIEM, and FortiSOAR, as well as comes with over 300 prebuilt third-party connectors along with respective actions that can be configured to respond according to your automatic incident response actions. Furthermore, customers can create other third-party connections and actions via REST API.

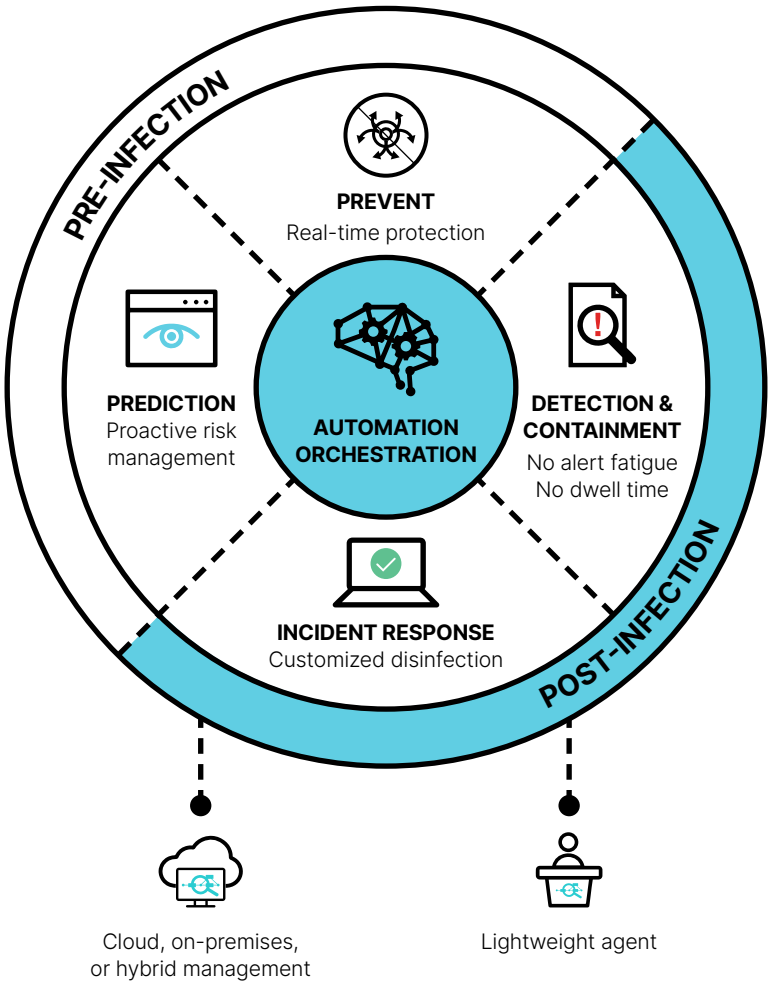

Figure 1: FortiEDR capabilities.

Key Benefits of FortiEDR

FortiEDR delivers tangible business value to OT organizations with benefits such as real-time automated response, production continuity, and nondisruptive risk mitigation.

Ransomware protection

FortiEDR blocks ransomware both pre-and post-execution. It is the only endpoint security solution that can protect systems and files even after an endpoint has been compromised. This feature is important because modern ransomware uses attack techniques such as script-based and fileless attacks and can also use existing tools on the system to evade detection. FortiEDR uses behavior-based detection to find and block file access to prevent encryption. It also can restore encrypted files in real time across Windows, Mac, and Linux systems.

Support for legacy operating systems

Commissioned OT and ICS components are expected to run for 20 years or longer, often exceeding the support period provided by operating system vendors. Ripping and replacing legacy OT environments because of end-of-support notifications from operating system vendors is often considered too costly, and it's usually deferred. Most endpoint vendors prefer to focus on supported operating system environments, which can leave many production systems vulnerable to cryptoware and other malware.

FortiEDR maintains support for old operating systems, including Windows XP Service Pack 2, Windows Server 2003, and variants of Linux that are 15 years old. Supporting these older operating systems helps FortiEDR address legacy OT environments.

> *"In our legacy environment, if our endpoint solution detected something, it would take at least half a day for remediation efforts to begin. In contrast, if FortiEDR detects an issue, the time to response is almost immediate."*
>
> - Shaun Guthrie, Senior Director, IT, Alberta Urban Municipalities Association (AUMA)

Real-time automated response

When FortiEDR detects potentially malicious processes, it defuses them in real time by blocking the potential malicious action automatically. This process effectively pauses the attack and stops ransomware encryption, lateral movement, credential theft, and data exfiltration. At the same time, the Fortinet Cloud Service continues to gather evidence and validate and classify the events. Using customized playbooks, security teams can prescribe automated actions based on endpoint group, mission criticality, and threat categorization. Automated response and remediation actions include terminating processes, removing malicious or infected files, cleaning up persistency, notifying users, and opening tickets.

By comprehensively securing endpoints in real time, both pre- and post-infection, FortiEDR helps eliminate alert fatigue and breach anxiety. It also standardizes incident response procedures and optimizes security and operations resources.

Production continuity

The potential pitfall of real-time automatic response is that legitimate application activities can trigger the detection system and generate false alarms. Blunt-force response actions can interfere with applications, or worse, cause blue-screen crashes that bring down mission-critical production systems.

Instead of terminating processes and quarantining endpoints, FortiEDR defuses threats by blocking their outbound communications and their attempts to access the file system. If the suspicious process turns out to be benign, FortiEDR releases the block with little impact on the production process. For security incidents, FortiEDR enables remediation actions without taking the machine offline. As a result, systems in the production plant environment remain online and users are not affected.

This capability is particularly important for converged IT/OT infrastructures because it allows security teams to take swift and effective action to secure OT devices while avoiding lost production. FortiEDR is uniquely able to defuse threatening cryptoware or high-risk command-and-control communications while maintaining OT availability.

Nondisruptive risk mitigation

Patching OT systems can be tricky. To avoid production disruptions, operations teams are often forced to follow a mandated change process that only allows mitigation within a scheduled maintenance window. In the meantime, the systems are vulnerable to attacks.

FortiEDR solves this problem with continuous application and vulnerability assessment, so security teams can proactively mitigate risks with virtual patching or application control. This proactive approach reduces the exposure and avoids taking production machines offline between scheduled maintenance windows or hardens devices to not run specific applications or only run certain ones.

How FortiEDR Protects OT Endpoints

Figure 2: FortiEDR in action.

Discover and predict

FortiEDR proactively discovers and reduces the endpoint attack surface. It does this by providing visibility into rogue devices and applications, identifying vulnerabilities in systems or applications, and proactively mitigating risks with virtual patching.

Prevent

Kernel-based NGAV provides automated prevention of file-based malware. When combined with continuously updated cloud-based threat-intelligence feeds and machine learning (ML), FortiEDR becomes smarter over time to more effectively identify threats.

Detect and defuse

Using behavioral-based detection, FortiEDR is the only solution that provides post-infection protection to stop breach and ransomware damage in real time.

Ransomware protection

FortiEDR provides an out-of-the-box security policy for ransomware protection. It detects and prevents, in real time, an attacker's attempt to encrypt, lock, or modify data. FortiEDR then generates an alert that contains the information required to initiate an investigation, so the root cause of the security breach can be uncovered and fully remediated. The infected devices continue to function as usual without disruption.

Respond and remediate

Using customizable playbooks, security teams can orchestrate incident response operations, streamline and automate incident response and remediation processes, and keep affected machines online. This approach avoids interrupting users and disrupting the business without exposing the network to risk.

Investigate and hunt

FortiEDR provides detailed information on threats to support forensics investigation. Its unique interface provides helpful guidance and best practices and suggests the next logical steps for security analysts.

Recent research found that ICS vulnerabilities have increased 41% in the six months leading up until August. Of these, 61% were remotely exploitable, and 66% did not require any user interaction for exploitation. Moreover, almost three-quarters of vulnerabilities (74%) did not require specific privileges.[3]

Fortinet Deployment and MDR Services:

- Fortinet Professional Services provides expert assistance for deployment, configuration, playbook setup, customization, and more
- FortiResponder, Fortinet's MDR service, offers 24×7 threat monitoring, alert triage, and remote remediation services
- Certified Fortinet MSSP partners also deliver MDR services including fully managed security operations centers (SOCs)

Simulation mode capabilities

Run FortiEDR in simulation mode first on OT systems to allow plant operators to tune the policies as they exercise all the normal day-to-day procedures associated with production. Operators using FortiEDR in simulation mode have found gaming and other services deployed that did not belong.

USB device control

FortiEDR protects USB ports with a granular policy to monitor and block unauthorized USB devices, such as USB mass storage devices. Users can completely lock down USB ports.

Secure remote shell

Grant administrators remote troubleshooting capabilities for their work-from-anywhere workforce with a suite of security utilities including the generation of single-use time-defined certificates to mitigate abuse.

Conclusion

With the steady increase in the number and sophistication of advanced threats—especially ransomware—organizations must increase their security measures across the board, including their OT endpoints. FortiEDR provides endpoint protection that is lightweight and easy to deploy on OT devices with limited resources. With FortiEDR, security teams can boost endpoint security, thereby speeding up incident response, streamlining security operations, and avoiding costly disruptions to production lines and user productivity.

[1] Mark Bristow, "A SANS 2021 Survey: OT/ICS Cybersecurity," SANS, August 24, 2021

[2] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

[3] Jeff Cornelius, "Why Are Industrial Control System Attacks Increasing?" InfoSecurity Magazine, September 22, 2021.

March 9, 2022 6:30 AM
1019901-A-0-EN