SOLUTION BRIEF

# Protecting OT Infrastructures with Real-time, Automated Endpoint Security

## Executive Summary

**The convergence of operational technology (OT) and information technology (IT) infrastructures is gaining momentum, and cybersecurity professionals are on board. A recent study found that 70% are supportive of OT/IT convergence.[1] In addition, the CISO is seen as a key player, with 65% of respondents pointing to the CISO as the individual most responsible for a secure converged infrastructure.[2]**

**CISOs face a number of challenges in fulfilling these expectations, among which is 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 avoiding disruptions to production activities.**

**FortiEDR provides superior endpoint protection for production environments featuring:**

- Real-time threat detection
- Post-compromise protection
- Remediation without production disruptions
- Virtual patching
- Support for air-gapped systems and legacy Windows systems
- On-premises deployment options

**Cyberattacks on critical infrastructure are on the rise: A recent survey found that 54% of respondents expect an attack on critical infrastructure in the next 12 months.[3]**

## The Vulnerable OT Endpoint

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 cryptoware, a form of ransomware that takes just seconds to encrypt crucial control information and thereby disrupt or even shut down production lines and safety systems. Motivations for such attacks vary: Some seek financial gain through ransom payments, while others aim to disable critical infrastructure and cause havoc in the community and beyond.

In the past, OT infrastructures were self-contained—often air gapped—and thus relatively isolated from internet-based threats. Now that OT and IT systems are converging, outdated and unpatched OT endpoints represent a tempting entry point for cyberattackers. 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 gaps in the security posture. In a recent survey, 55% of respondents identified “isolated and fragmented systems” as a significant challenge in managing OT security.[4]

## FortiEDR for OT Environments

FortiEDR addresses these problems and more with advanced, real-time threat protection, both pre- and post-infection, for the full range of OT endpoints. FortiEDR is a next-generation endpoint security solution that packs a broad set of EDR capabilities into a lightweight footprint that is easy to deploy, even on legacy OT devices with limited system resources.

Key capabilities of FortiEDR include next-generation antivirus (NGAV), application communication control, automated endpoint detection and response (EDR), real-time blocking, threat hunting, incident response, and virtual patching capabilities (Figure 1). FortiEDR leverages the Fortinet Security Fabric architecture and integrates with Security Fabric components such as FortiGate, FortiNAC, FortiSandbox, and FortiSIEM.

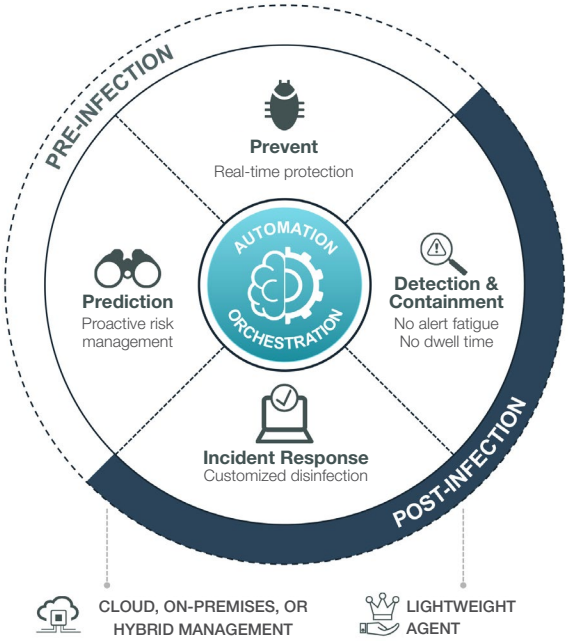



Figure 1: FortiEDR capabilities.

## 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.

### Real-time Automated Response

When FortiEDR detects potentially malicious processes, it defuses them in real time with automatic blocking. At the same time, the Fortinet Cloud Service continues to gather evidence and validate and classify the events. Customized playbooks allow security teams to 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.

Comprehensively securing endpoints in real time, both pre- and post-infection, FortiEDR eliminates alert fatigue and breach anxiety, standardizes incident response procedures, and optimizes security and operations resources.

### Production Continuity

Real-time automatic response has a potential pitfall that can make life difficult for security professionals. Legitimate application activities can trigger the detection system and thereby generate false alarms. Blunt-force response actions can interfere with applications, or worse, cause blue-screen crashes that bring down the mission-critical production system.

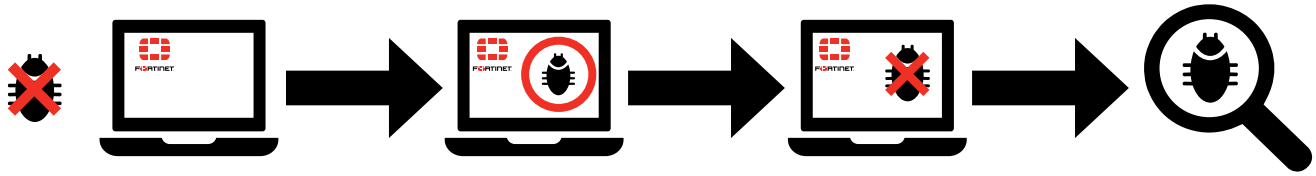
Instead of terminating processes and quarantining endpoints, FortiEDR defuses threats by blocking their outbound communications and attempts to access the file system. If the suspicious process turns out to be benign, FortiEDR releases the block with little impact on the production systems. For security incidents, FortiEDR enables remediation actions without taking the machine offline. As a result, systems on the manufacturing floor 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 unintended consequences on the IT side of the house.

### Non-disruptive Risk Mitigation

Patching OT systems can be tricky. To avoid production disruptions, operations teams are often forced to follow the 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 that allows the security team to proactively mitigate risks with virtual patching. This proactive approach reduces the exposure and avoids taking production machines offline between scheduled maintenance windows.

## How FortiEDR Protects OT Endpoints



**The FortiEDR agent on the endpoint blocks most file-based malware pre-execution to prevent infection.**

**When infection occurs, FortiEDR detects and defuses the threat in real time to contain damage.**

**Once the threat is contained, FortiEDR orchestrates incident response based on playbooks and cloud-based intelligence.**

**FortiEDR retains memory, snapshots and provides guidance for forensic investigations.**

Figure 2: FortiEDR in action.

### Discover and Predict

FortiEDR proactively discovers and mitigates 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, FortiEDR will also become 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.

### 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 guided interface provides helpful guidance and best practices and suggests the next logical steps for security analysts.

**In the global utilities industry, 64% of decision-makers say that sophisticated cyberattacks are a top challenge.[5]**

### Fortinet Deployment and MDR Services:

- Fortinet Professional Services provides expert assistance for deployment, configuration, playbook setup and customization, and more.
- FortiResponder, Fortinet's MDR service, offers 24x7 threat monitoring, alert triage, and remote remediation services.
- Certified Fortinet MSSP partners deliver MDR services including fully managed SOCs.

## 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 offers next-generation 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] "Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT," Ponemon Institute, February 2019.

[2] Ibid.

[3] Ibid.

[4] "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?" Siemens and Ponemon Institute, 2019.

[5] Ibid.

FORTINET®

www.fortinet.com



March 31, 2020 6:15 AM

579128-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\FortiEDR in OT\sb-protecting-ot-infrastructures-V2.1-3312020-604AM