SOLUTION BRIEF

Protecting OT Infrastructures With Real-time, Automated Endpoint Security

Executive Summary

The convergence of operational technology (OT) and information technology (IT) infrastructures continues to grow. Organizations now recognize the security of their industrial control systems (ICS) assets as fundamental to their business.[1] In fact, the number one concern for ICS organizations is ensuring reliability and availability of control systems.[2]

CISOs face a number of challenges in fulfilling these expectations, among which is securing OT endpoints. A recent survey by SANS found that "Endpoints—engineering workstations and ICS server assets—present the greatest risk for compromise."[3] 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 by accelerating threat responses, automating response actions, and avoiding disruptions to production activities.

The Vulnerable OT Endpoint

OT infrastructures in energy, manufacturing, transportation, utilities, and other critical industries are increasingly becoming the targets of sophisticated cyberattackers. The weapon of choice is cryptoware—a form of ransomware that takes just seconds to encrypt crucial information necessary to operate the ICS 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 past, OT infrastructures were self-contained and 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 Now that OT and IT systems are converging, outdated and unpatched OT endpoints represent a tempting entry point for cyberattackers.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 systems often run on legacy operating systems with limited system resources, making them difficult to protect with traditional endpoint security solutions.

To date, many organizations have tried adding 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, nearly 60% of respondents indicated that technical integration of legacy and aging OT technology with modern IT systems was their biggest challenge when securing OT technologies and processes.[6]

FortiEDR delivers superior endpoint protection for production environments by providing:

- Attack surface reduction complemented by virtual patching
- Real-time threat detection
- Post-compromise protection
- Remediation without production disruptions
- Support for legacy Windows, macOS, and Linux systems

Cyberattacks on critical infrastructure are on the rise. A recent study found that 83% of organizations suffered an operational technology (OT) cybersecurity breach in the prior 36 months.[4]

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

Fortinet's **FortiEDR** solution comprehensively secures endpoints in real time—both pre- and post-infection. It includes several key capabilities for protecting vulnerable OT endpoints: ML-based next-generation antivirus, application communication control, automated endpoint detection and response (EDR), real-time blocking, threat hunting, incident response, and virtual patching capabilities. In addition, FortiEDR also leverages the broader Fortinet Security Fabric architecture by integrating with Security Fabric components such as FortiGate, FortiNAC, FortiSandbox, and FortiSIEM.

FortiEDR—Cloud-native EPP + EDR

Detect, Defuse, Respond, and Remote Remediation

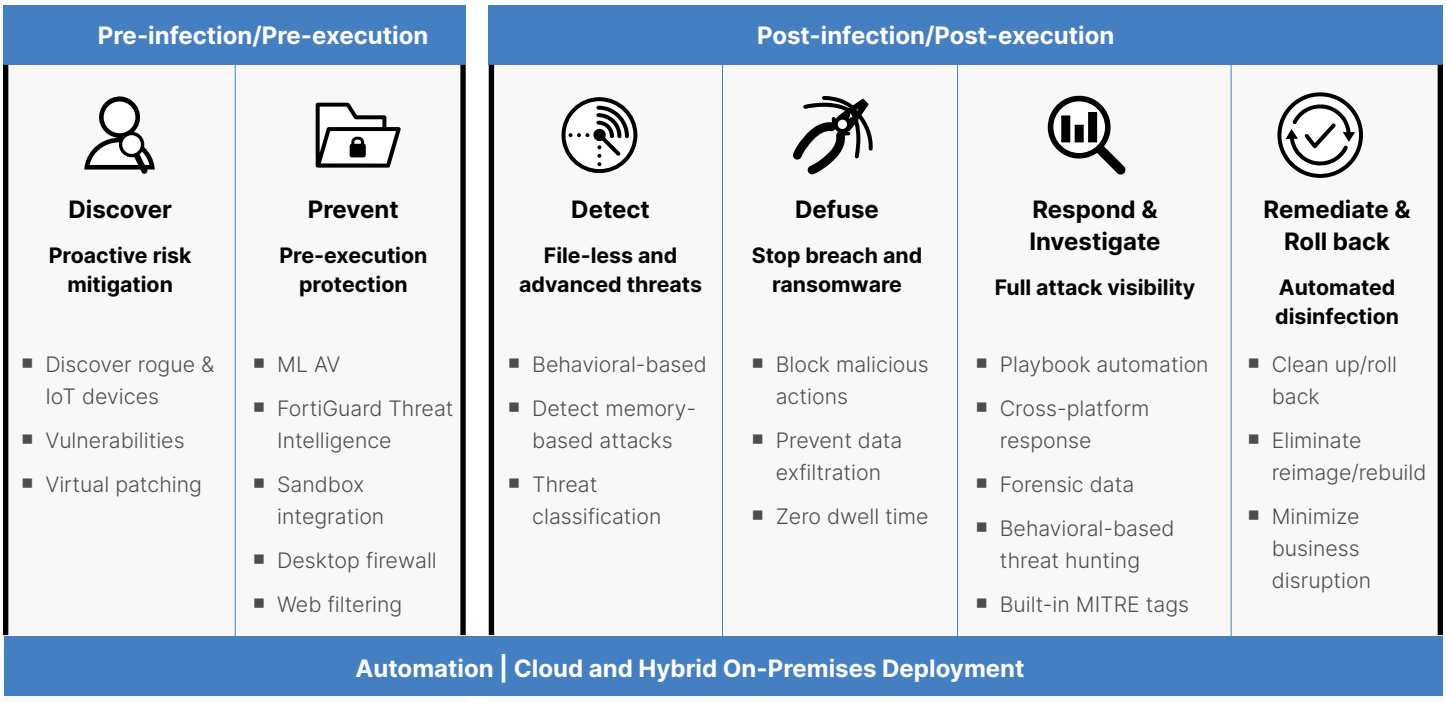

Figure 1: FortiEDR combines both pre-infection and post-infection endpoint defenses.

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, validate, and classify the events with its multiple sandboxes and code tracing technologies. Customized playbooks allow security teams to prescribe automated actions based on endpoint group, mission criticality, and threat classification. Automated response and remediation actions may include terminating processes, deleting malicious or infected files, cleaning up persistency, notifying users, and forwarding event logs to a syslog server. This all helps FortiEDR eliminate alert fatigue and breach anxiety, standardize incident response procedures, and optimize security and operations resources.

Production continuity. Real-time automatic responses can make life difficult for security teams when a legitimate application triggers the detection system and generates a false alarm. Blunt-force response actions can interfere with applications—or worse, cause operating system crashes that bring down a mission-critical production system. FortiEDR continuously classifies events until a final verdict is made. If Fortinet Cloud services classifies an event as safe, an automatic exception is created to prevent such occurrences in the future. FortiEDR's policy baselining and simulation features can help OT plant managers and security professionals avoid these sorts of occurrences. By running the system in simulation mode, the plant team can exercise all normal plant activities and ensure that endpoint protection and critical plant floor operations are in tune with one another. Recent FortiEDR deployments have been able to find critical OT policy violations such as connected mobile devices, Android services, and unauthorized systems—even before the system was taken out of simulation mode.

But instead of terminating processes and quarantining endpoints (which can disrupt sensitive OT operations), FortiEDR can be configured to just defuse threats by blocking their outbound communications and any 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 production floor remain online and productivity is 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 protecting the IT and OT networks.

Nondisruptive risk mitigation. Patching OT systems can be tricky. To avoid production disruptions, operations teams are typically forced to follow a mandated change process that only allows mitigation within a scheduled maintenance window. In the meantime, the systems remain vulnerable to attacks. FortiEDR addresses this common problem with continuous application and vulnerability assessment plus virtual patching capabilities to prevent vulnerable applications from communicating. This proactively mitigates risk exposure without taking production machines offline for unscheduled maintenance.

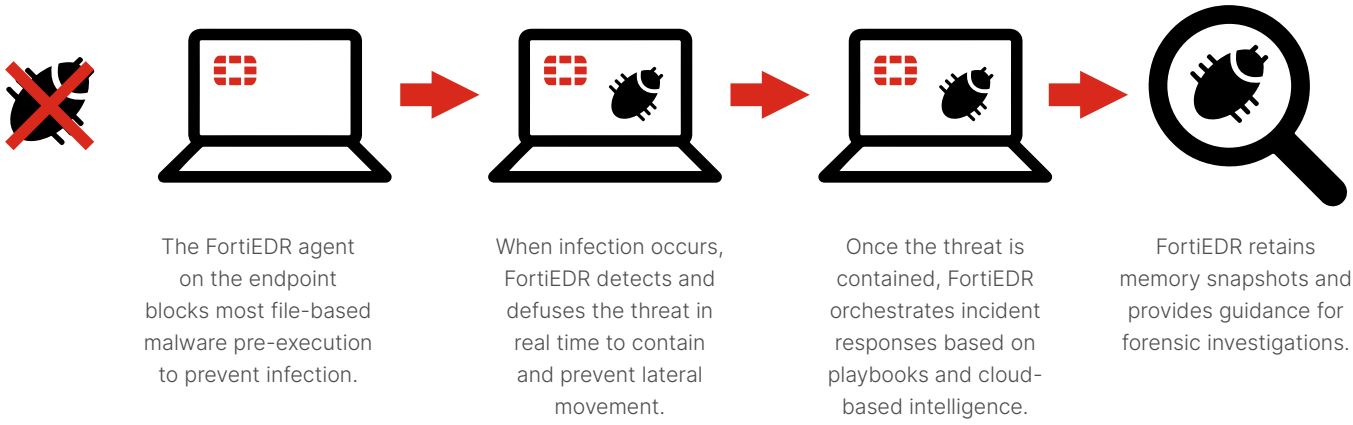

Figure 2: FortiEDR contains threats without disrupting OT systems.

Discover and predict. FortiEDR proactively discovers and mitigates risks across the endpoint attack surface. It does this by providing visibility into rogue devices and applications, identifying vulnerabilities in systems or applications, and providing virtual patching to cover exposures.

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 becomes smarter over time to more effectively identify threats.

Detect and defuse. Using behavior-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 business disruptions without exposing the network to risks.

Investigate and hunt. FortiEDR provides detailed information on threats to support forensics investigations. Its unique guided interface provides helpful support and best practices by suggesting the next logical steps for security analysts.

FortiEDR Deployment Prerequisites

FortiEDR can be deployed in an on-premises/hybrid model. The purpose of this deployment model is to accommodate scenarios where the endpoints need to be on-premises or isolated from the internet. In all other cases, a fully cloud-managed deployment will be required. Infrastructure requirements include:

- FortiEDR infrastructure services MUST be installed via the provided ISO installation files. These files contain the following software:
  - Security-hardened CentOS with only the required dependencies installed
  - FortiEDR infrastructure software
  - FortiEDR collector software
- Public cloud networking requirements:
  - A static public IP address for the Central Manager's outbound communication to the public cloud services. Fortinet Cloud Services are access controlled by public IP address.
  - Outbound access to this hostname "reputation.ensilo.com" on TCP port 443 is required. (Note: FortiEDR is formerly known as enSilo.)

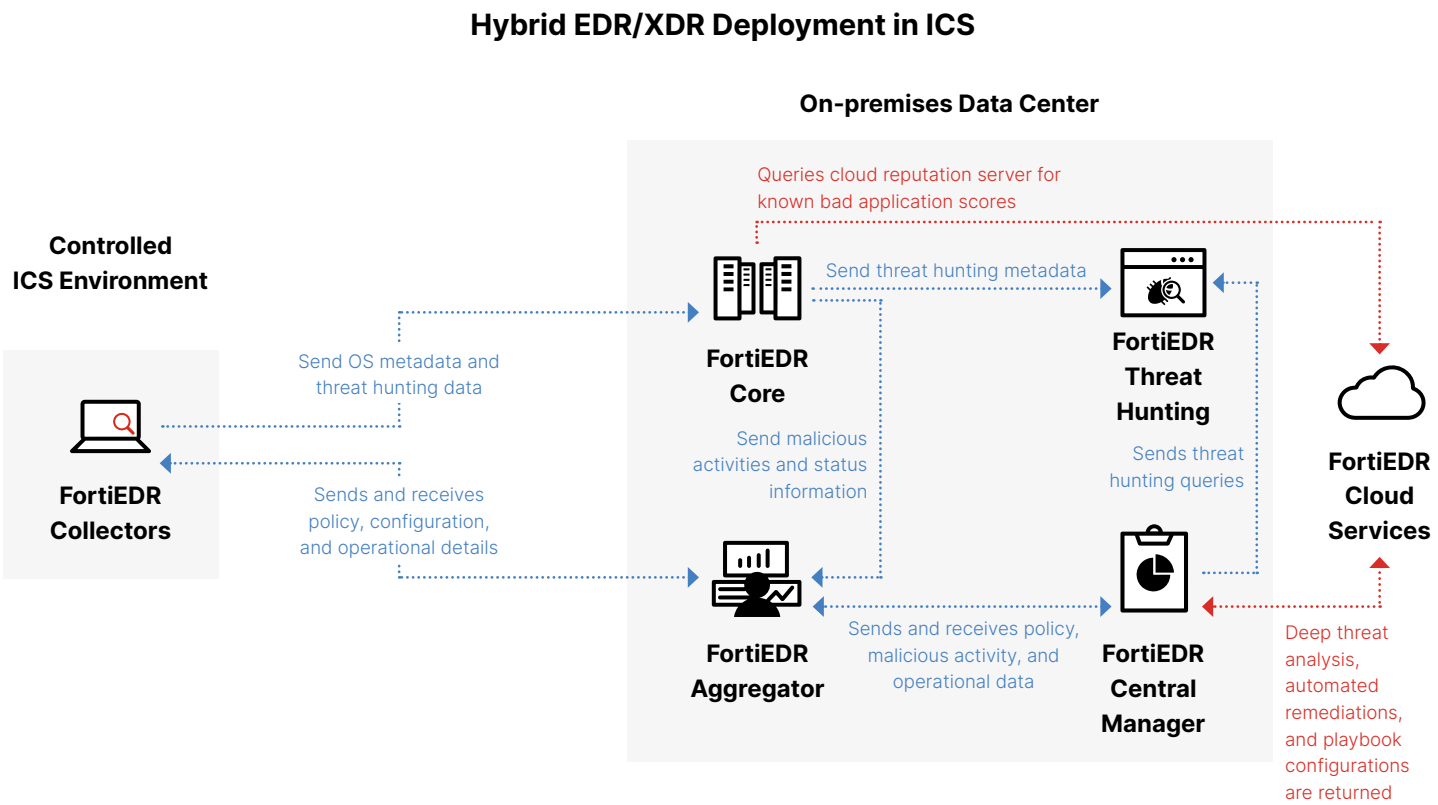

Figure 3: FortiEDR protects ICS environments.

Unsupported functionalities. SSL/TLS deep packet inspection is not supported. This deployment model requires a mutual trust relationship: client trusts server and server trusts client. SSL deep packet inspection is designed for single-way trust: client trusts server (such as with online shopping).

FortiEDR hybrid deployment

FortiEDR's hybrid deployment model includes the following components: Fortinet Cloud Services (FCS), FortiAV, and FortiGuard IP Reputation Services.

- In this architecture, FCS is a key part of FortiEDR. It enhances the post-execution protection and provides the following capabilities:
  - Sandboxing
  - Commonality analysis
  - Classification of events
  - File analysis (static and dynamic)
  - Flow analysis via machine learning
  - Automated incident response using the playbook feature
- FortiAV provides enhanced pre-execution protection against threats and uses intelligence from FortiGuard Distribution Services (FDS).
- Reputation services are used to allow or deny an application from communicating outside the organization and is part of FortiEDR's "Communication Control" feature.
  - Applications with a known bad reputation or that are distributed by questionable vendors are classified as such and can be blocked.
  - Attack surface reduction using risk-based proactive policies that are based on application CVE severity.
  - Outbound access to "reputation.ensilo.com" on TCP port 443 is required.

Fortinet deployment and support services

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

Conclusion

With a sharp 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 systems with limited resources. FortiEDR enables security teams to boost OT endpoint security by accelerating incident response, streamlining security operations, and avoiding costly disruptions to system operations and user productivity.

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

[2] Ibid.

[3] Ibid.

[4] "83% of critical infrastructure organizations suffered breaches, 2021 cybersecurity research reveals," PR Newswire, November 9, 2021.

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

[6] Ibid.

April 28, 2022 8:42 AM
1461001-0-0-EN