SOLUTION BRIEF

Operational Technology Cybersecurity Assurance with FortiDeceptor

Executive Summary

In 2024, more operational technology (OT) organizations are experiencing high numbers of intrusions. In a recent survey, nearly one-third of respondents had six or more intrusions, up from only 11% in 2023.[1] It was also notable that all types of intrusions increased, except malware.

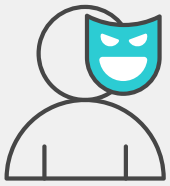
Many OT organizations must secure legacy supervisory control and data acquisition (SCADA) and industrial control system (ICS) devices found in OT environments, which is challenging. The problems often relate to incompatible IT security controls and the complexity of building a holistic security infrastructure encompassing OT, Internet of Things (IoT), and IT environments.

FortiDeceptor is a simple-to-use, non-intrusive solution that provides early detection of threats that target OT and IT environments. By deploying decoys and honeytokens, FortiDeceptor automates the containment of cyberattacks before serious damage occurs.

OT Environments Are Vulnerable

As OT network environments are increasingly integrated with IT environments for external access, OT systems have become more vulnerable to the types of intrusions typically found in IT. Organizations that design and build an OT infrastructure without considering cybersecurity must implement security controls later. Some organizations may consider applying their IT-based security solutions for OT, but these solutions were not designed with OT systems in mind. Here are a few examples of the problems that can arise:

- The latest antivirus software products are often not compatible with legacy systems because of a lack of operating system support or a failure to meet the minimum hardware requirements.
- A typical firewall can detect threats within IT-based services and applications but it isn't able to decode OT communications such as OPC, BACnet, and Modbus.
- Typical intrusion detection or prevention systems protect IT-based application vulnerabilities but not OT-based vulnerabilities.
- Most external threat feeds are applicable for IT but not OT.



Deception technology is well established but often misunderstood. Some organizations believe that deception technology remains the domain of advanced security teams, but this is a fallacy. Innovative deception technology, like FortiDeceptor from Fortinet, combines the value of honeypots and honeynets with ease of use, automation, actionable intelligence, and integration with existing security controls, creating an active defense. These benefits are especially important for organizations with limited security staff and skills and those merging IT and OT.[2]

Early Threat Detection and Minimal Network Impact with FortiDeceptor

OT organizations need to adopt an assume-breach strategy with in-network detection. Fortinet FortiDeceptor is a deception solution that provides an agentless OT/IoT/IT deception layer to detect active in-network threats with no false positives. FortiDeceptor deploys in minutes with decoys that generate high-fidelity, intelligence-based alerts, resulting in an automated incident response to stop attacks early across IT and OT segments.

Unlike other security solutions that require infrastructure changes or the need to take operations offline to implement cybersecurity, FortiDeceptor is easy to use and not intrusive. To lure threat actors away from critical assets, it creates a fake environment that simulates real assets.

FortiDeceptor works by deploying and running decoys from the FortiDeceptor manager using available IP addresses. As decoys leverage unused IP addresses across the different network segments, they do not impact network availability or correspond to a real host or device on the network. To the attacker, the decoys seem like an integral part of your network.

FortiDeceptor consists of several deception components. Together, they provide an authentic and scalable layer of deception assets identical to other assets across your network. The decoys are fake assets, such as industrial control systems, medical devices, ATMs, tank gauges, point-of-sale and IoT devices, and network infrastructure that run real operating systems and services. They generate fake but limited traffic to lure attackers to them and divert them away from sensitive assets. FortiDeceptor provides an extensive inventory of decoys. You can also bring your own decoys and upload your own golden images. To expand the deception layer event further, FortiDeceptor places breadcrumbs (or tokens) on real endpoints and servers. These breadcrumbs are fake documents, files, or fake credentials, that attackers look to leverage to move laterally or encrypt.

The breadcrumbs, which are indistinguishable from real files and credentials, are designed to deceive the attacker or malware to move to the decoy laterally. When attackers engage with a decoy or use fake tokens (such as fake credentials), FortiDeceptor immediately detects this activity, generates alerts, and automatically isolates the endpoint using built-in endpoint isolation capabilities or can be integrated with security orchestration, automation, and response (SOAR) to initiate isolation.

Accelerated Incident Response

FortiDeceptor correlates every action of the threat actor into a campaign timeline with contextual intelligence of their tactics, techniques, and procedures (TTPs), which provides options to mitigate a newly discovered threat. Organizations that have a large security operations center (SOC) may prefer to use deception to engage with threat actors so the activities can be studied. Then once the investigation is complete, the necessary mitigation and response can be performed. Other organizations may prefer integrating deception into their automation framework, supporting threat response and hunting.

Because FortiDeceptor is part of the Fortinet Security Fabric, in addition to integrations with third-party solutions, it supports seamless integration with the following Fortinet products:

- **FortiGate Next-Generation Firewall** (NGFW) integration enables instant quarantine triggered by FortiDeceptor alerts of infected assets. In addition, deception decoys are visible through the network's physical and logical (decoys' network location) topology map.
- **FortiNAC** integration enables automated isolation of infected assets based on FortiDeceptor threat detection alerts.
- **FortiSOAR** integration enriches playbooks with real-time threat intelligence data and enables automated incident response triggered by FortiDeceptor alerts to help accelerate time to resolution.
- **FortiSIEM** integration facilitates effective incident response processes by feeding the security information and event management (SIEM) with high-fidelity alerts and threat intelligence data.
- **FortiAnalyzer** integration helps SOC analysts identify and respond to evidence of attack activities shared by FortiDeceptor.
- **FortiSandbox** integration provides a complete static and dynamic analysis against malicious code captured by FortiDeceptor decoys. Analysis reports are available on the FortiDeceptor admin console.
- **FortiEDR** integration enables instant isolation of infected endpoints from the network based on detecting suspicious activity by FortiDeceptor.

Extensive IT, OT, and IoT Support

FortiDeceptor offers extensive SCADA and ICS support, including Rockwell Ethernet/IP, Siemens S7, and others. It also broadly covers the IT segment of an organization by simulating Windows and Linux clients and servers. Besides the devices themselves, deception supports various applications and services, such as Git repositories, virtual private networks (VPNs), Server Message Block (SMB), Structured Query Language (SQL), and others.

Industrial facilities looking to modernize their ICS architecture also may consider the Purdue model as a systematic approach to applying security to each zone of the OT network that spans to the IT network. FortiDeceptor applies to Purdue zones, including process control, operations and control, and business and enterprise in the Purdue model.

50%

Around 50% of FortiDeceptor deployments are in OT sectors such as energy and utilities, transportation, logistics, and several manufacturing sectors, including chemical, food and beverage, automotive, aerospace, and defense.[3]

Partial List of FortiDeceptor Decoys

The following table shows a partial list of FortiDeceptor decoys. View the full list.

FortiDeceptor Supported Decoys	
OT Decoys (Note: OT decoys are only supported in SCADA v3 OS.)	
Ascent Compass MNG	HTTP, FTP, SNMP, BACnet
C-More HMI	SNMP, HTTP, HTTPS, FTP
Emerson iPro by Dixell	SNMP, MODBUS, HTTP
GE PLC 90	SNMP, HTTP, SRTP
Guardian AST	Guardian-AST/no-port
IPMI Device	HTTP, FTP, SNMP, IPMI
Kamstrup 382	KAMSTRUP
Lantronix XPORT V1.8	SNMP, HTTP, Lantronix/no-port
Lantronix XPORT V2.0	SNMP, HTTP, Lantronix/no-port
Liebert Spruce UPS	TFTP, SNMP, HTTP
MOXA NPORT 5110	SNMP, TELNET, HTTP, MOXA
Modicon M241	TFTP, SNMP, MODBUS, ENIP, HTTP
Modicon M580	TFTP, SNMP, MODBUS, ENIP, HTTP
Niagara4 Station	SNMP, HTTP, BACnet
NiagaraAX Station	SNMP, HTTP, BACnet
Phoenix contact AXC 1050	HTTP, SNMP, PROFINET, FTP
PowerLogic ION7650	SNMP, MODBUS, DNP3, HTTP
Rockwell 1769-L16ER/B LOGIX5316ER	SNMP, ENIP, HTTP
Rockwell 1769-L35E Ethernet Port	SNMP, ENIP, HTTP
Rockwell PLC	HTTP, TFTP, SNMP, ENIP
SIEMENS S7-1500 PLC	HTTP, TFTP, SNMP, S7COMM, IEC104, PROFINET
Schneider EcoStruxure BMS server	SNMP, BACnet, HTTP, TRICONEX
Schneider Power Meter - PM5560	SNMP, BACnet, ENIP, HTTP, DNP3
Schneider SCADAPack 333E	SNMP, DNP3, TELNET

FortiDeceptor Supported Decoys (continued)	
Siemens S7-200 PLC	HTTP, TFTP, SNMP, MODBUS, S7COMM
Siemens S7-300 PLC	TFTP, SNMP, IEC104
VAV-DD BACnet controller	SNMP, BACnet
IOT Decoys	
Printers	
HP Printer	SNMP, HTTP, Jetdirect
Brother MFC Printer	SNMP, HTTP, Jetdirect
Lexmark Printer	SNMP, HTTP, Jetdirect
IP Camera	
Hikvision IP camera	SNMP, HTTP, RTSP, UPnP
Network Devices	
Cisco Router	TELNET, HTTP, SNMP, CDP 4 Cisco images (models) are supported: 2691, 3660, 3725 and 3745
NetGear MR60 Router	HTTP, SNMP, UPnP
TP-LINK Router	CWMP, HTTP, TP-LINK WEB
Switch	SNMP, TELNET, CDP, HTTP
MikroTik Router	SNMP, TELNET, CDP, HTTP
Medical Decoys	
PACS	TELNET, FTP, PACS, PACS-WEB, DICOM Server
SPACECOM	HTTP, HTTPS, FTP, CANBus, SSH
INFUSOMAT	HTTP, HTTPS, CanBus, B.BRAUN
Bank Decoys	
SWIFT VPN Gateway	TELNET, HTTPS
App Decoys	
ERP	ERP-WEB,HTTP
SAP	SAP Router, SAP Dispatcher, HTTP
Elastic Search	(Elastic Search) ScadaBR Decoy (ScadaBR-HTTP)
Tomcat	HTTP, HTTPS, SSH
MySql MariaDB	SSH, MariaDB
VOIP: SIP	SIP/TCP, UDP
XMPP	XMPP/HTTP
MQTT	MQTT/HTTP, CoAP
4G/5G 3GPP	NextEPC/HTTP, SCTP&GTP-C, GTP-U
EV-CPO	HTTP, HTTPS
TrueNAS	SSH, HTTP, HTTPS, SAMBA, SNMP
IT Decoys	
Windows 7 / 10 / 11	RDP, SMB, SMTP, TCP, NBNS, ICMP, FTP, SWIFT
SSL-VPN	SSLVPN, HTTPS
FortiGate	SSLVPN, HTTPS

Early Detection and Isolation of Sophisticated Human and Automated Attacks

Incorporating the early detection and response characteristics as a proactive defense strategy elevates an organization's existing security posture and reduces business disruption from external or internal threats.

Deploying security in an OT environment is complex, but FortiDeceptor is non-intrusive and does not add delay to OT operations before, during, and after its deployment. FortiDeceptor isn't just for OT environments. It also works for IT so that security operations staff can close gaps with comprehensive coverage of the dynamic attack surface.

FortiDeceptor can easily integrate with Fortinet and third-party security solutions to enable automated threat response and contextual threat hunting, improving efficiencies within SOC processes.

[1] Fortinet 2024 State of OT and Cybersecurity Report.

[2] Jon Oltsik, Distinguished Analyst and Fellow, Active Defense and Deception Technology: The Time is Now!, June 2023.

[3] Fortinet customer data.

October 2, 2024 4:25 PM / 988459-B-0-EN