WHITE PAPER

HPE IT OT Convergence Security Solution With Fortinet

Table of Contents

Background

Internet-of-Things (IoT) environments are extremely complex. There are many different types of devices and sensors, different vendors, different software, and different operating systems. Securing this complex environment can be challenging because there are different protocols that need to be secured, and each of these entities and protocols can have different behaviors.

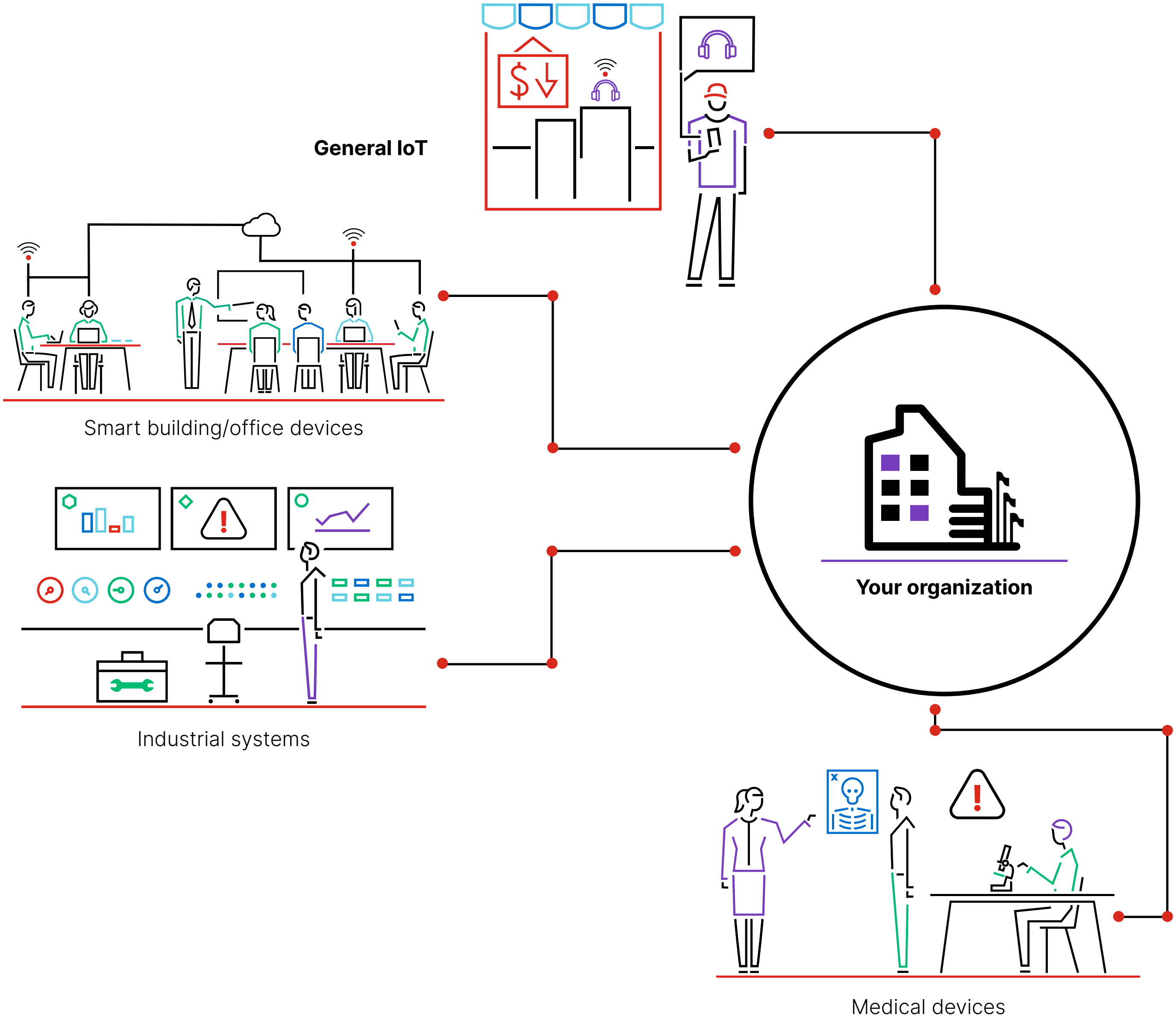


Figure 1: A complex IoT landscape.

A lot of IoT devices out there are unmanaged. They have been running on closed networks for many years without being touched, which makes these devices inherently vulnerable to attack—this is primarily the case in enterprise IoT and operational technology (OT) environments. Many are running old and/or outdated operating systems that the customer is fearful of patching in case the system stops working—so they leave them alone.

What we also see is that many devices have not been built with security in mind. For example, they may have hard-coded passwords, which can be easily guessed. They often also have backdoors for administrative access and lack a consistent and controlled configuration approach. This is challenging from a security point of view.

The Purdue model (Figure 2) is an industry-adopted conceptual model for industrial control system (ICS) network segmentation. From a security perspective, an IoT solution such as the HPE OT Link software would typically be deployed in what is known as the operational DMZ; this is Level 3.5 in the Purdue model. It is the traditional zone in which systems live that provide a bridge between the OT and IT worlds. These interfaces are one area that we will address in this technical white paper.

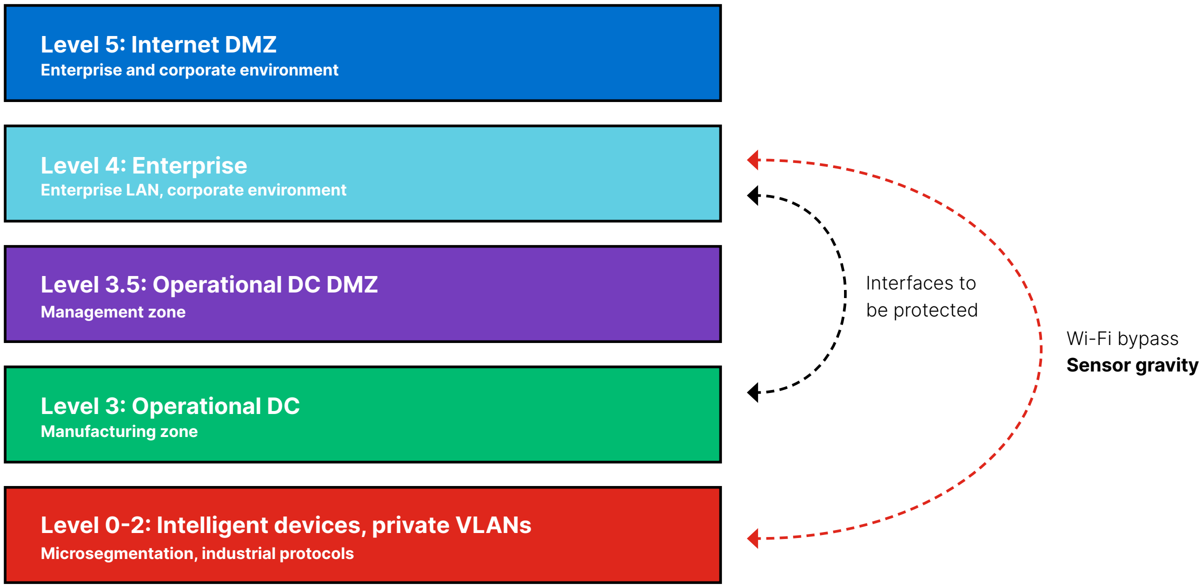

Level 5: Internet DMZ
Enterprise and corporate environment
Level 4: Enterprise
Enterprise LAN, corporate environment
Level 3.5: Operational DC DMZ
Management zone
Level 3: Operational DC
Manufacturing zone
Level 0-2: Intelligent devices, private VLANs
Microsegmentation, industrial protocols
Interfaces to be protected
Wi-Fi bypass
Sensor gravity

Figure 2: Simplified Purdue model.

The other area is where modern sensors and IoT devices are increasingly more capable due to advances in technology. As a result, many devices are Wi-Fi connectable, backed up by cloud services, and are often deployed with a direct connection to the enterprise networks without thinking about the security implications of doing so. This is typically because the enterprise has no other Wi-Fi network to connect, and rather than setting up new infrastructure, they simply connect the devices to the enterprise Wi-Fi. This phenomenon is called **sensor gravity**, and it is an area of growing concern in the IoT security space. It is illustrated in Figure 2 as Wi-Fi bypass, and as you can see, it creates a direct bridge that bypasses the operational DMZ.

To aid in the understanding of the solution components, we will primarily focus on the wired scenario where devices are hardwired to the network. We will also highlight where alternate products can be used to prevent bypassing of the security controls through Wi-Fi.

The need to connect these two environments (IT and OT) is becoming a requirement because businesses are looking for intelligence sharing and cost optimization (cross-leveraging hardware and systems). Therefore, we need to address how to remove the historic air gap while maintaining an air gap level of security and control between the two areas.

Problem statement

Figure 3 shows a simplified view of an IoT solution that bridges the OT and IT networks. On the left, we have the OT network where all the programmable logic controllers (PLCs) reside and are connected to the sensors and actuators. On the right is the enterprise IT network. The IoT solution is deployed on an edge compute device that could be running HPE OT Link, PTC Kepware, or other solutions such as Azure IoT. Anyway, the solution is communicating with the OT network to read or write to the PLCs and send data to or receive commands from either a local on-premises or a cloud solution.

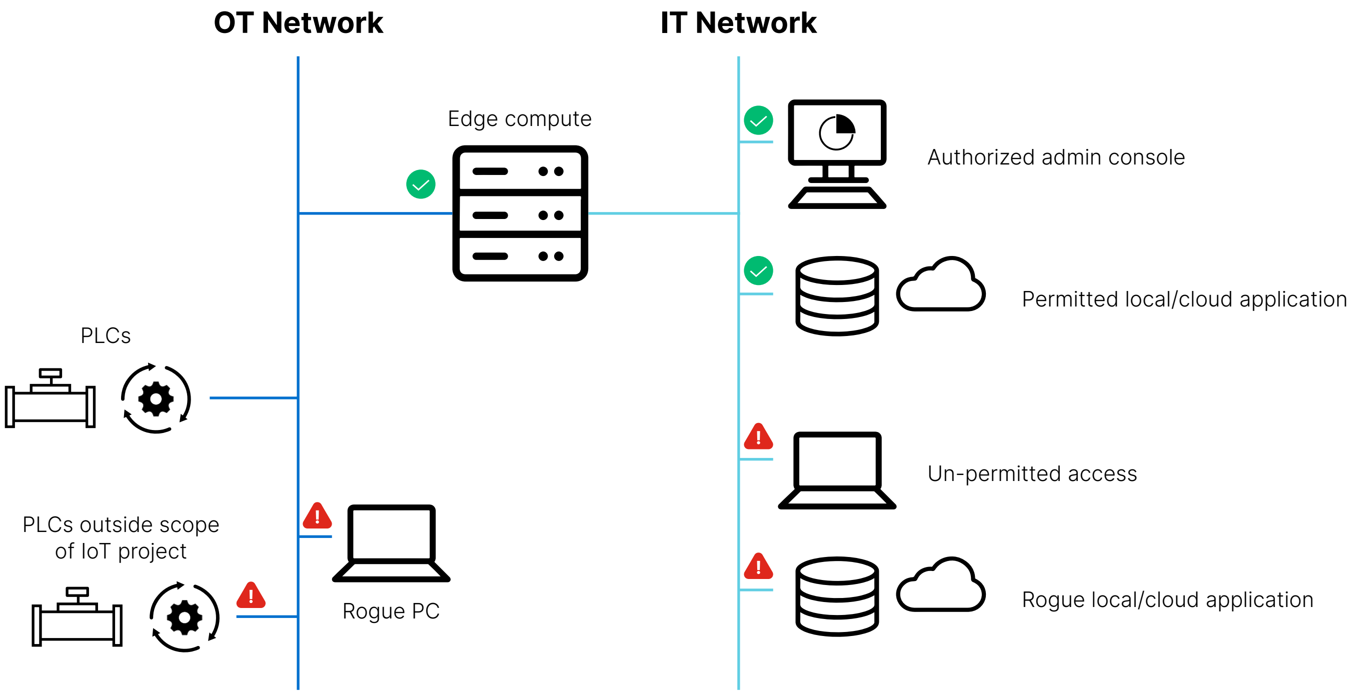

OT Network
IT Network
Edge compute
Authorized admin console
Permitted local/cloud application
PLCs
Un-permitted access
PLCs outside scope of IoT project
Rogue PC
Rogue local/cloud application

Figure 3: The problem.

Why do we need to protect such an environment?

One of the issues we face today is that many, if not all, IoT solution enablers (HPE OT Link, PTC Kepware, and others) do not permit access to the OT-side protocols before data is extracted and put into their datastores and workflows. This means that we cannot build the security layer within the application stack. The only place that we can reliably perform these security activities is outside of the IoT solution; this is on the network between the edge compute device and the OT and IT networks.

Traditional enterprise IT firewalls will not be able to protect the networks in this scenario, as they are not physically deployed in these locations. They are typically somewhere else on the network, for example, protecting internet access or segregating various segments of the enterprise network. Also, note that we need to achieve this without causing the customer to redesign their OT network routing. (Most OT networks are flat Layer 2 networks with no routing configured at all.)

We will now consider a set of protection scenarios.

Scenario A: PLC is controlling a pump valve and the customer must ensure that the IoT solution cannot instruct the valve to open or close for safety reasons. The IoT solution is only permitted to read the current status.

To protect the pump, the IoT solution could implement specific coding to ensure that only read actions are allowed. However, we cannot rely on that to protect the PLCs, as code can easily be changed. Also, we must ensure that no upstream system could inject a badly formatted message that would simply flow down to the pump and enact change. In other words, we must intercept all traffic between the IoT solution and the pump to ensure that only read requests are sent to the PLC.

Scenario B: A computer on the IT network gains access to the edge computer, enabling the user to modify the IoT solution.

If a remote computer on the IT network can get administrative access to the IoT solution, it could be modified to collect sensitive data from the PLCs or send the collected data to a rogue cloud or local application. If you think this could never be an issue, then take a look at the following article that illustrates how quickly OT networks can be breached and filled with malware: Ransomware: Hackers took just three days to find this fake industrial network and fill it with malware.

Scenario C: Protect production OT assets during proof of concept (POC) or pilot IoT project.

In this scenario, there is a requirement to only allow the IoT project access to a limited set of PLCs. We can use the firewall on the OT side to restrict access from the IoT solution to just the permitted set of PLCs and deny all other access.

Securing the IT OT Boundary With HPE Edgeline and Fortinet

HPE and Fortinet can secure the IoT scenarios we described previously by using Fortinet's ruggedized FortiGate. The FortiGate Rugged Series offers an industrially hardened, all-in-one security appliance that delivers specialized threat protection for securing critical industrial and control networks against malicious attacks. Combined with FortiGuard Industrial Security Services, the FortiGate can utilize application signatures to identify and police most of the common OT protocols for granular visibility and control. This means that if there is a FortiGate next-generation firewall (NGFW) positioned in-line with the edge computing environment hosting the IoT solution, attempted exploits and breaches can be mitigated, prevented, and reported. Conventional firewalls that only identify ports, protocols, and IP addresses cannot identify and control applications, but a Fortinet NGFW can. FortiGate NGFWs offer extensive visibility into application usage in real time, as well as trends over time through views, visualizations, and reports. You can use application control to keep malicious, risky, and unwanted applications out of your network or control what specific registers an industrial operator is reading or writing.

The FortiGate firewalls are hardware accelerated by Fortinet's custom application-specific integrated circuits (ASICs.) The F model FortiGates are now powered by a new fourth generation system-on-a-chip technology. What this means is that instead of processing traffic and firewall duties such as legacy firewalls do, the FortiGates use hardware for processing and inspecting.

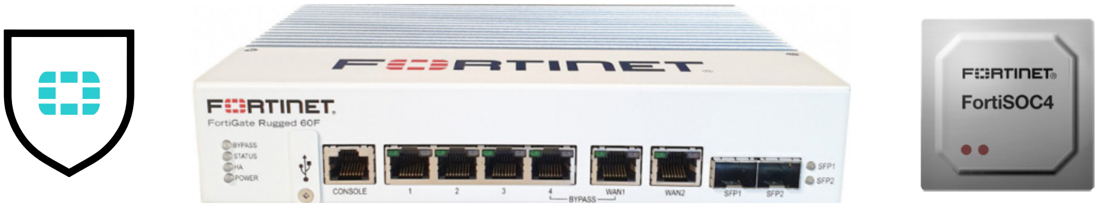


Figure 4: Fortinet FortiGate Rugged 60F.

Firewall placement

Figure 5 is the same diagram as before, but here we have overlaid it with the Fortinet firewalls protecting the networks in an integrated approach to IoT security. Note that although you can see multiple **virtual** firewalls, there is only a single physical firewall protecting both sides and connected to different network segments.

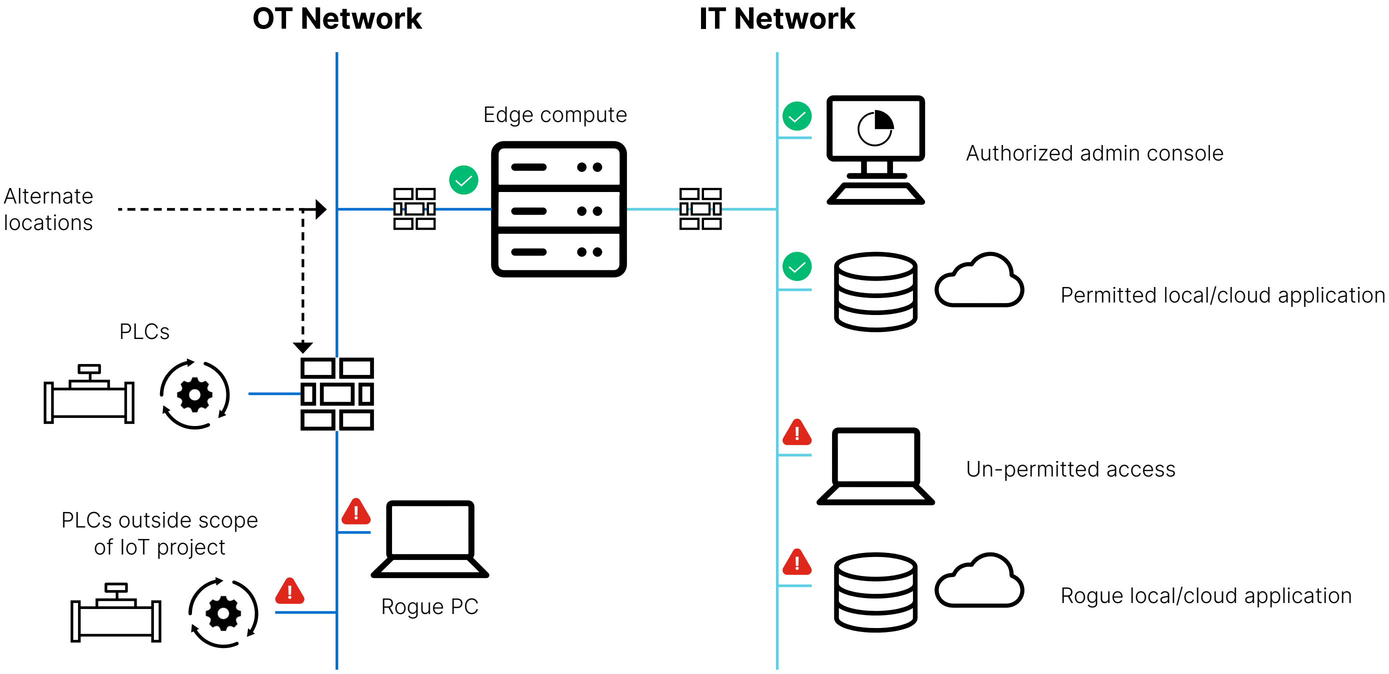


Figure 5: The solution.

On the IT network side, the choice is simple—the firewall is simply in-line between the edge compute device and the IT network, thereby protecting all traffic to or from the IoT solution and coming from and going to the IT side.

On the OT network side, we have different options on where to place the firewall.

- If connected in-line with the OT network connection for the IoT solution, then it can only protect the OT network connection of the edge compute device, and it will not intercept unauthorized OT network access from other devices on the OT network.
- If it can be placed prior to the network switch connecting all the devices on the OT network, then the firewall is not only able to intercept traffic from the IoT solution but also protect the entire OT network. In fact, it may not be necessary to protect the complete OT network during the startup of a project, but placing the firewall in the right place from the start will keep you from having to move it later as the solution scales out.

Let's take a closer look at the setup now and how we can use one device to achieve the previously mentioned using the ruggedized FortiGate NGFW as shown in Figure 6.

On the IT side, the FortiGate is provisioned with an IP address from the enterprise network. It provides the route through which all access is controlled to and from the IoT solution to the enterprise network. The FortiGate is then configured to provide a private IP address to the edge compute system. This allows strict security policies to be applied between these two connections to control exactly who and how other systems can get access and where the IoT solution is permitted to make outbound connections (for example, to upload data to a specific Azure cloud solution).

On the OT side, things are a bit different. As mentioned earlier, one of the requirements is that we can ensure you do not have to reconfigure the OT networks. To achieve this, we take advantage of a feature within FortiGate known as a **virtual wire pair** or **virtual wire**.

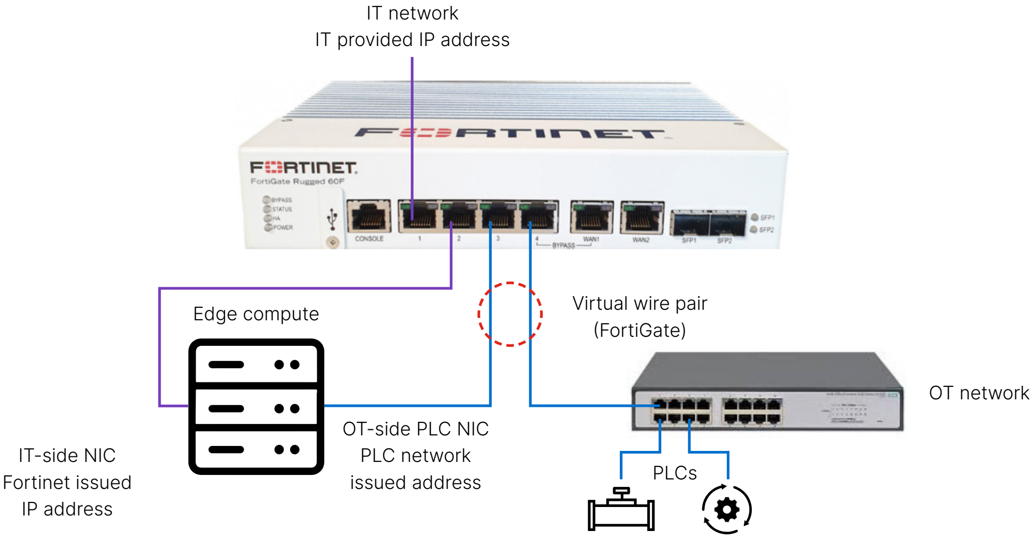


Figure 6: FortiGate physical connectivity.

The FortiGate virtual wire feature is ideal for environments that require a consolidated security infrastructure, including controls for in-line intrusion prevention system, application control, deep packet inspection, and network antivirus protection, without added infrastructure complexity. The FortiGate acts as a bump in the wire that can police, identify, and protect traffic flowing through the network. A FortiGate that uses virtual wire enables us to add security controls without purchasing additional hardware. The FortiGate virtual wire can be inserted anywhere in the network and start protecting critical segments from exploits and breaches immediately. With FortiGate virtual wire, we can inspect OT- and IT-specific protocols and applications to better protect the infrastructure against vulnerabilities and threats.

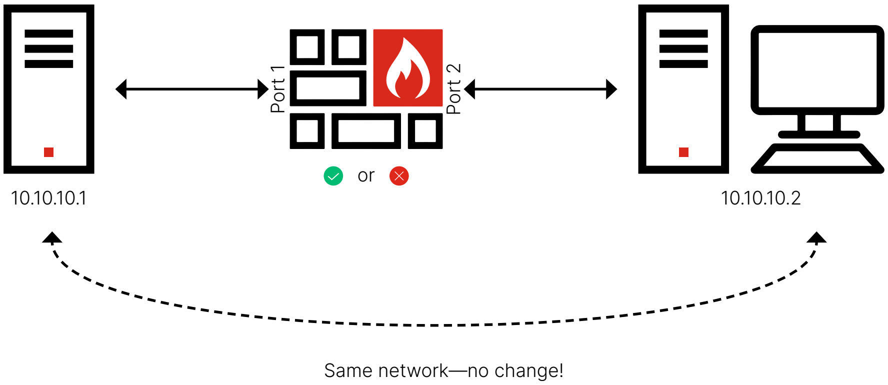


Figure 7: FortiGate virtual wire pair.

Once the firewall is physically deployed, the protection of the OT and IT networks is achieved using the FortiGate **application control** feature.

The application control feature provides real-time visibility into the applications that are running on the OT or IT network. Powered by FortiGuard Labs, an industry-leading vulnerability research organization, the application control technology combines application intelligence with intrusion prevention services to provide high levels of next-generation firewall and next-generation intrusion prevention security effectiveness. FortiGuard security services are designed to optimize performance and maximize the protection across the entire Fortinet Security Fabric and are available as both individual and bundled subscriptions. They cover every aspect of the attack surface from industrial to enterprise networks. With FortiGuard security services, you can quickly and seamlessly create policies to allow, deny, or restrict access to industrial applications or entire categories of applications.

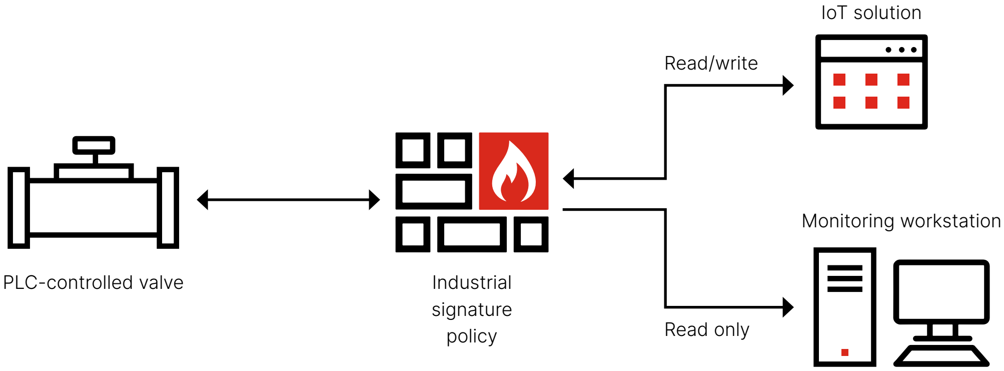
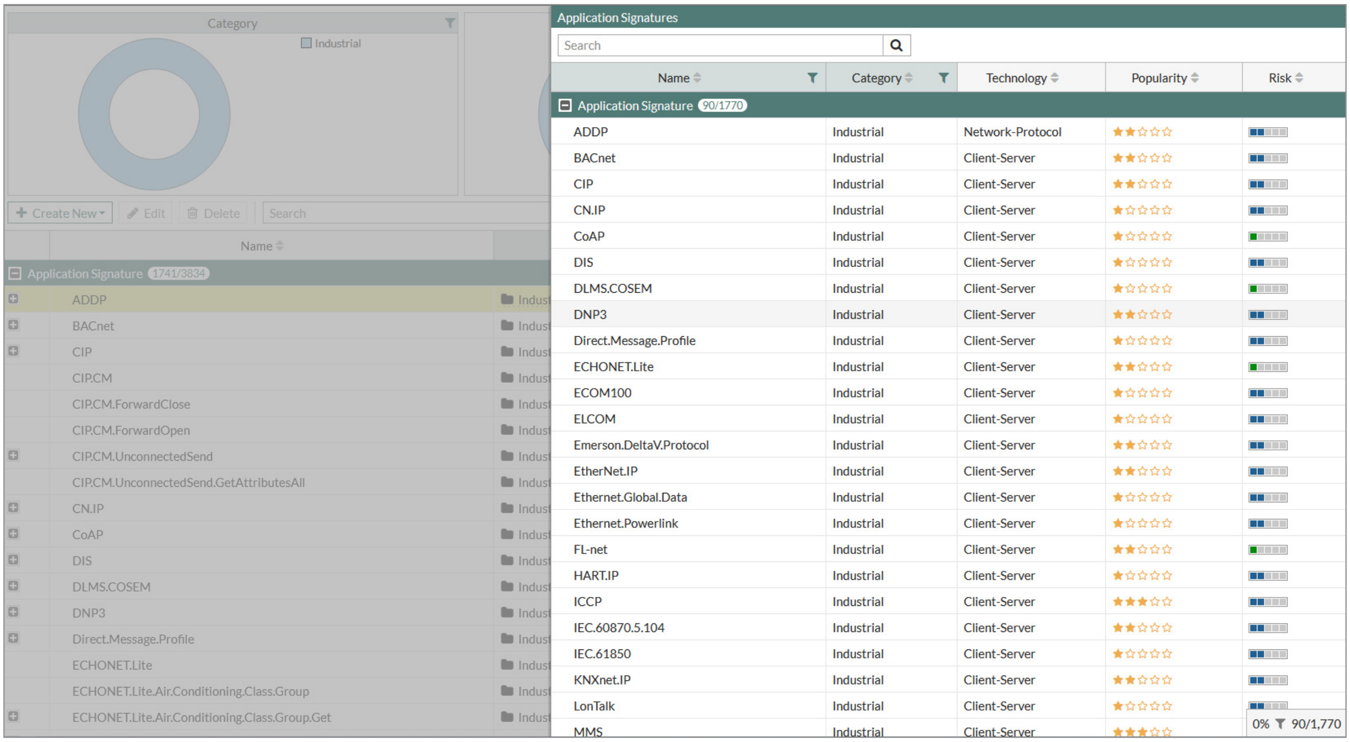


Figure 8: FortiGuard application control.

Why OT needs application control?

The operating conditions of an OT environment require an OT-specific approach to threat detection and response. Traditional antivirus solutions are not a good fit because they require frequent signature updates, large quantities of memory, and the ability to terminate potentially malicious processes—all of which are infeasible in OT environments since these can all impact OT device availability and message latency. Protecting OT systems requires deploying security controls at the network level. A FortiGate NGFW provides the necessary level of protection by monitoring and filtering all traffic entering and exiting an ICS. The differences between IT and OT environments also implicate that ICS often face different threats and require security monitoring controls that are tailored to their unique threat landscape.

Fortinet's more than 15 years of experience securing OT environments and membership of the largest OT-specific partner ecosystem give it a deep understanding of the OT-specific threats. This enables FortiGuard Labs to develop OT-specific threat intelligence based on the analysis of over 100 billion security alerts per day. The application control engine can identify 48 different OT-specific network protocols, such as Modbus, BACnet, and OPC Classic, with over 1,500 different signatures. Combining these capabilities with the OT-specific threat intelligence provided by FortiGuard Labs enables OT operators to identify and monitor the different types of traffic flowing over their networks and apply extremely granular security controls to restrict the data flows within their environments.



Name	Category
Application Signature 1741/8834	
ADDP	Indust
BACnet	Indust
CIP	Indust
CIP.CM	Indust
CIP.CM.ForwardClose	Indust
CIP.CM.ForwardOpen	Indust
CIP.CM.UnconnectedSend	Indust
CIP.CM.UnconnectedSend.GetAttributesAll	Indust
CN.IP	Indust
CoAP	Indust
DIS	Indust
DLMS.COSEM	Indust
DNP3	Indust
Direct.Message.Profile	Indust
ECHONET.Lite	Indust
ECHONET.Lite.Air.Conditioning.Class.Group	Indust
ECHONET.Lite.Air.Conditioning.Class.Group.Get	Indust

Application Signatures

Name	Category	Technology	Popularity	Risk
Application Signature 90/1770				
ADDP	Industrial	Network-Protocol	★★☆☆☆	🟦🟦⬜⬜⬜
BACnet	Industrial	Client-Server	★★☆☆☆	🟦🟦⬜⬜⬜
CIP	Industrial	Client-Server	★★☆☆☆	🟦🟦⬜⬜⬜
CN.IP	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
CoAP	Industrial	Client-Server	★☆☆☆☆	🟩⬜⬜⬜⬜
DIS	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
DLMS.COSEM	Industrial	Client-Server	★☆☆☆☆	🟩⬜⬜⬜⬜
DNP3	Industrial	Client-Server	★★☆☆☆	🟦🟦⬜⬜⬜
Direct.Message.Profile	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
ECHONET.Lite	Industrial	Client-Server	★★☆☆☆	🟩⬜⬜⬜⬜
ECOM100	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
ELCOM	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
Emerson.DeltaV.Protocol	Industrial	Client-Server	★★☆☆☆	🟦🟦⬜⬜⬜
EtherNet.IP	Industrial	Client-Server	★★☆☆☆	🟦🟦⬜⬜⬜
Ethernet.Global.Data	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
Ethernet.Powerlink	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
FL-net	Industrial	Client-Server	★★☆☆☆	🟩⬜⬜⬜⬜
HART.IP	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
ICCP	Industrial	Client-Server	★★★☆☆	🟦🟦⬜⬜⬜
IEC.60870.5.104	Industrial	Client-Server	★★☆☆☆	🟦🟦⬜⬜⬜
IEC.61850	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
KNXnet.IP	Industrial	Client-Server	★★☆☆☆	🟦🟦⬜⬜⬜
LonTalk	Industrial	Client-Server	★☆☆☆☆	🟦🟦⬜⬜⬜
MMS	Industrial	Client-Server	★★★☆☆	

0% 90/1,770

Figure 9: Built-in FortiGuard application control signatures.

Adding custom signatures

Besides an extensive list of preconfigured application signatures, Fortinet also allows you to add custom application signatures in case your deployment uses a different protocol. After a Wireshark trace has been captured of the traffic, the new signature can be created using the lightweight definition language that is used by the Fortinet intrusion prevention system (IPS) engine.

The latest information on creating and applying custom signatures can be found in the Fortinet Document Library at docs.fortinet.com.

Support for Wireless Services

Protecting against sensor gravity

Earlier we mentioned the concept of sensor gravity whereby Wi-Fi-enabled sensors can bypass the security layers by being connected directly to the customer's enterprise network. In many cases, it may not be appropriate or cost-effective to deploy a completely new Wi-Fi IoT network just for a few devices.

The FortiWiFi series of firewalls mentioned previously have the ability to switch the Wi-Fi configuration of a Wi-Fi client to that of an access point (AP). (AP is the default out-of-the-box configuration.) This allows FortiWiFi to present a Wi-Fi service set identifier (SSID) to the IoT devices, thereby allowing the required security policies to be implemented. The simplest solution utilizes the FortiGate itself to provide the Wi-Fi network for the OT sensors. This is shown in Figure 10.

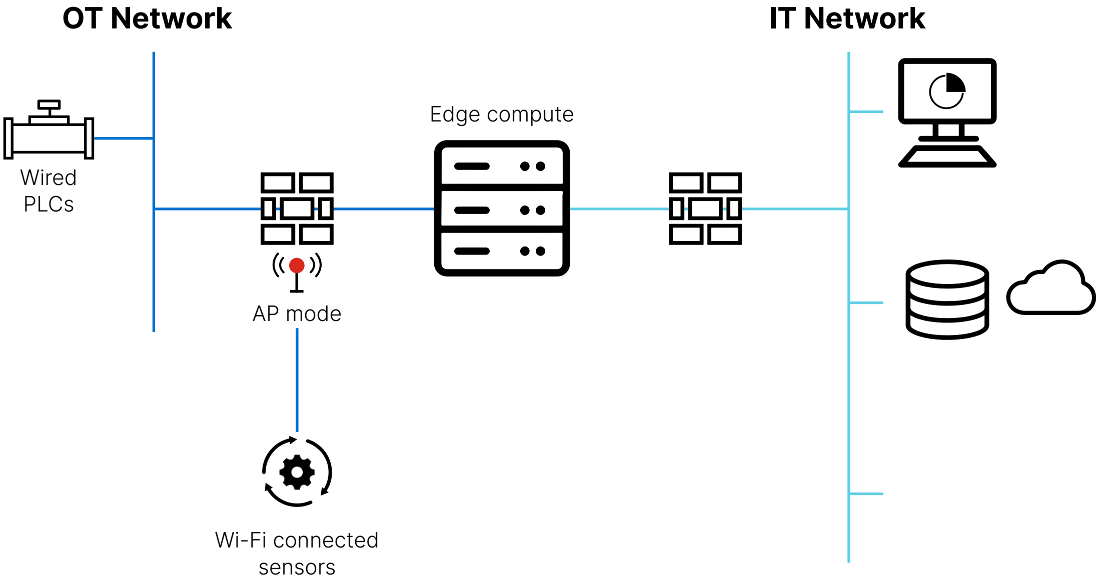


Figure 10: FortiGate in AP mode.

However, in large-scale deployments, you can deploy multiple Wi-Fi APs, from any vendor, and isolate that network back to the FortiGate for inspection. This is shown in Figure 11.

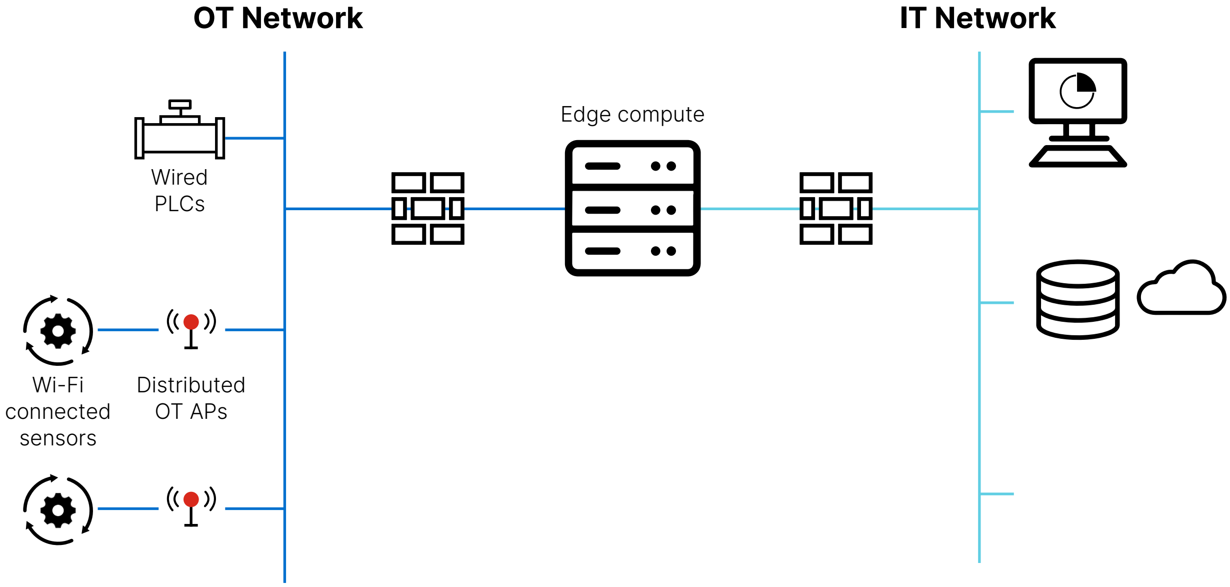


Figure 11: Distributed OT network APs.

Wi-Fi or LTE uplink

The FortiGate can easily be inserted into a wired industrial environment for transparent protection and inspection alongside HPE Edgeline products. However, what if there was a requirement to protect an industrial network without a hard-wired uplink and still protect industrial traffic? To help in this scenario, Fortinet has variants of scalable ruggedized and nonruggedized FortiGates that include a built-in Wi-Fi radio or Long-Term Evolution (LTE) connectivity. The FortiWiFi solution, for example, can be connected to an existing wireless network and provides secure connectivity to downstream equipment as needed.

Since FortiGates are built for all-in-one networking, in this scenario, there would be enough FortiGate physical interfaces to also support a virtual wire, as well as an outbound connection for the HPE Edgeline connectivity. The FortiGate can take your security a step further by carving out and isolating virtual contexts to completely air gap and isolate networks, all from a single appliance. In addition, LTE FortiGates are built to leverage mobile carriers for out-of-band management or implement redundant external connections.

This type of flexibility, integration, and support for industrial networks alongside HPE Edgeline products is unique as the products are purpose-built for security and optimization in industrial environments. Once Fortinet protection is integrated into an environment, it can provide the situational awareness for actionable intelligence across the entire attack surface.

Figure 12: Wi-Fi and LTE FortiGate models.

NOTE: FortiWiFi can only operate in either Wi-Fi AP or client mode. If both a Wi-Fi uplink and OT-side AP are required, then an alternative configuration would be needed requiring additional hardware, for example, as shown in Figure 11 or 13.

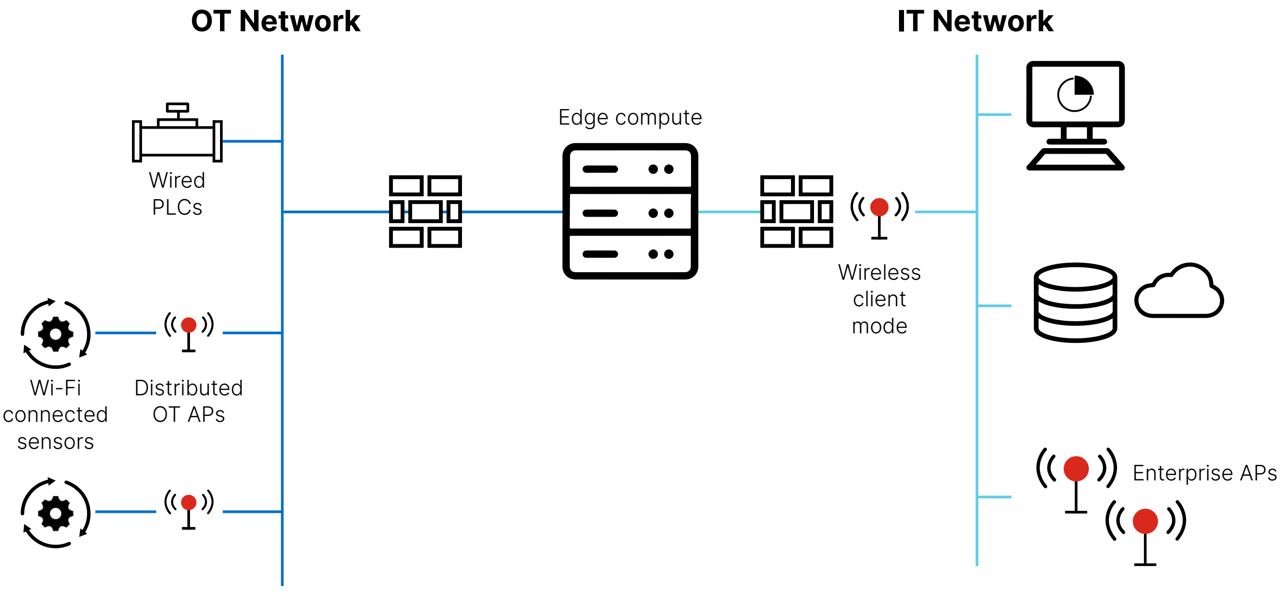


Figure 13: Combined OT-side APs and wireless uplinks.

Scale Up or Scale Out When It Comes to Security

The initial solution set and scenarios described here are targeted at HPE Fast Start and other early-adoption IoT projects where you may be connecting a single edge compute device to a targeted set of sensors, for example, as in our HPE Fast Start Condition Monitoring Solution. But what happens when you want to scale the solution to include more devices, more locations, more IoT solutions? Can we still apply this security offering? The answer is yes. Whether or not additional firewalls, HPE Edgeline, and other devices are required will depend on the physical location of the additional systems and scale of the IoT solution.

However, we would strongly recommend that the solution is not grown incrementally with devices and firewalls added at different stages without proper consideration of the overall security architecture. As more elements are added to the solution, there will be a need for additional security and management capabilities, for example, single-pane-of-glass management tools or extra access control solutions to provide two-factor authentication. These will add more complexity, and of course, more opportunities for attack.

To support you in this, HPE Security Practice has developed IoT-specific security reference architectures. These are frameworks that allow us to demonstrate that we have a holistic and methodological approach to securing IT environments. In order to structure these reference architectures, we use HPE Global Method for IT Solution Architecture (GM ITSA). When we look at the security of a certain target environment, we always look at it from the four ITSA viewpoints—business, technical, functional, and implementation view—as illustrated in Figure 14, which shows screenshots of the security practice's enterprise IoT security solution reference architecture. As you move forward from your initial project toward a full production environment, security architecture becomes more and more important as the number of devices, gateways, and services that are interconnected will continue to grow.

The security solution outlined in this white paper is a first step in securing the OT networks and needs to be implemented for every POC or HPE Fast Start early engagement. We need to ensure that what we are doing is secure right from the start, and as the solution grows beyond this, it can be scaled up and out in-line with our IoT security reference architecture.

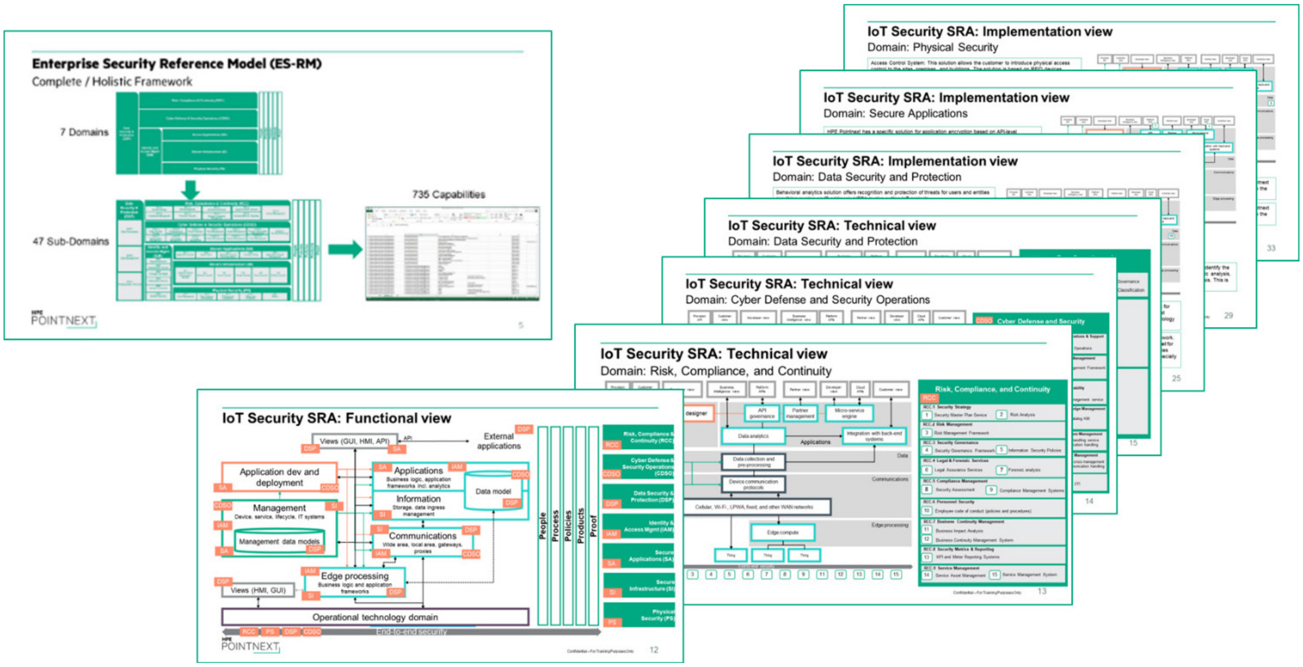

Enterprise Security Reference Model (ES-RM)
Complete / Holistic Framework
7 Domains
47 Sub-Domains
735 Capabilities
POINTNEXT
IoT Security SRA: Implementation view
Domain: Physical Security
IoT Security SRA: Implementation view
Domain: Secure Applications
IoT Security SRA: Implementation view
Domain: Data Security and Protection
IoT Security SRA: Technical view
Domain: Data Security and Protection
IoT Security SRA: Technical view
Domain: Cyber Defense and Security Operations
Cyber Defense and Security
IoT Security SRA: Technical view
Domain: Risk, Compliance, and Continuity
Risk, Compliance, and Continuity
IoT Security SRA: Functional view
Views (GUI, HMI, API)
External applications
Application dev and deployment
Applications
Management
Device, service, lifecycle, IT systems
Information
Data model
Management data models
Communications
Edge processing
Views (HMI, GUI)
Operational technology domain
End-to-end security
People
Process
Policies
Products
Proof
POINTNEXT

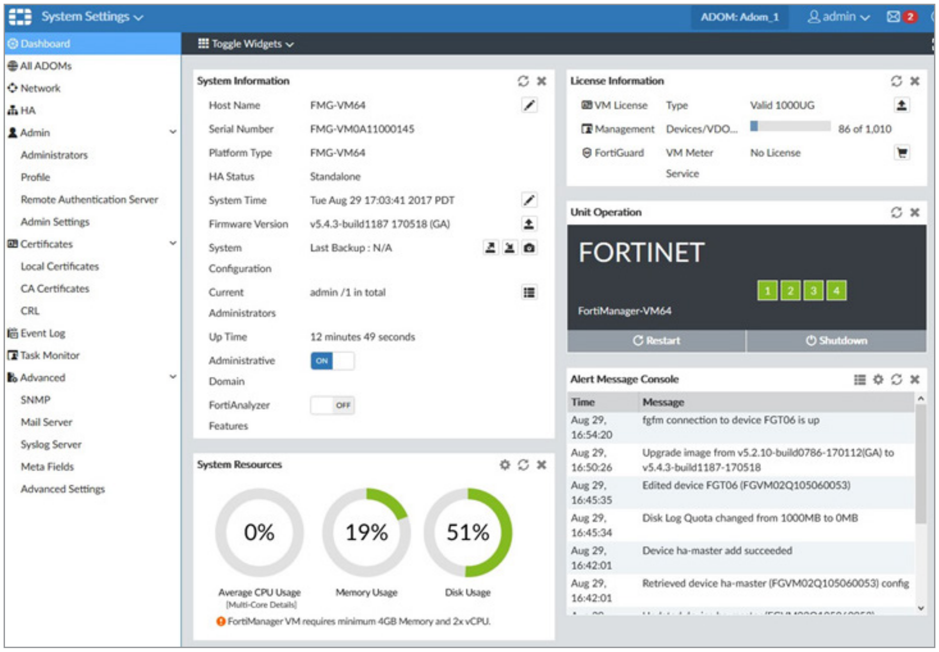
Figure 14: HPE Security CoE reference architectures.

Fortinet solution growth

As the number of FortiGate products grows within the solution, at one point in time, it will be necessary to consolidate the management and reporting capabilities. To help with this, the following Fortinet products are recommended to provide a single pane of glass for management and reporting views.

- **FortiManager**

  A key part of the Fortinet Security Fabric, FortiManager supports network operations use cases for centralized management, best practices compliance, and workflow automation to provide better protection against breaches.



System Information

Host Name	FMG-VM64
Serial Number	FMG-VM0A11000145
Platform Type	FMG-VM64
HA Status	Standalone
System Time	Tue Aug 29 17:03:41 2017 PDT
Firmware Version	v5.4.3-build1187 170518 (GA)
System Configuration	Last Backup : N/A
Current Administrators	admin /1 in total
Up Time	12 minutes 49 seconds
Administrative Domain	ON
FortiAnalyzer Features	OFF

License Information

VM License	Type	Valid 1000UG	
Management	Devices/VDO...		86 of 1,010
FortiGuard	VM Meter Service	No License	

Unit Operation

FortiManager-VM64

System Resources

FortiManager VM requires minimum 4GB Memory and 2x vCPU.

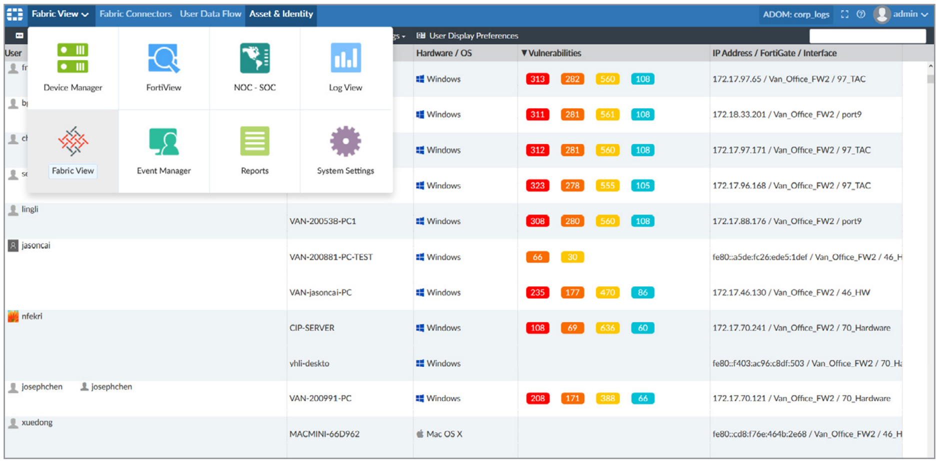
Alert Message Console

Time	Message
Aug 29, 16:54:20	fgfm connection to device FGT06 is up
Aug 29, 16:50:26	Upgrade image from v5.2.10-build0786-170112(GA) to v5.4.3-build1187-170518
Aug 29, 16:45:35	Edited device FGT06 (FGVM02Q105060053)
Aug 29, 16:45:34	Disk Log Quota changed from 1000MB to 0MB
Aug 29, 16:42:01	Device ha-master add succeeded
Aug 29, 16:42:01	Retrieved device ha-master (FGVM02Q105060053) config

Figure 15: FortiManager—centralized management.

- **FortiAnalyzer**

  An integrated security architecture with analytics-powered security and log management capabilities can address the lack of visibility. As part of the Fortinet Security Fabric, FortiAnalyzer supports analytics-powered use cases to provide better detection against breaches.



User		Hardware / OS	▼Vulnerabilities	IP Address / FortiGate / Interface
fr		Windows	313 282 560 108	172.17.97.65 / Van_Office_FW2 / 97_TAC
bj		Windows	311 281 561 108	172.18.33.201 / Van_Office_FW2 / port9
ch		Windows	312 281 560 108	172.17.97.171 / Van_Office_FW2 / 97_TAC
se		Windows	323 278 555 105	172.17.96.168 / Van_Office_FW2 / 97_TAC
lingli	VAN-200538-PC1	Windows	308 280 560 108	172.17.88.176 / Van_Office_FW2 / port9
jasoncai	VAN-200881-PC-TEST	Windows	66 30	fe80::a5de:fc26:ede5:1def / Van_Office_FW2 / 46_H
	VAN-jasoncai-PC	Windows	235 177 470 86	172.17.46.130 / Van_Office_FW2 / 46_HW
nfekri	CIP-SERVER	Windows	108 69 636 60	172.17.70.241 / Van_Office_FW2 / 70_Hardware
	yhli-deskto	Windows		fe80::f403:ac96:c8df:503 / Van_Office_FW2 / 70_H
josephchen josephchen	VAN-200991-PC	Windows	208 171 388 66	172.17.70.121 / Van_Office_FW2 / 70_Hardware
xuedong	MACMINI-66D962	Mac OS X		fe80::cd8:f76e:464b:2e68 / Van_Office_FW2 / 46_H

Figure 16: FortiAnalyzer—analytics-driven security management.

Learn more at:

hpe.com/pointnext

FORTINET®

www.fortinet.com

May 27, 2021 4:27 AM

1048851-0-0-EN