SOLUTION BRIEF

Fortinet and Ordr for Federal Healthcare Agencies

Industry-leading Security Across Network-connected Devices

Government healthcare agencies collect and maintain a massive amount of citizen data to effectively deliver services to their patients. Strict guidelines not only mandate security controls for the vast array of different data types that agencies collect, share, and maintain, but also for the devices that collect, transmit, and store this data. While regulatory compliance standards like Federal Information Security Modernization Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI-DSS) impose fines for unprotected data, most government healthcare agencies take a proactive approach to compliance. Proactive compliance means maintaining a continuous and accurate asset inventory, understanding device behavior and risk, and properly segmenting their network to prevent potential loss of data.

The number of devices connected to healthcare networks, from conference TVs to business-critical infrastructure, has grown exponentially. Unfortunately, this brings with it a significant increase in the attack surface since these devices often run legacy software without security agents. Without the means to be patched or to protect themselves against attack, these devices are extremely vulnerable and therefore lucrative targets. Government healthcare agencies need to secure access to and from these devices to protect against direct attacks, lateral movement, and business interruption. This requires complete awareness of all devices, their risks, and their ongoing behavior, and then translating this knowledge into proper and automated network segmentation workflows.

Fortinet and Ordr have partnered to deliver a network security solution by integrating the FortiGate next-generation firewall (NGFW), FortiManager automation-driven network management, and the Ordr Systems Control Engine (SCE). The solution provides organizations with complete visibility of their network-connected devices, baselining of safe device behavior, and the ability to protect critical information technology (IT), Internet of Things (IoT), operational technology (OT), and unmanaged devices with automated segmentation at the firewall. Combining the solution with the Fortinet FortiNAC creates a comprehensive solution to secure both network access and local area network (LAN) communications, as well as all communications between security zones using a FortiGate NGFW.

Joint Solution

Ordr and Fortinet have partnered to deliver an industry-leading security solution to address the challenge of widespread, unmanaged, network-connected devices. The integration of the Ordr Systems Control Engine (SCE) with FortiManager, FortiGate, and FortiNAC, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers the ability for customers to reduce the time and effort to create and maintain a proper asset inventory, determine asset communication patterns, and create effective, business-relevant firewall and network access control (NAC) segmentation policies that automatically update as devices are added, removed, and move around the network.

Solutions

- Ordr Systems Control Engine
- Fortinet FortiManager
- Fortinet FortiGate
- Fortinet FortiNAC

Joint Solution Benefits

- Discover and inventory every connected network asset, including the massive volume of connected medical devices
- Establish comprehensive security controls that restrict medical IoT devices to known-good network behaviors
- Manage firewall and NAC policies using business-relevant context such as device type, manufacturer, location, and function—rather than IP addresses
- Automate updates of firewall groups and address information to ensure consistent policy enforcement regardless of device location, VLAN, or IP assignment, thus drastically reducing operational costs and downtime
- Protect critical devices with automated, zone-based segmentation and micro-segmentation within zones

Unmanaged network-connected devices pose a unique security challenge to healthcare agencies. A large majority of IoT devices run neither anti-malware nor patch management software and are thus an inherent risk to an organization. The only way to handle these devices is to proactively segment them from your critical assets.

Within minutes of a device appearing on an organization's network, Ordr automatically discovers, identifies, classifies, risk assesses, and groups it with peers. With just a few clicks, administrators can create business-relevant segmentation policies in FortiGate firewalls that ensure devices of a specific type and role only connect over approved communication channels with necessary destinations—all specific to your agency.

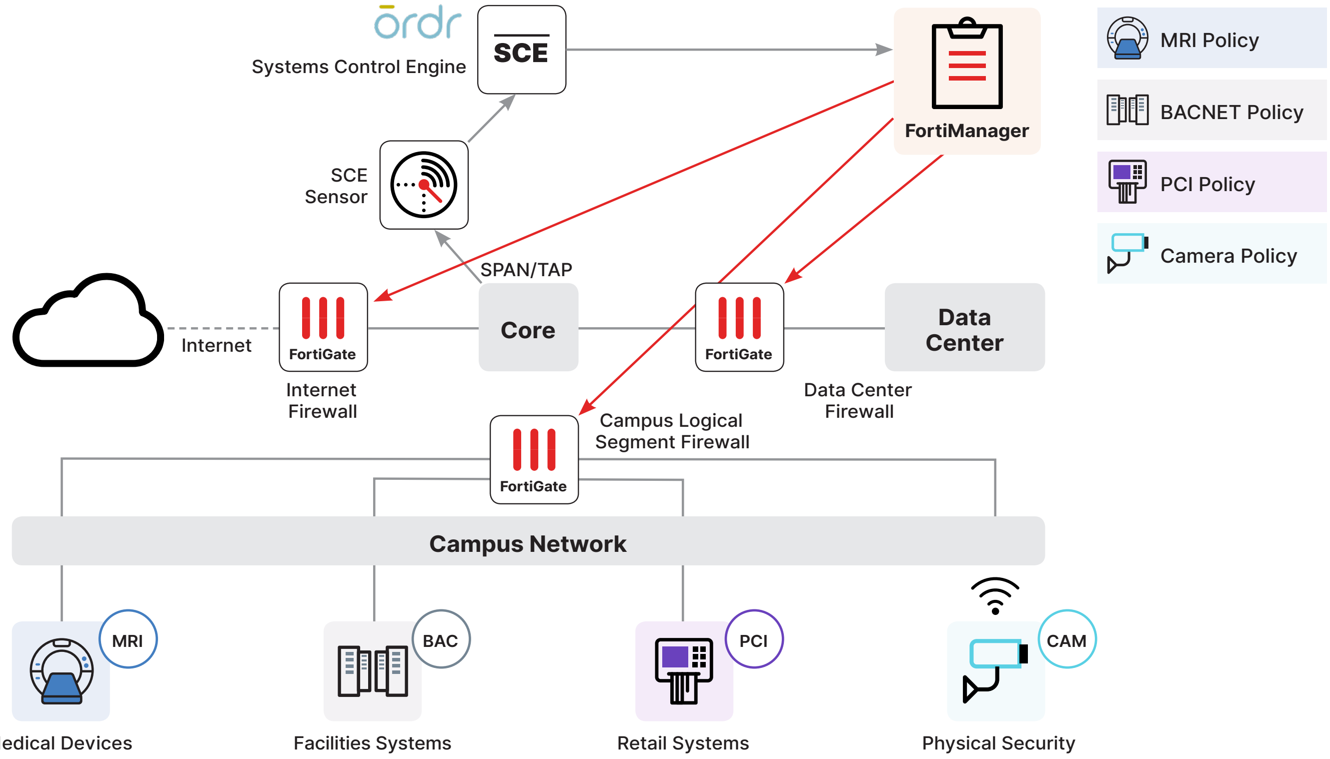
When a device changes physical location and its Internet Protocol (IP) address changes, or similar devices are discovered, Ordr will automatically update the device membership in Fortinet solutions to reduce manual processes (for example, requiring devices of a specific type be assigned to a specific virtual LAN [VLAN] or subnet) and maintenance tasks (for example, costly and time-consuming change control windows to implement firewall policy changes based on IP address changes). Additionally, because Ordr transmits granular device details to FortiGate, FortiManager, and FortiNAC, administrators can further tune policies and make informed decisions about their network without deciphering IP and media access control (MAC) addresses.

The FortiGate NGFW enhances Ordr's visibility into north-south and east-west communications by sending flow data to a centralized Ordr sensor. This extends the visibility in remote and lateral communications to improve visibility, enhance anomaly detection, and increase the efficacy of FortiGate zone-based segmentation and FortiNAC access control policies. FortiGate NGFWs can also reduce incident response efforts by informing Ordr when malicious traffic is dropped at the firewall. This closed-loop integration allows clearing of associated Ordr security incidents related to potentially malicious device communications to known-bad websites and destinations.

Joint Use Cases

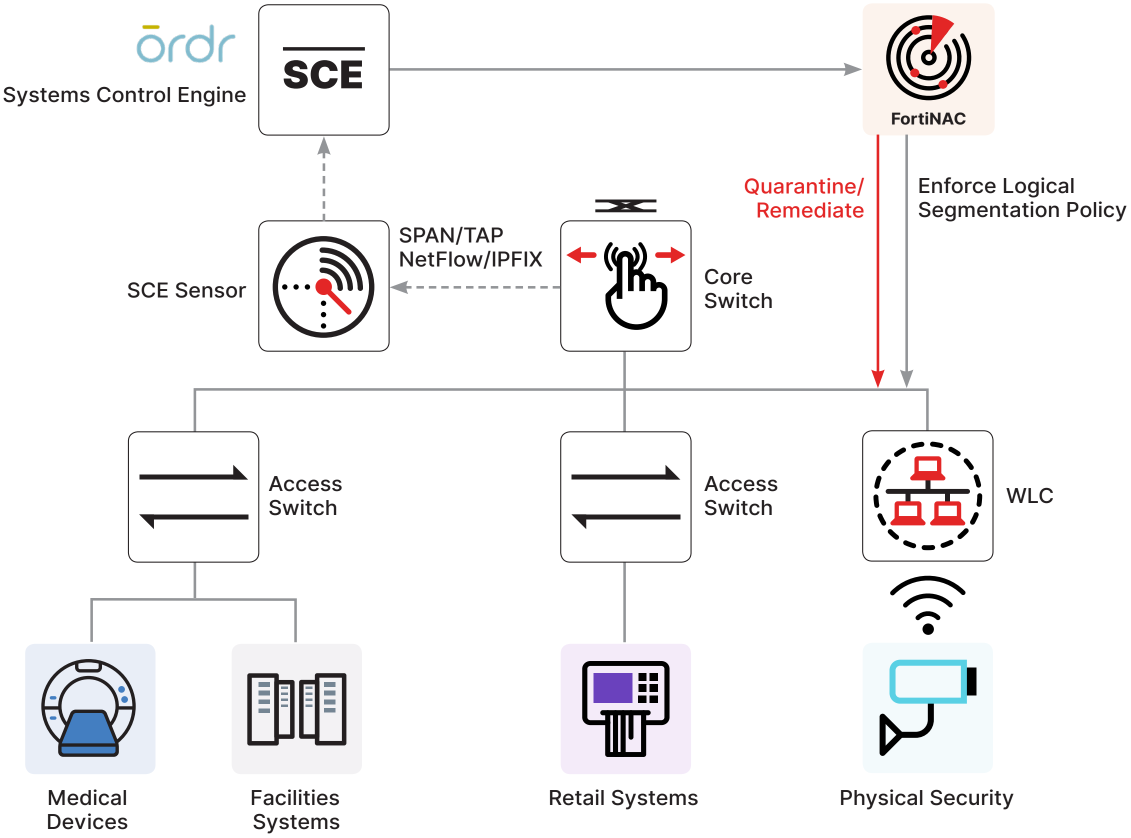
Protect Critical IoT Running Unsupported OS at the Secure Access Service Edge

Critical IoT devices are commonly deployed with deprecated operating systems. While typical user workstations are managed by desktop management services, organizations are often blind to unmanaged IoT devices running vulnerable software. Ordr informs FortiGate firewalls of all devices running unsupported operating systems such as Windows XP/7 and seamlessly provides the visibility necessary to apply protection policies that segment these devices from external and internal threats.



Business-relevant Microsegmentation in the Campus and Data Center

Unsanctioned IoT devices that lack authentication can easily connect to the network and become both targets and launch points for malware and compromise. Ordr augments FortiNAC with additional intelligence, needed to ensure only authorized devices can access the network, and further automates the application of consistent segmentation policies to FortiNAC and FortiGate firewalls to restrict both lateral movement and access to critical resources in the data center.



www.fortinet.com

April 14, 2021 10:43 AM
D:\Fortinet\Work\2021\0414\sb-federal-healthcare-agencies
941100-0-0-EN