SOLUTION BRIEF

Fortinet and Ordr Connected Device Visibility and Security Solution

Automated Visibility and Protection for ALL Connected Devices—From Traditional Servers, Workstations, and PCs to IoT, IoMT, and OT Devices

Executive Summary

Fortinet and Ordr have partnered to deliver an industry-leading Internet-of-Things (IoT) and unmanaged device security solution by integrating FortiGate next-generation firewall (NGFW), FortiManager automation-driven network management, and 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 IoT, operational technology (OT), and unmanaged devices with automated segmentation at the firewall. When combined with Fortinet FortiNAC, you have a comprehensive solution to secure both network access and local area network (LAN) communications as well as all communications between security zones using FortiGate NGFWs.

Challenge

The number of IoT and unmanaged devices connected to corporate networks, from conference TVs to business-critical infrastructure, has grown exponentially. Unfortunately, this brings with it a significant increase in attack surface since these devices often run legacy software without security agents. Without the means to be patched or to protect themselves against attack, IoT and unmanaged devices are extremely vulnerable and therefore lucrative targets. Organizations need to secure access to and from these devices to protect against direct attacks, lateral malware movement, and business interruption. This requires granular details of all devices, their risks, and their ongoing behavior, and then translating this knowledge into proper and automated security workflows. Ordr and Fortinet have teamed to deliver a solution that provides organizations with this ability to discover, assess, and use rich device context to power proactive device policies across the Fortinet fabric. FortiNAC administrators can use Ordr asset details and classifications to easily build dynamic business-driven rules, while firewall administrators can further reduce manual efforts and errors by pushing automated protection policies directly to FortiGate firewalls. Ordr's deep application programming interface (API) integration scales from midsize businesses with individual FortiGates to complex enterprises leveraging extensive FortiManager and FortiGate deployments.

Joint Solution

Ordr and Fortinet have partnered to deliver an industry-leading security solution to address the challenge of widespread IoT and unmanaged device sprawl. The API integration of the Ordr Systems Control Engine (SCE) with FortiManager, FortiGate, and FortiNAC, enabled through 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

Joint Solution Components

- 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 IoT and unmanaged devices, illuminating critical details like operating system, manufacturer, model, and location
- Establish comprehensive security controls that restrict IoT devices to known-good network behaviors
- Manage firewall and NAC policies using business-relevant context such as device classification, function, and risk rating
- Automate updates of firewall policies leveraging existing Fortinet tags and groups, with consistent policy enforcement regardless of changes to device location, VLAN, or IP assignment, thus drastically reducing operational costs and downtime
- Protect critical devices with zero-trust segmentation policies using a combination of top-down zones and network groupings or granular device-centric microsegmentation

Fabric-Ready

asset communication patterns, and create effective, business-relevant firewall and network access control (NAC) segmentation policies that automatically update as devices are added, moved, and changed.

IoT and unmanaged devices pose a unique and growing security challenge to organizations. By nature, 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. Ordr transmits this device context to FortiNAC to dramatically speed and simplify NAC policy creation. And, 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 unique and custom to your organization.

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 local-area network [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.

FortiGate NGFWs enhance 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 Solution Components

Ordr Systems Control Engine (SCE)

Ordr is IoT and unmanaged device security made simple. Ordr discovers every connected device, profiles device behavior and risks, and then automates response through dynamic policy generation and segmentation. Organizations use Ordr to understand risks, bring devices into compliance, and support device procurement decisions.

Fortinet Security Fabric—FortiGate, FortiManager, and FortiNAC

Fortinet FortiGate Next-Generation Firewall

FortiGate NGFWs enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. FortiGate NGFWs are powered by artificial intelligence (AI)-driven FortiGuard Labs and deliver proactive threat protection.

Fortinet FortiManager

FortiManager provides full visibility and control of the Fortinet Security Fabric and enables management of Fortinet products and devices, including FortiGate firewalls.

Fortinet FortiNAC

The FortiNAC solution protects both wireless and wired networks with a centralized architecture that enables distributed deployments with automated responsiveness. FortiNAC enables three key capabilities to secure IoT devices: network visibility to see every device and user as they join the network, network control to limit where devices can go on the network, and automated response to speed the reaction time to events from days to seconds. Collectively, these three capabilities provide the tools that network owners need to secure a world that is embracing the Internet of Things (IoT).

Joint Solution Integration

The Fortinet FortiGate, FortiManager, and FortiNAC integration with Ordr SCE allows customers to reduce the amount of time spent on establishing a proper asset inventory, establishing where those assets are communicating, and creating firewall and NAC segmentation policies. Further, the integration allows for automated segmentation and microsegmentation.

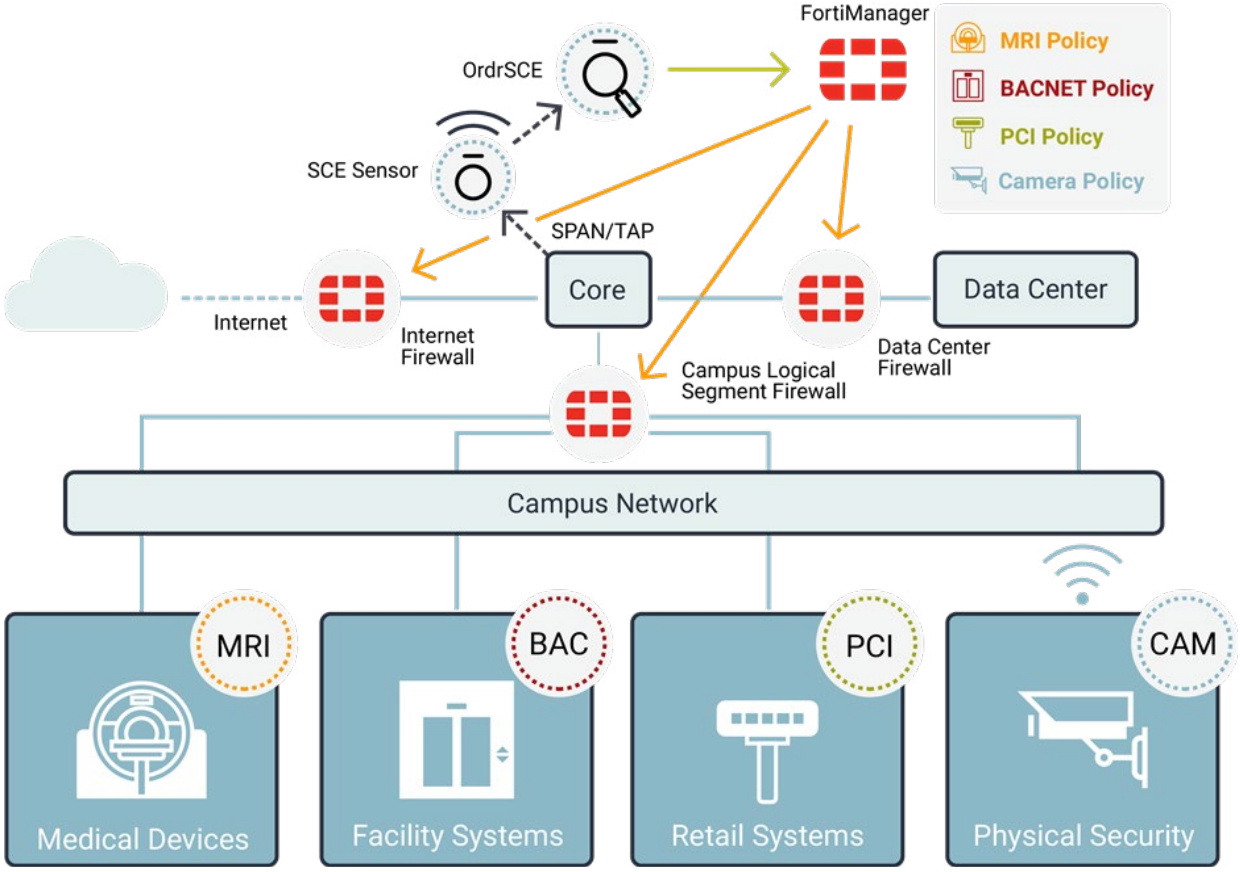

Figure 1: Scale your zero-trust security without scaling your administrators.

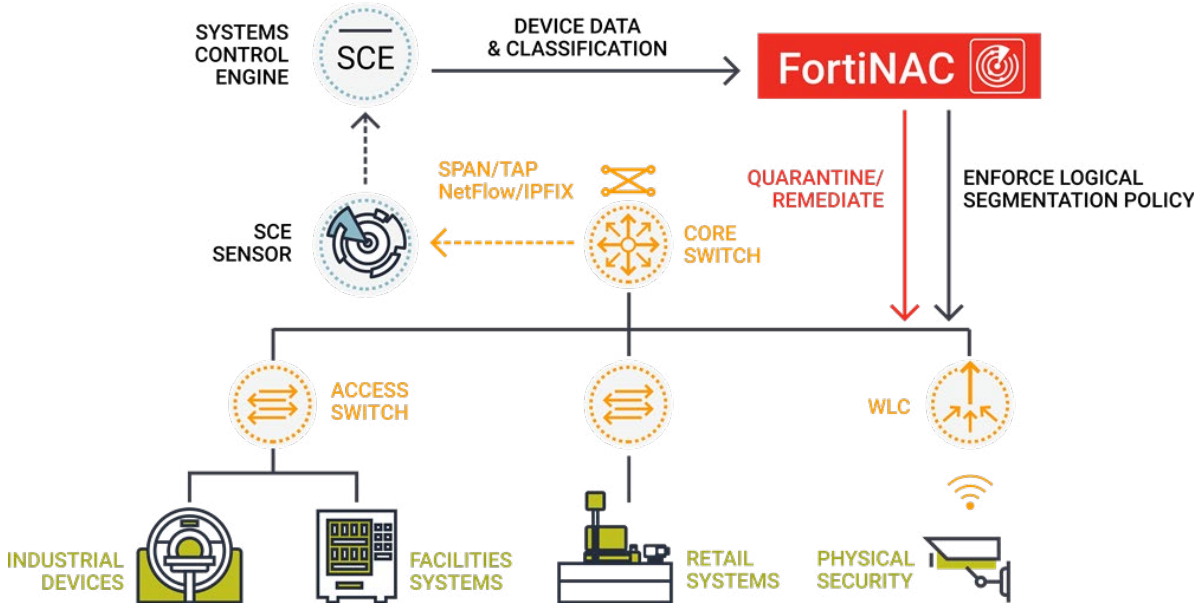

Figure 2: Ordr SCE discovers granular data and augments FortiNAC for complete visibility, response, and control.

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.

About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.

February 11, 2021 10:38 AM

903135-0-0-EN

D:\Fortinet\2020 Old templates\Solution Brief\Grey Solution Brief\Ordr\sb-fortinet-and-ordr-connected-device-2112021\sb-fortinet-and-ordr-connected-device-2112021