SOLUTION BRIEF

Enable Secure Guest Experiences and Safeguard Against Cyberattacks With FortiEDR

Executive Summary

Cyber criminals consider retail operations attractive targets. Vulnerable internet-connected point-of-sale (POS) systems and devices provide a path to valuable information, including customer payment card data, personal information, and corporate intelligence. Often facing cybersecurity staffing shortages, many retailers struggle to cover security gaps. And this situation is exacerbated by the proliferation of point security products and the advanced threat landscape.

Real-time, automated endpoint protection that includes orchestrated incident response across any communication device can help defend retailers against cyberattacks. FortiEDR helps retailers predict, prevent, and detect threats. It also helps them respond and recover from attacks for complete protection across the entire kill chain.

Cyberattacks Risk Positive Shopping Experiences

Some retailers may feel caught between protecting the business against security threats and providing the type of seamless, responsive shopping experience that customers expect. First, there's the task of managing risk and compliance. Payment data must be protected across distributed and complex networks while adhering to growing data privacy requirements. The threat landscape has also grown more sophisticated, and data stored on POS systems, e-commerce, and big data platforms are a common target of cyber criminals.

Speed is the key to breaking the Cyber Kill Chain, and first-generation endpoint detection and response (EDR) tools simply cannot keep up. They require manual triage and responses that are slow and generate many alerts. These first-generation EDR solutions can drive up the cost of security operations and slow incident response processes, which can lead to production shutdowns and disruption for system users. Retailers need an EDR solution that can solve these challenges and is easy to use that offers a low total cost of ownership (TCO).

Fortinet Delivers Advanced, Automated EDR

Built from the ground up for end-to-end security, FortiEDR provides transparent visibility across all endpoints, including POS systems. It has an intuitive user interface that gives retailers the ability to manage endpoint policies and remediate infections quickly and easily. In a single agent, FortiEDR combines next-generation antivirus (NGAV) protection, application communication control, virtual patching, and automated EDR for real-time blocking, threat hunting, and incident response.

- **Protection.** FortiEDR offers proactive, real-time, automated endpoint protection with orchestrated incident response across platforms. It stops breaches with real-time post-infection blocking to protect data from exfiltration and ransomware encryption.
- **Management.** A single unified console features an intuitive interface to access and manage FortiEDR. The cloud-managed platform closes the loop and automates mundane endpoint security tasks, freeing your staff to tackle other assignments.

Connected environments to meet customer demand.

More than 40% of retailers point to network complexity as the top barrier to data security. And 66% believe that newly deployed technology is very secure.[1]

Retailers adapt to new markets.

Retailers are accelerating merchandise cycles, moving supply chains closer to the consumer, and deploying advanced technologies.[2] COVID-19 has compounded problems with margins becoming even more compressed as consumers shift online.[3]

From bricks to clicks.

96% of retailers use sensitive data on digitally transformative technologies and 62% report they have been breached at some point in their history.[4]

- **Scalability.** With a native cloud infrastructure and a small footprint, FortiEDR can be deployed quickly and scale up to protect hundreds of thousands of endpoints.
- **Flexibility.** Endpoints are protected both online and offline, and you can address an array of scenarios, from on-premises in an air-gapped environment to a secure cloud instance.
- **Cost.** With a low, predictable cost, and capped TCO, FortiEDR can help eliminate post-breach operational expenses and breach damage to the organization.

In 2020, there were over a hundred thousand incidents investigated and around 3,900 confirmed breaches with over 400 confirmed breaches taking place in retail alone. 61% of all breaches occurred via web application exploits, POS attacks, or the use of crimeware.[5]

FortiGuard Labs extracts threat intelligence from over 100 billion security events daily.[6]

Pre- and Post-infection Real-time Endpoint Threat Protection

FortiEDR can help protect retail organizations from constant threats, whether attackers are trying to steal customer financial data or sabotage operations. Its capabilities include:

- **Proactive attack surface risk mitigation.** FortiEDR delivers advanced automated attack surface policy control with vulnerability assessments and Internet-of-Things (IoT) security.
- **Malware prevention.** A machine-learning (ML) antivirus engine helps stop malware pre-execution. This cross-operating system NGAV capability is configurable and comes built into the single, lightweight agent, so users can assign anti-malware protection to any endpoint group without requiring additional installation.
- **Real-time automated breach protection.** FortiEDR detects suspicious process flows and behaviors and immediately defuses potential threats by blocking outbound communications and access to the file system from suspicious processes, which prevents data exfiltration, command-and-control communications, file tampering, and ransomware encryption. At the same time, the FortiEDR back end continues to gather additional evidence, enrich event data, and classify the incidents. The solution surgically stops data breach and ransomware damage in real time to automatically keep the business running even on devices that have been compromised.
- **Customizable incident response.** With FortiEDR, you can orchestrate incident response operations using tailor-made playbooks with cross-environment insights. You can streamline incident response and remediation processes and manually or automatically roll back malicious changes done by already contained threats on a single device or on devices across the environment.
- **Guided interface with data enrichment.** FortiEDR automatically enriches data with detailed information on malware both pre- and post-infection to conduct forensics on infiltrated endpoints. This unique interface provides helpful guidance, recommends best practices, and suggests the next logical steps for security analysts.

Retailers that use FortiEDR also benefit from the Fortinet Security Fabric architecture and integration with other components of the Security Fabric, including FortiGate, FortiSandbox, and FortiSIEM.

Detection and Remediation Without the Aggravation

With FortiEDR, retail organizations can strategically reduce the complexity and cost associated with the detection and remediation of advanced malware across POS and other endpoints. In addition, FortiEDR minimizes incident response time pressures and alert fatigue, while preventing the exploitation of vulnerable endpoints that commonly leads to data breaches and disruption from cyberattacks.

[1] "2019 Thales Data Threat Report—Retail Edition," Thales, September 24, 2019.

[2] "2019 Retail Industry Outlook," Deloitte, 2019.

[3] "2021 Retail Industry Outlook," Deloitte, 2020.

[4] "2019 Thales Data Threat Report—Retail Edition," Thales, September 24, 2019.

[5] "2020 Data Breach Investigations Report," Verizon, 2020.

[6] "FortiGuard Security Services," Fortinet, September 2020.

FORTINET

www.fortinet.com

May 12, 2021 1:32 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\May\Retail EDR\sb-FA-retail-edr-5122021\sb-FA-retail-edr-5122021

1022667-0-0-EN