FORTINET

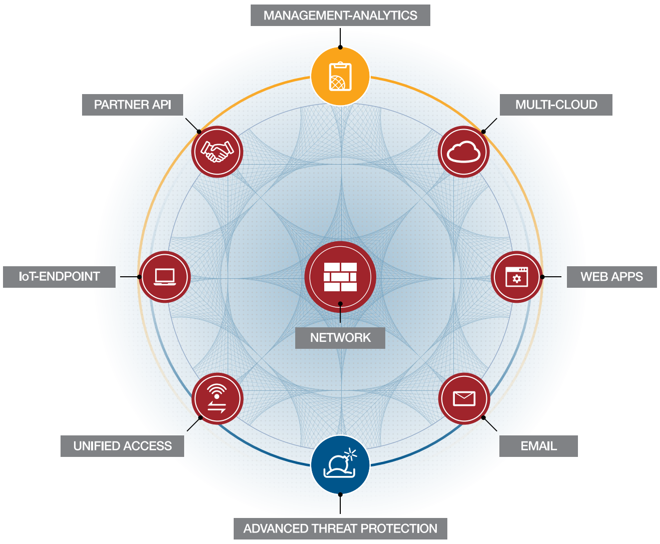
FORTINET SECURES THE DISTRIBUTED RETAIL ENTERPRISE

The digital economy is here and evolving, and requires retail organizations to drive business value by leveraging technology to connect users, devices, data, products, and services.

To operate in the most effective, efficient and profitable manner, retail organizations have digitally transformed the way they do business. They are adopting new models of connectivity and data sharing, such as enabling the Internet of Things and omni-channel models, making them more agile and more responsive to consumer needs and market demands. What are the impacts of this digital transformation on retail networks and can their current security infrastructure support these new requirements?

The answer is simple. This digital evolution leads to an unparalleled attack surface which continues to expand making retailers even more vulnerable to attacks. With Personal Identifiable Information (PII) and Financial records having a high value on the black market, retailers are prime targets for opportunistic cyber criminals. The aftershocks of a breach on a retailer can be devastating affecting brand reputation and customer trust which translates to loss of business.

Unfortunately, most retail organizations implement security strategies that do not take into account the complex nature of their distributed and disparate environment. It's clear from the continued breaches that the traditional methods of securing the network no longer work. In order to support these new technologies and maintain consumer trust, retail organizations need to rethink their security posture. Fortinet offers retail a new approach to cybersecurity, the Fortinet Security Fabric, which promises security that is Broad, Integrated, and Automated.



Broad: Cybersecurity that covers the entire attack surface through industry-leading solutions and technologies that scale and deliver seamless protection from the end-point, access, application to the cloud with visibility extended to other vendor solutions.

Integrated: Collaborative cybersecurity where multiple technologies work together for the detection of advanced threats. The integration of devices using open standards, common operating systems, and unified management platforms enables the sharing and correlation of real-time threat intelligence.

Automated: Proactive cybersecurity that can quickly and dynamically respond to threats with all security elements seamlessly exchanging real-time threat intelligence and coordinating actions.

IMPORTANT NUMBERS IN RETAIL

56% of every dollar spent in retail was influenced by a digital device in 2016[1]

39% of retailers ranked 'Ability to turn customer data into intelligent and actionable insight' one of their greatest challenges[2]

16% of retail organizations suffered losses of over $1 million as a result of a cybersecurity incident[3]

33% of consumers wouldn't shop at a retailer within 3 months of a cyber-attack*

Sources:
[1] Deloitte Digital Influence Survey 2016
[2] PWC – Total Retail 2017
[3] PwC - Global State of Information Security Survey 2017
*Thales Data Threat Report – Retail Edition 2017

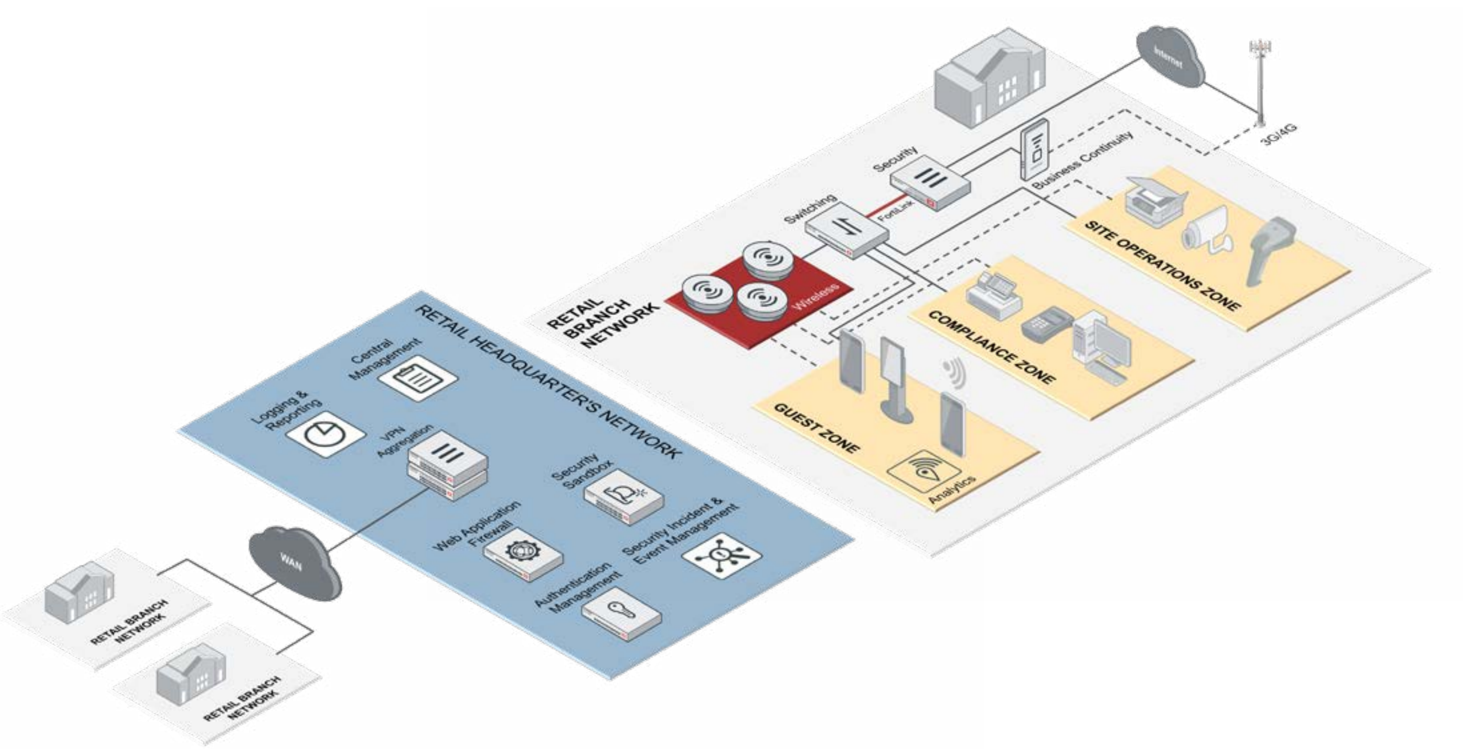


FIGURE 1: THE FORTINET SECURITY FABRIC IN ACTION – COMPREHENSIVE SECURITY FOR THE DISTRIBUTED RETAIL ENTERPRISE

With the Fortinet Security Fabric, retail organizations are well positioned to meet both their current as well as future security needs. As demonstrated in Figure 1, through the realization of having multiple technologies work together, the Fortinet Security Fabric can easily adapt to retail's evolving industry dynamics; IT infrastructure and threat landscape enabling them to provide quality consumer services and grow their business today, tomorrow, and well into the future.

www.fortinet.com