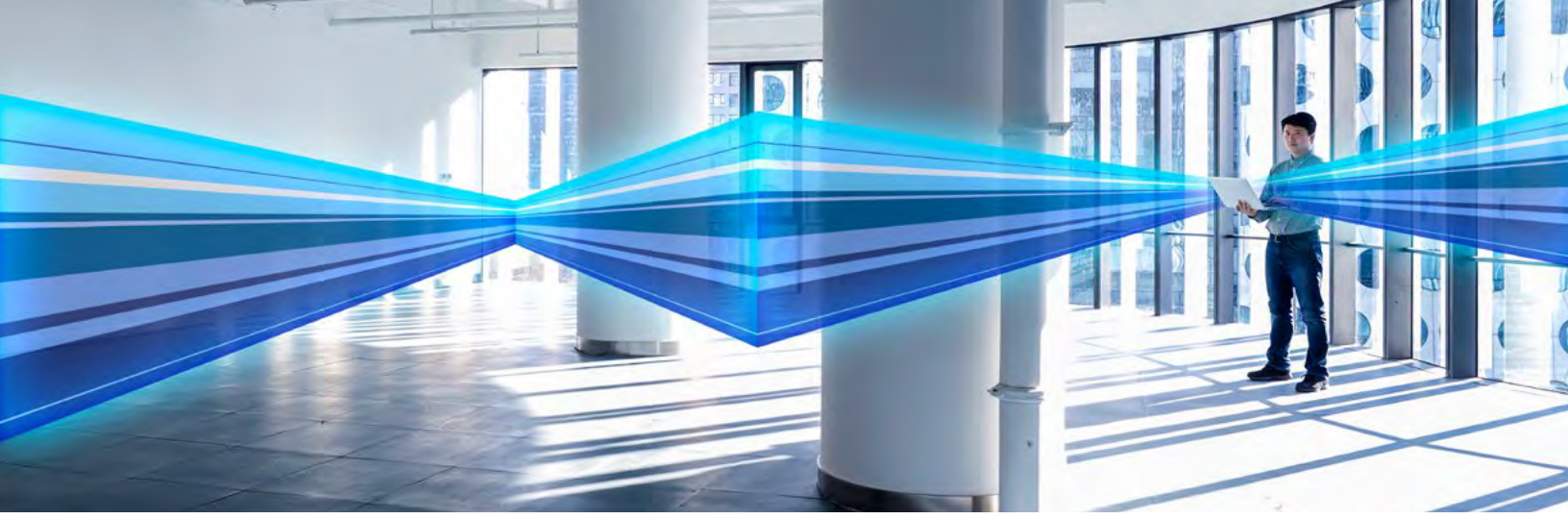

RETAILERS, ARE YOU PREPARED TO DEFEND AGAINST TODAY'S ADVANCED CYBER THREATS?

Check this list twice to protect the omnichannel in 2017 and beyond.

Don't Just Rely on PCI Compliance:
PCI compliance is a little like making sure a lock is on your front door, but it doesn't guarantee the lock stays in place. Cyber criminals are constantly uncovering new entry points and vulnerabilities to invade your network outside of the cardholder data environment (CDE).

Average Retail Dwell time is 197 days[1]

Make Threat Intelligence Your Secret Weapon:
To take your security posture to the next level and better identify suspicious activity, retailers should leverage threat intelligence that tracks two-way network communications. It's critical to find a provider with broad visibility into internet traffic, cyber risks and malicious activity worldwide.

Botnets represent **83%** of all eCommerce fraud attacks in the US in 2016.[2]

Leverage Private Connectivity to the Cloud:
Help minimize threats and enhance security of sensitive data and personally identifiable information (PII) transported to and from your cloud-based applications through private connectivity to cloud service providers (CSPs).

68% of retailers cite security concerns when moving applications to the cloud.[3]

Combat Malware at the Storefront:
Many retailers bypass security controls to implement the latest in-store technologies and SaaS applications, leaving the door open for vulnerabilities and exploits. High-performance, cloud-based firewalls can provide next-generation security capabilities across the retail store network.

58% of retailers cite malware as the greatest security risk of 2016.[4]

Protect Online Shopping with DDoS Mitigation:
With DDoS attacks growing in size and sophistication, retailers must ensure their provider not only has the ingest capacity but also takes a proactive approach to defending against advanced network threats.

86% of websites contain **at least one** serious vulnerability.[5]

Mind the Increased Risk of In-Store Wi-Fi:
Beyond just following the PCI DSS for Wi-Fi, retailers should implement supplementary security measures to help protect both customers and employees using in-store Wi-Fi systems. Cloud-based firewalls that offer instruction protection and detection, web content filtering and sandboxing enable retailers to do just that.

42% of retailers cite in-store Wi-Fi technology as posing the greatest security risk in 2016.[6]

Know Seasonal Employees Can Elevate Risk:
Because temporary and contract employees can bring infected devices into the network, retailers need tools that help detect and mitigate threats with improved network visibility.

According to Ovum, only **20%** of enterprises have a policy governing BYOD behavior.[7]

Don't Forget the Contact Center:
Contact centers are also a doorway into fraudulent activity and social engineering aimed at stealing customer data. For the best defense, retailers should leverage cloud-based contact center platforms that easily integrate advanced authentication and fraud detection/prevention technologies.

Call center fraud grew **45%** between 2013 and 2016.[8]

TO STOP THREATS, YOU FIRST HAVE TO SEE THEM COMING

Contact Level 3 to learn more about implementing next-gen defenses to better safeguard your omnichannel retail environment.

[1] Infosecurity Magazine, *Retailers Take 197 Days to Discover Advanced Attacks*, 2015
[2] PYMNTS/Forter, *Global Fraud Attack Index*, Q3 2016
[3] Innovative Retail Technologies, *Retail Tech Spending 2016*, 2015
[4] Retail Info Systems News, *Business-Driven Security*, July 2016
[5] WhiteHat Security, *Website Security Statistics Report*, 2015
[6] Retail Info Systems News, *Business-Driven Security*, July 2016
[7] Security Magazine, *Bring Your Own Risk With BYOD*, April 2016
[8] Pindrop, *State of Phone Fradu Report: 2016 Call Center Fraud Report*, 2016

Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠