ZIMPERIUM®

PCI & Mobile Devices

The Facts About Mobile Security & Compliance

Fact #1: PCI has included mobile since 2013

By now, anyone who is concerned about processing credit cards and securing cardholder data is familiar with PCI. The mandate requires merchants who accept credit cards to comply with PCI Security Council standards. It was established in 2001 with the release of PCI DSS Version 1.0.

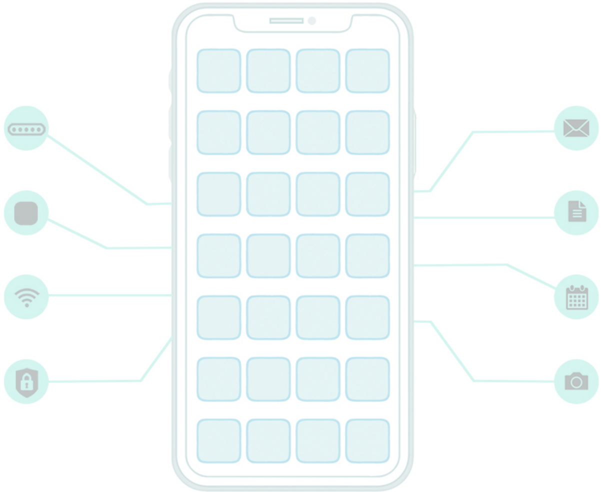
As far back as 2013, with the publishing of PCI Mobile Payment Acceptance Security Guidelines, PCI has explicitly included mobile devices in its scope. In 2019, PCI and mobile will blend even more when the PCI Security Council releases the PCI Contactless Payments on COTS Standard, a forthcoming security standard for accepting contactless payments on commercial, off-the-shelf (COTS) phones or tablets.

In short, if your PCI compliance measures do not yet include mobile devices, you are out of compliance.

Fact #2: Mobile devices are 60% of PCI-covered endpoints

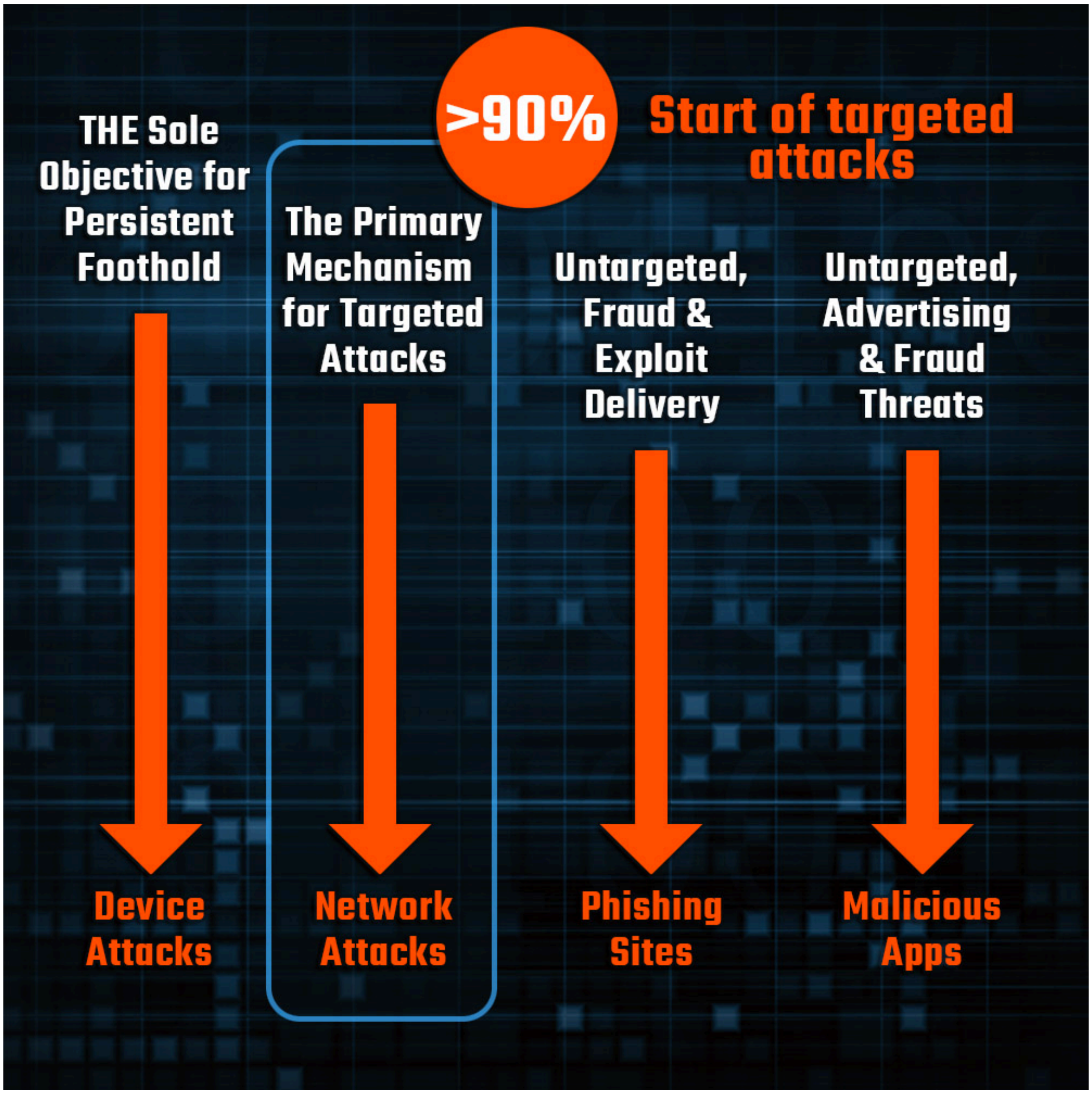
A 2018 report by a leading telecommunications firm found that PCI compliance had recently been trending downward. Even so, most enterprises subject to the regulation have invested significant resources toward achieving compliance. The problem arises when enterprises focus on protecting endpoints without realizing that mobile devices are endpoints, both with respect to PCI and in general.

Mobile devices are now the de facto platform for productivity in business. Today, the traditional computing devices (e.g., servers, desktops and laptops) upon which enterprises have focused their security and compliance efforts represent only 40% of the relevant endpoints. The remaining 60% of devices that connect to your enterprise network—mobile devices—must be brought into PCI compliance as well.



Fact #3: Mobile endpoints are under attack

One critical difference between mobile devices and other types of endpoints is the variety of attack vectors to which mobile devices are subject. Ensuring the integrity of mobile devices requires protecting them against all of these forms of attack.


>90%
Start of targeted attacks
THE Sole Objective for Persistent Foothold
The Primary Mechanism for Targeted Attacks
Untargeted, Fraud & Exploit Delivery
Untargeted, Advertising & Fraud Threats
Device Attacks
Network Attacks
Phishing Sites
Malicious Apps

Fact #4: PCI requirements for mobile are explicit

The Zimperium platform helps you bring your enterprise's mobile devices into compliance, whether they are corporate-owned or employee-owned. Specifically, Zimperium helps you meet the mobile mandates of the PCI DSS requirements shown below.

SECTION	SUBSECTION	PROVISION
Req 5		**Protect all systems against malware and regularly update anti-virus software or programs**
	5.1	Deploy anti-virus software on all systems commonly affected by malicious software.
	5.11	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.logs which are retained per PCI DSS Requirement 10.7.
	5.2	Ensure that all anti-virus mechanisms are maintained as follows: Are kept current, Perform periodic scans Generate audit logs which are retained per PCI DSS Requirement 10.7.
	5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.
Req 5		**Develop and maintain secure systems and applications**
	6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.
	6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.
	6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes).

Fact #5: Zimperium is the solution for mobile PCI compliance

Zimperium leverages a patented engine to detect mobile device, network, phishing and app attacks in real time. The engine runs efficiently on smartphones and tablets without violating user privacy. To date, the engine has detected 100 percent of zero-day device exploits without requiring an update or suffering from the delays and limitations of cloud-based detection or legacy security architectures, making Zimperium uniquely capable of meeting PCI mobile requirements. Additionally, Zimperium's advanced app analysis capability enables organizations to meet 6.3.2 by identifying all privacy and security risks inherent in any PCI-relevant mobile app code.

Contact Zimperium for PCI mobile compliance

When you are ready to ensure compliance with PCI mobile requirements, please contact us for a custom evaluation.

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc
4055 Valley View, Dallas, TX 75244