NDB & Mobile Devices

The Facts About Mobile Security & Compliance

Fact #1: NDB has included mobile since it took effect in 2018

By now, anyone doing business in Australia should be familiar with Notifiable Data Breaches (NDB) scheme. The scheme applies to businesses whose annual turnover in Australia exceeds $3 million AUD and requires prompt notification to customers in the event of a data breach in which the customer's personal information is lost or stolen.

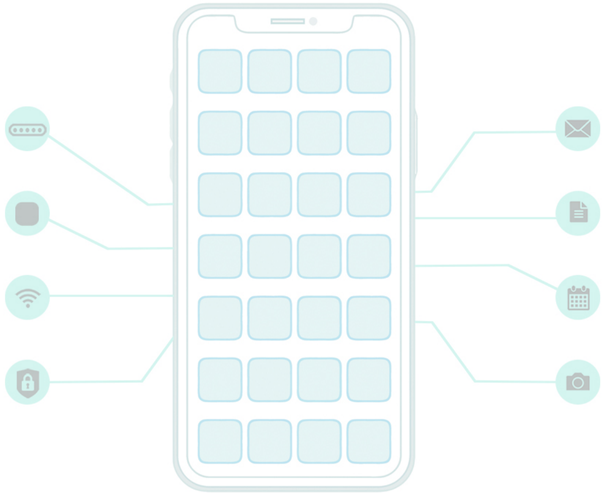
What may not be as widely known is that NDB requirements around protecting customer data have applied to mobile devices since the act came into effect on February 22, 2018. As one leading Australian communications company observed, protection against mobile device threats "must cover multiple access levels, including device, app, network, and content protection" and "real-time monitoring is an essential part" of the required security measures.

In other words, if your NDB compliance measures do not yet include mobile devices, you are out of compliance.

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

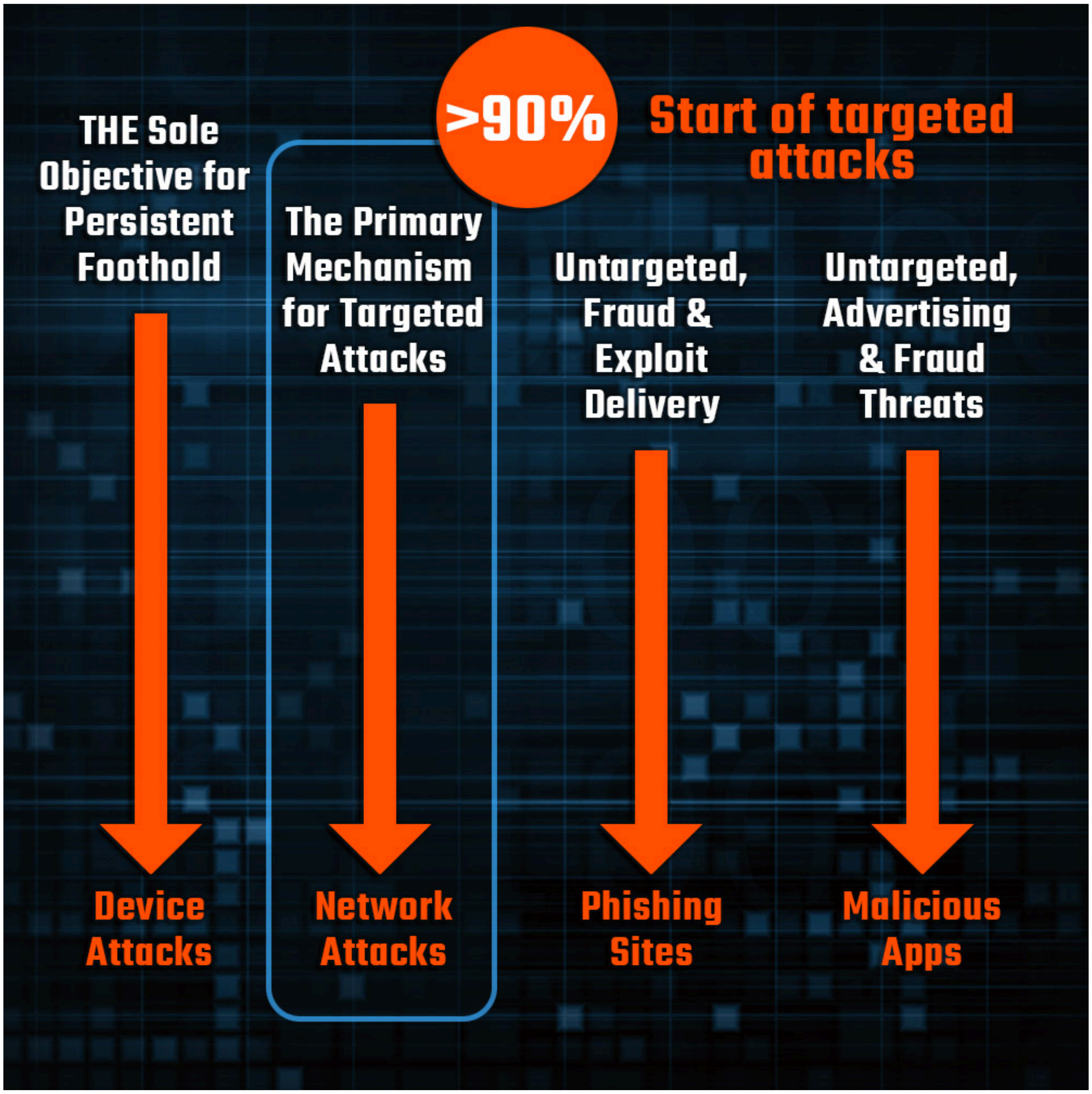
In the fourth quarter of 2018 alone, the Office of the Australian Information Commissioner (OAIC) received 216 notifications under the Notifiable Data Breaches (NDB) scheme. So, it is not surprising that most enterprises subject to NDB have invested significant resources toward achieving compliance. The problem arises when enterprises focus on protecting endpoints without realizing that **mobile devices are endpoints**, both with respect to NDB and in general.

Mobile devices are now in wide use as a platform for productivity in business. That means that the traditional computing devices (e.g., servers, desktops and laptops) that enterprises have focused their security and compliance efforts on are only about 40% of their enterprise's endpoints. The other 60% of devices that connect to your network—mobile devices—must be made NDB-compliant 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 that mobile devices are exposed to. 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: Zimperium is the solution for mobile NDB compliance

Zimperium leverages a patented, machine learning-based 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 NDB mobile requirements.

Contact Zimperium for NDB mobile compliance

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

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

Zimperium, Inc
4055 Valley View, Dallas, TX 75244