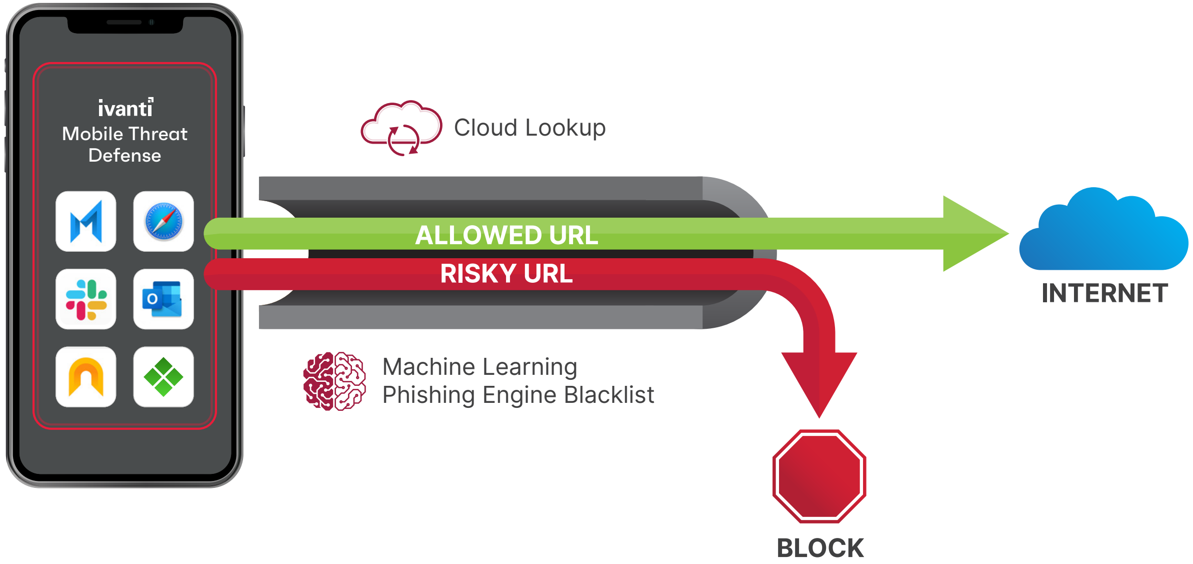
Complete Mobile Phishing Protection

Achieve 100% User Adoption

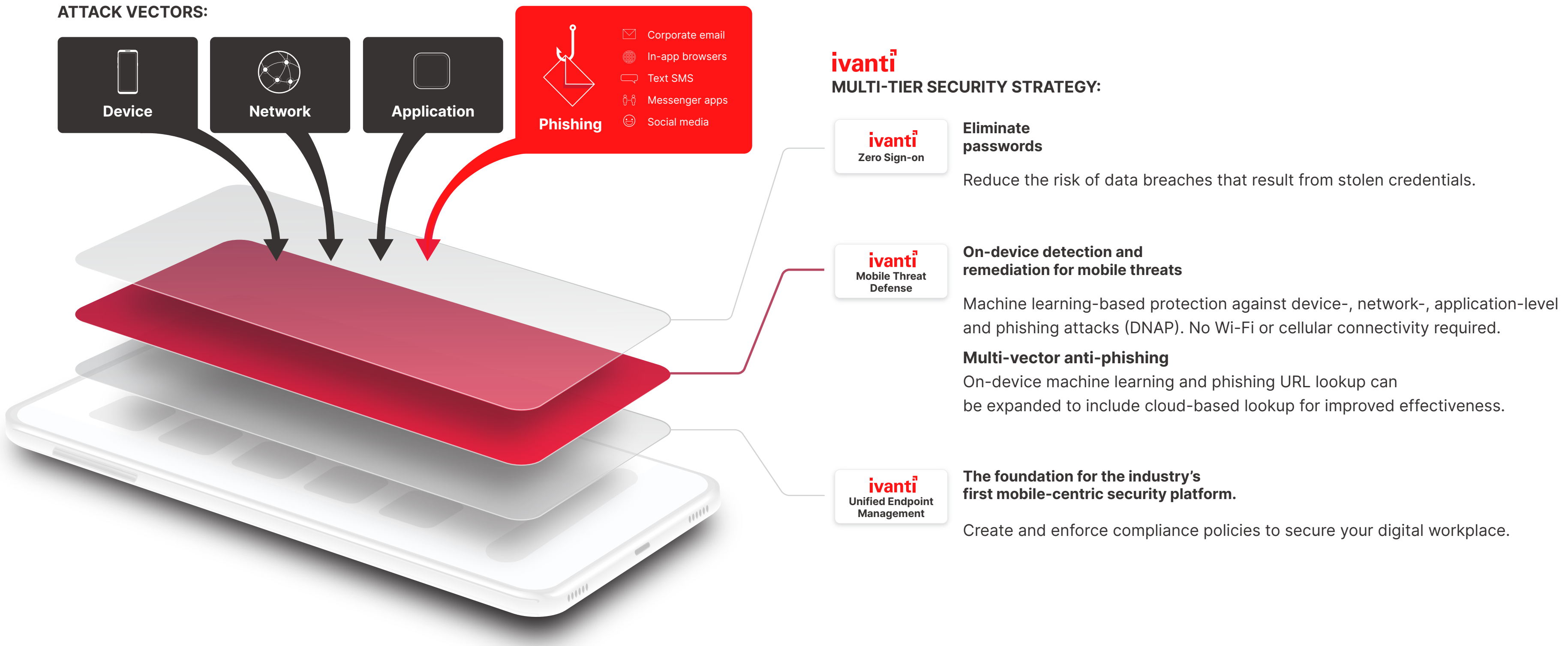
Key Benefits

- Achieve 100% user adoption for anti-phishing
- Deploy multi-vector phishing protection and remediation
- Control the balance between security and user privacy



Overview

Phishing attacks leverage deception to trick individuals into divulging personal information that can then be leveraged for fraudulent purposes. For instance, an individual might be tricked into clicking on a link and then providing their personal login credentials. Or, they might be tricked into downloading malware or an exploit kit onto their device. According to the 2021 Verizon Data Breach Investigations Report (DBIR), phishing was the top tactic used in data breaches for the third straight year. This trend shows no signs of stopping as DBIR data reveals the percentage of breaches where phishing was present rose 25% from 2019 to 2020.[1]



ivanti MULTI-TIER SECURITY STRATEGY:

Eliminate passwords

Reduce the risk of data breaches that result from stolen credentials.

On-device detection and remediation for mobile threats

Machine learning-based protection against device-, network-, application-level and phishing attacks (DNAP). No Wi-Fi or cellular connectivity required.

Multi-vector anti-phishing

On-device machine learning and phishing URL lookup can be expanded to include cloud-based lookup for improved effectiveness.

The foundation for the industry's first mobile-centric security platform.

Create and enforce compliance policies to secure your digital workplace.

Why are mobile devices increasingly targeted by hackers?

There are many reasons that mobile devices have become a favorite target for hackers. For example, mobile devices now outnumber traditional endpoints (desktops and laptops) in the enterprise, yet many organizations still view mobile security as a low priority. This is often because they have not yet experienced a data breach or are simply unaware. As a result, budget earmarked for mobile security is often a mere fraction of what has been dedicated to traditional endpoint security. In addition, the appeal of mobile devices as a launching point for phishing attacks can also be attributed to their small screen size, which makes it more difficult for the user to access and view key information in order to make a well-informed decision. Also worth highlighting is the difficulty in verifying the authenticity of text/SMS messages

Multi-vector anti-phishing with Ivanti Mobile Threat Defense (MTD)

Ivanti Mobile Threat Defense (MTD) includes on-device and cloud-based phishing protection to secure all internet-based traffic across iOS and Android devices in the Everywhere Workplace, where corporate data flows freely across devices and servers in the cloud, empowering workers to be productive from anywhere. No user interaction is required to activate MTD on mobile devices that are enrolled in Ivanti UEM. Instead, activation is remotely managed by IT departments.

Achieve 100% user adoption for anti-phishing

MTD enables seamless deployment for anti-phishing, as well as protection and remediation for attacks at the device, network and application levels. No user interaction is required to activate, so admins can ensure 100% adoption. Tiered compliance actions can be leveraged to help drive and keep adoption in order to improve your organization's overall security posture.

Deploy multi-vector phishing protection and remediation

MTD anti-phishing detects and remediates phishing attacks across all mobile threat vectors, including text and SMS messages, instant messages, social media and other modes of communication, beyond just corporate email. Multi-vector phishing protection leverages on-device machine learning and database lookup. Extend to include cloud-based phishing URL database lookup for even greater effectiveness. In addition, phishing analytics can be used to provide fast and easy insight to better understand your organization's anti-phishing coverage.

Control the balance between security and user privacy

MTD anti-phishing puts your organization in complete control of maintaining balance between security and user privacy to best meet your needs and comfort level. Leverage MTD's highly-effective on-device phishing detection or easily expand detection into the cloud if you choose to do so. The choice is yours!

Complete mobile phishing protection

MTD includes on-device and cloud-based phishing protection to secure all internet-based traffic across iOS and Android devices in the Everywhere Workplace. No user interaction is required to activate MTD on mobile devices that are enrolled in Ivanti UEM. Activation is instead managed remotely by IT departments, helping organizations achieve 100% user adoption, without impacting productivity. To further secure their digital workplaces and reduce the risk of phishing attacks, organizations can implement Ivanti's Zero Sign-On (ZSO) solution for secure and passwordless authentication to enterprise cloud services.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Verizon: 2021 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/