iVerify.

Data Sheet

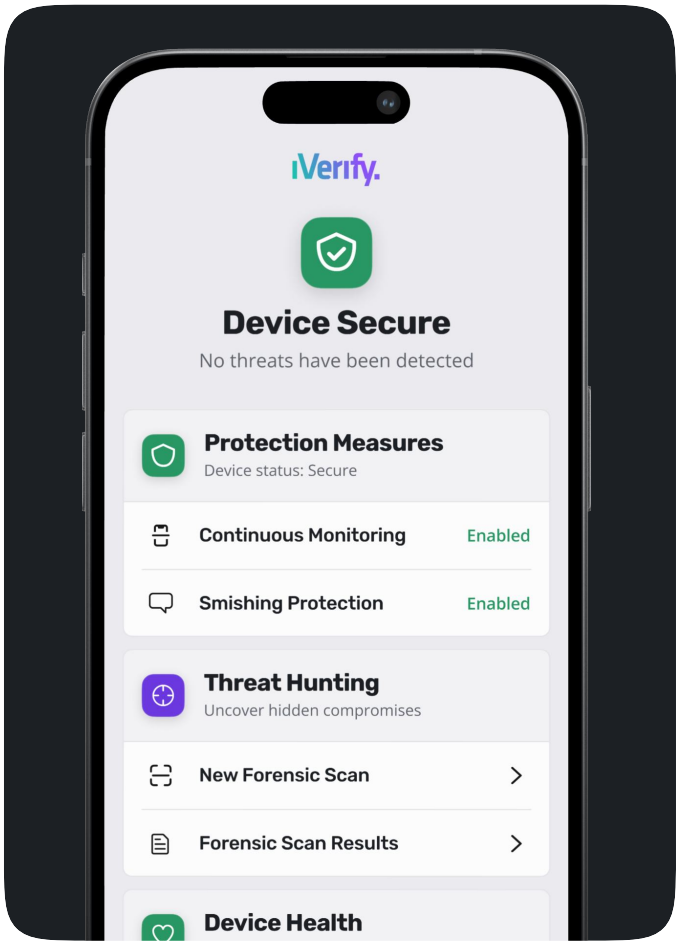
Mobile BYOD

Premium mobile security that respects user privacy for companies with a BYOD workforce.

Threats to mobile devices are real. They store sensitive information, like credentials, business data, emails, chat logs, and intellectual property, and often lack adequate protection, making them prime targets of ransomware, espionage, and access broker threats.

Protecting mobile BYOD can be a challenge to organizations trying to strike a balance between productivity, security and privacy. Regulators and compliance requirements like PCI and HIPAA are starting to take a more active role in the mobile security landscape and business drivers are requiring companies to roll-out mobile security for all employees.

iVerify offers premium mobile security for companies with a BYOD workforce, where user privacy is a priority. Protect against credential theft, smishing, spyware, vulnerabilities, and advanced mobile threats. Conditional access management without the need for an MDM.



iVerify Mobile BYOD offers:

VPN-Less Smishing Defense

Prevent mobile devices from accessing compromised websites and customize DNS blocklist

MDM-Less Access Control

Centralized device management and alerts console with easy to configure access controls to critical company resources like email, Slack, and cloud data

Advanced Threat Protection

Stop smishing, credential theft, account takeover, spyware, vulnerabilities and zero-day threats

Vulnerability Management

Administrative oversight of the mobile fleet to monitor exposure risk including out-of-date OS and risky device settings

User Privacy

Protect every mobile device that connects to corporate resources while respecting users' privacy

Security Education

Security guides to educate users on how to stay safe from mobile threats and OS vulnerabilities

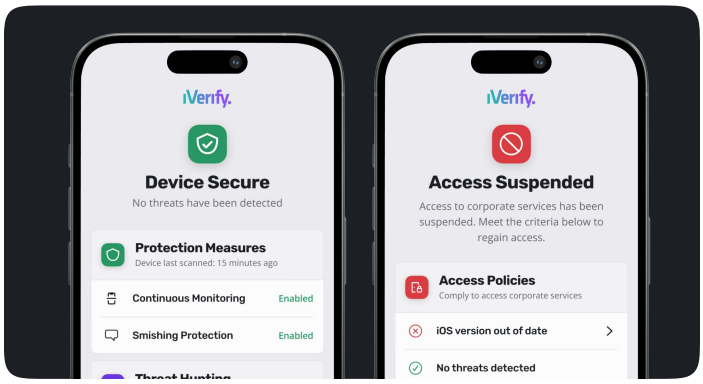
iVerify Mobile BYOD does not access personal data, so there is no trade-off between employee privacy and security.

Privacy First

Only essential security-related data is gathered and processed

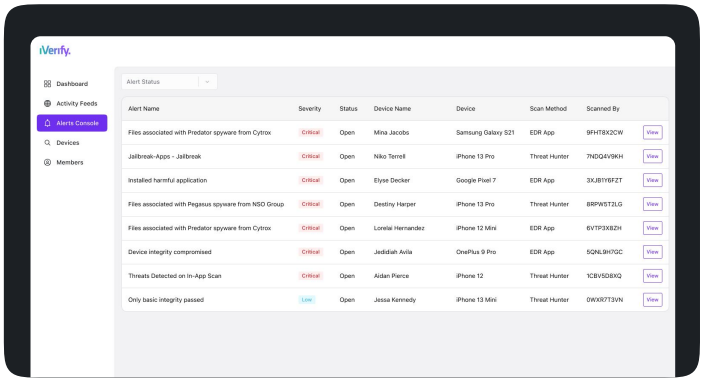
Bring Your Own Device

Users can access corporate applications without sharing private data



Easily deployed

Monitor users' security status, including vulnerability management, via the iVerify dashboard



Conditional Access

Security teams can prevent compromised or insecure devices from accessing corporate resources without impacting personal data

> "We wanted security checks in a privacy-protective mode for employees, and iVerify aligns with this."
>
> *Leading Global Technology Company, Security Manager, Platform Security*

---

iVerify.

iVerify believes users shouldn't have to sacrifice privacy for security. Our easy-to-deploy solution provides fleet-wide iOS and Android security telemetry without requiring a management profile on the device. This lets users keep their personal data private and secure their mobile devices from advanced malware, vulnerabilities, and targeted smishing attacks.

Request more information or a demo at iverify.io/contact