iVerify.

Mobile Compliance Control Mapping

How Mobile EDR extends CIS, NIST 800-53, NIST CSF, ISO/IEC 27001, PCI DSS, GLBA, and HIPAA coverage to the device layer MDM can't reach.

The Problem: Mobile Is a Blind Spot in Compliance Programs

Mobile devices are Tier-1 endpoints. They carry the credentials, MFA tokens, and cloud access that make up an organization's identity layer. Most compliance frameworks and security stacks still don't treat them that way.

Traditional MDM covers two things well:

- Policy enforcement and configuration control
- Visibility into device posture

It has no visibility into the threats operating underneath that layer:

- Zero-day and fileless malware
- Credential phishing and smishing
- Malicious profiles and certificates
- Network-based attacks, including malicious telecom infrastructure
- Advanced persistent threats (APTs) and commercial spyware

That gap doesn't just sit between MDM and the threat landscape. It sits between what a compliance framework requires and what a security team can actually demonstrate during an audit or incident review.

At a Glance

- **The gap:** MDM proves a device is configured correctly. It can't prove a device hasn't been compromised and most compliance frameworks assume that second capability exists.
- **The fix:** iVerify adds OS-level threat detection, monitoring, and incident response that map directly to controls across seven major frameworks.
- **What's inside:** A control-by-control crosswalk across five capability areas: malware protection, logging and monitoring, network security, vulnerability management, and risk and data protection.
- **Why it matters for audits:** Where MDM produces a configuration report, iVerify produces detection evidence — the kind of documentation compliance reviews and cyber insurance underwriting increasingly ask for.

The Solution: Mobile Threat Defense Mapped to Compliance Controls

iVerify is a Mobile EDR platform: it collects operating system-level telemetry from iOS and Android devices and turns it into the detection, monitoring, and response capabilities that MDM and legacy Mobile Threat Defense (MTD) tools weren't built to provide. Each capability below maps to specific controls across the frameworks your compliance program already tracks.

Key Capabilities

OS-level threat detection
Including fileless malware

Privacy-First Architecture
Data anonymization built-in

Network threat & smishing protection
Powered by SmishGuard

Device integrity monitoring
Including jailbreak and root detection

Real-time logging & SIEM/SOAR integration
Via open API and webhooks

Remote mobile forensic analysis & IR
Powered by Threat Hunter IR

Zero-click & APT detection
Catches exploitation with no user interaction

Coverage at a Glance

Where each capability area maps across the seven frameworks in this datasheet.

Capability Area	CIS v8	ISO 27001	PCI DSS	NIST CSF	GLBA	HIPAA	NIST 800-53
Threat Detection & Malware Protection	✓	✓	✓	✓	✓	—	✓
Logging, Monitoring & Incident Response	✓	✓	✓	✓	✓	✓	✓
Network Security & Threat Intelligence	✓	✓	✓	✓	—	—	✓
Vulnerability & Configuration Management	✓	✓	✓	✓	—	✓	✓
Risk Management & Data Protection	—	✓	✓	✓	✓	—	✓

Detailed Control Mapping

The tables below show how iVerify's capabilities align to specific control requirements across five areas. Some controls appear more than once because a single requirement — GLBA 314.4(c), for example — can span more than one capability area; where that happens, the control language is kept consistent across tables.

Threat Detection & Malware Protection

Framework	Control	Control Description
CIS v8	Control 10	Prevent or control the installation, spread, and execution of malicious applications, code, or scripts
ISO 27001	A .8.7	Protection against malware shall be implemented and supported by appropriate user awareness.
PCI DSS	Req. 5	Processes and mechanisms for protecting all systems and networks from malicious software
NIST CSF	D E.AE	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents

GLBA	314.4(c)	Design and implement controls to manage identified risks
NIST 800-53	SI-3	Implement anti-malware and scanning
NIST 800-53	SI-7	Verify software and firmware are not tampered with

iVerify's Solution

iVerify detects fileless malware and other OS-level threats that never touch the app layer MDM and antivirus tools scan, alongside malicious Android APKs. That combination extends CIS Control 10, NIST 800-53 SI-3 and SI-7, and the malware-protection controls in ISO 27001, PCI DSS, and NIST CSF to a layer of the device MDM alone can't see.

Logging, Monitoring & Incident Response

Framework	Control	Control Description
CIS v8	Control 8	Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.
CIS v8	Control 13	Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
ISO 27001	A.8.15	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed.
ISO 27001	A.8.16	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.
PCI DSS	Req. 10	Processes and mechanisms for logging and monitoring all access to system components and cardholder data
NIST CSF	DE.CM	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events
NIST CSF	D E.AE	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents
GLBA	31 4 .4(c)(8)	Detect unauthorized access or tampering
HIPAA	164 .312(b)	Activity logging, anomaly detection
NIST 800-53	SI-4	Monitor and analyze security events

iVerify's Solution

iVerify streams detection data into existing SIEM and SOAR platforms in real time through an open API and webhooks, producing the mobile audit trail that CIS Controls 8 and 13, PCI DSS Requirement 10, and NIST 800-53 SI-4 call for. When an alert needs deeper investigation, iVerify's Threat Hunter Incident Response service correlates device logs, process metadata, and known adversary TTPs to confirm compromise and document findings for the record.

Network Security & Threat Intelligence

Framework	Control	Control Description
CIS v8	Control 13	Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
ISO 27001	A.5.7	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.
PCI DSS	Req. 5	Processes and mechanisms for protecting all systems and networks from malicious software
NIST CSF	DE.CM	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events
NIST CSF	DE.AE	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents
NIST 800-53	AC-20	Verification of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans
NIST 800-53	AC-17	Remote access monitoring and control
NIST 800-53	S I-10	Validate data inputs

iVerify's Solution

SmishGuard blocks smishing links and access to malicious telecom infrastructure at the network layer, addressing the network-monitoring intent behind CIS Control 13, ISO 27001 A.5.7, and NIST 800-53 AC-17 and AC-20. iVerify's Threat Intelligence platform adds visibility into telecom-layer risk and named adversary infrastructure from iVerify's own research, so security teams have documented threat context behind a mobile finding, not just an alert.

Vulnerability & Configuration Management

Framework	Control	Control Description
CIS v8	Control 7	Continuously assess and track vulnerabilities on all enterprise assets.
ISO 27001	A.8.8	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities should be evaluated, and appropriate measures should be taken.
ISO 27001	A.8.9	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.
PCI DSS	Req. 11.3	External and internal vulnerabilities are regularly identified, prioritized, and addressed.
NIST CSF	PR.PS	The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability

HIPAA	164.312(c)	Audit controls, software and patch management
NIST 800-53	SI-7	Verify software and firmware are not tampered with
NIST 800-53	SI-10	Validate data inputs
NIST 800-53	CM-6	Apply and monitor secure settings

iVerify's Solution

iVerify continuously reports OS version and patch level across the fleet, giving compliance teams the visibility CIS Control 7, NIST 800-53 CM-6, and PCI DSS Requirement 11.3 require without waiting on an MDM configuration profile to sync. Because detection runs independently of patch status, iVerify can identify active exploitation on a device that hasn't been patched yet, closing the window between a published vulnerability and a device actually receiving the fix.

Risk Management & Data Protection

Framework	Control	Control Description
ISO 27001	A.8.1	Information stored on, processed by or accessible via user endpoint devices shall be protected.
PCI DSS	Req. 1.5	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.
PCI DSS	Req. 12.3	Risks to the cardholder data environment are formally identified, evaluated and managed.
NIST CSF	ID.RA	The cybersecurity risk to the organization, assets, and individuals is understood by the organization
NIST CSF	PR.DS	Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
GLBA	314.4(b)	Identify foreseeable risks to customer data on mobile devices
GLBA	314.4(c)	Design and implement controls to manage identified risks
NIST 800-53	RA-3	Assess risks associated with mobile devices
NIST 800-53	AC-20	Verification of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans

iVerify's Solution

iVerify supports Zero Trust conditional access with Okta and Entra ID, verifying device integrity before granting access to sensitive systems — the control intent behind NIST 800-53 AC-20 and the risk- management requirements in GLBA 314.4(b) and (c). Detection runs on an anonymized data architecture: no message content, personal data, or device-specific identifiers are exposed beyond a structured finding, supporting ISO 27001 A.8.1 and PCI DSS's requirement to manage risk to the cardholder data environment without introducing a new source of sensitive data exposure.

Close the Gap Between Compliance and Actual Coverage

Compliance frameworks were written with the assumption that every enterprise endpoint has real detection and response behind it. For most organizations, mobile is the exception. iVerify closes that exception — giving security and compliance teams OS-level visibility, detection, and response mapped to the frameworks they're already accountable to.

This mapping is intended to help compliance and security teams evaluate how iVerify's capabilities support existing control frameworks. It is a starting point for assessment, not a substitute for a formal audit, control validation, or legal compliance determination. Confirm control language and version currency (e.g., CIS v8, PCI DSS version) against the framework owner's latest published standard.