Security Services for Mobility

Data Sheet

Benefits

Develop a mobile strategy aligned with the IT security strategy

- Enables effective alignment of security strategies to mobile business imperatives

Ensure effective security assessment of the most critical mobile technologies

- Provides comprehensive testing of mobile devices, OS, applications, networks, and/or backend cloud infrastructure

Provide recommendations for securing mobile devices

- Provides detailed recommendations which may include either remediation techniques or solutions such as MAM, MDM and anti-tampering, or both

The benefits of an increasingly mobile workforce are undeniable. Employees can work effectively from airports, doctors can monitor their patients without an office visit, and we have instant access to everything from banks, to shopping, to endless entertainment in our pockets.

The importance of data security has been well understood by global enterprises for years, yet how can security be managed effectively when data can be, literally, anywhere in the world, and on devices that the business does not own? And for mobile platform and application developers, how can you demonstrate appropriate security design and implementation to your customers and prospects?

Cisco Security Services help organizations secure their complex mobile environments in a comprehensive manner. Depending on the need, this can include development of strategic and operational strategy or might entail a mobile device, operating system, or application assessment. For some this may also include technology selection and development of a security model for connectivity to backend networks or cloud infrastructures. Our experts have years of experience and proven methodologies to help protect critical business data by enabling secure mobility.

Mobile Application Assessment

Our experts have conducted hundreds of mobile application assessments for both enterprise customers and mobile application independent software vendors (ISVs). Our consultants test mobile applications using a combination of public, commercial, and proprietary tools, to evaluate the application for a range of security vulnerabilities.

We take advantage of a live test environment and source code, if available, to demonstrate the effects of real-world threats, and thereby test the efficacy of the deployed application's security posture. This service includes specialized tools and techniques that target applications deployed on mobile devices, including the Apple iPhone, Google Android platform, RIM Blackberry, and Qualcomm BREW devices.

Mobile application assessments provide the kind of thorough results that are only possible through an independent and expert code review. The consultant can often maximize results by identifying programming patterns and security-risk routines that propagate vulnerabilities through an application. This information allows you to proactively address security concerns before the vulnerabilities occur. These assessments can be conducted to varying levels of depth, from focusing only on the most security critical portions of your application, to extremely thorough testing providing the highest degree of assurance for your most critical applications.

Mobile Device Security

Mobile Device Forensics: Cisco Security Services provides mobile device incident response and forensic services to investigate possible fraud, misuse, or sophisticated cyberattacks. We evaluate data stored on a device, including data that may have been deleted but not entirely destroyed, and collect forensically sound details on information accessed and activities performed.

Our services also extend beyond traditional post-incident analysis. We can work with you to create practical, actionable response plans, approaches for monitoring and logging, and e-discovery compliance strategies that can result in significant time and cost savings when mobile device breaches occur.

Mobile Firmware and OS Code Review: Mobile device firmware and operating systems are highly complex yet relied upon by consumers and enterprises alike to provide the baseline security and privacy protections they expect. Using low-level code review and device-based security testing, our mobile security experts help identify core security issues.

We recommend actionable remediation to ensure that the base devices, and operating systems running on them, are secured. This enables device manufacturers and OS providers to safeguard their intellectual property, maintain the device and operating system experience they desire, and protect their customers' information and privacy.

Mobile Strategy and Policy Management

Finding the right balance between control and agile adoption of emerging mobile technologies is a challenge. Mobile security strategy is built on coordinated development of both long-term and more tactical security approaches. It also crosses into technology selection, mobile application architectures, and protection of data in mobile and cloud computing contexts.

An essential element of an effective strategy is the determination of "Bring Your Own Device" (BYOD) and associated policies required to govern how corporate data is handled on personal devices. Cisco helps enterprises across multiple industries with an intelligent approach to building these strategies to manage mobility-related risks.

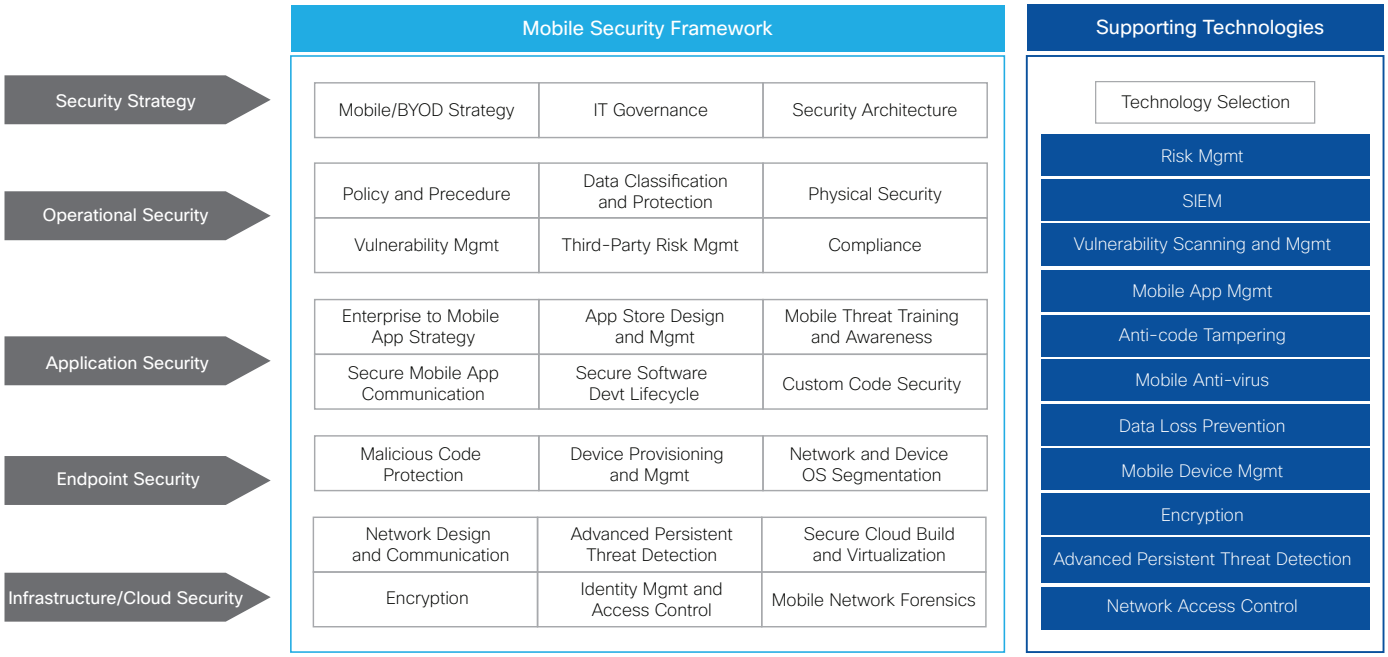
Mobile Security Framework Assessment

There are many layers to secure mobility; some areas require brand new approaches or technologies, and some simply require updates to current policies or operations. Add BYOD to the scenario of various devices, operating systems, applications, connectivity, and back-end systems and the complexities deepen as seen in Figure 1.

Using the Mobile Security Framework allows us to assess your ability to provide a secure mobile environment, and to help you develop a roadmap to address any gaps in a planned and budgeted way.

Security Services for Mobility

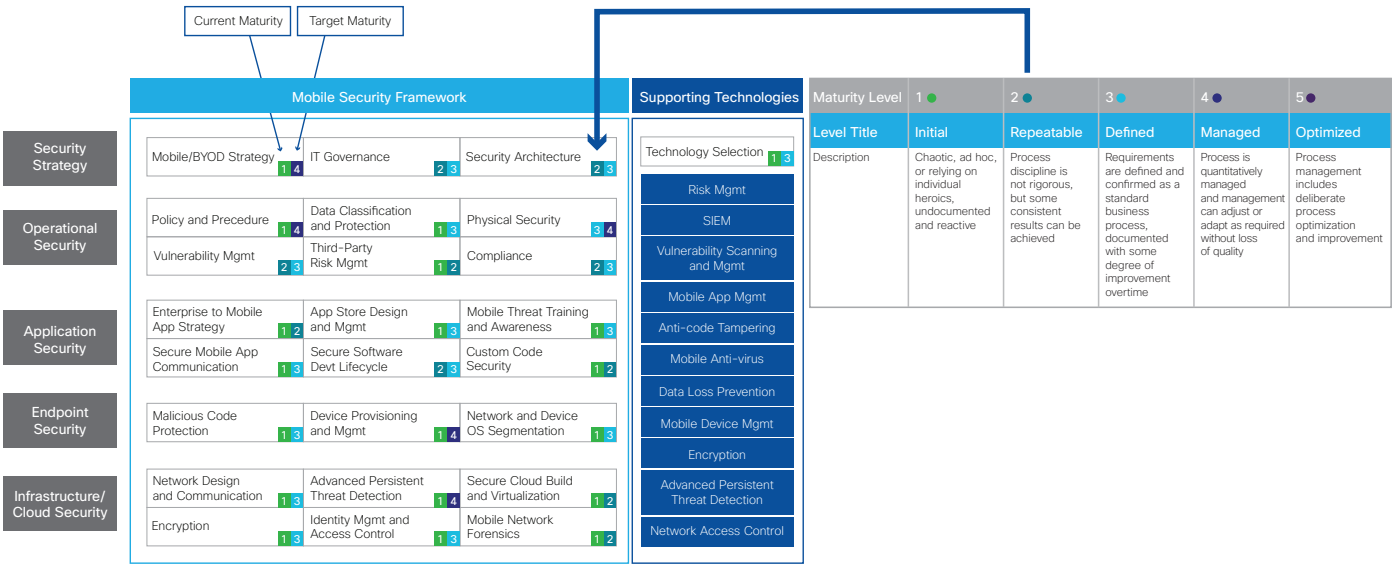
Figure 1 Mobile Security Framework



A Mobile Security Framework Assessment (Figure 2):

- Aligns IT security strategy to business growth and productivity objectives
- Effectively ties mobile strategy to tactical plans for application use, infrastructure, policy, emerging threat management, and technology investment
- Provides an efficient assessment of current mobile and cloud-related risks and opportunities
- Assesses maturity against a five-point scale to enable clear communication of current and future state
- Provides a baseline to measure future progress or to be anonymously benchmarked against other similar organizations

Figure 2 Mobile Security Framework Assessment-Sample Deliverable Graphic Shows Current and Target Maturity in Each Critical Area



Security Services for Mobility

Data Sheet

Mobile Security Strategy Workshop

A Mobile Security Strategy Workshop provides a review focused on selected areas of the broader Mobile Security Framework. The workshop allows an organization to benefit from a quick, high-level review to identify gaps in mobile business strategy and supporting policies.

The Mobile Security Strategy Workshop consists of three phases:

1. **Workforce Survey:** Identifies attitudes and expectations concerning mobile technology use in the enterprise
2. **Strategy Workshop:** Measures current and target state maturity against the Cisco Mobile Security Framework
3. **Final Report and Executive Summary:** Defines a strategic and tactical roadmap for achieving desired maturity

A Mobile Security Strategy Workshop enables an enterprise to:

- Support mobile business productivity goals and align IT security strategy
- Capture workforce attitudes toward, and expected usage of mobile technologies and applications
- Have an expert-facilitated assessment of their maturity against the Mobile Security Framework
- Measure data protection and IT compliance readiness for the client's mobile enterprise
- Identify gaps with mobile business strategy and supporting policies
- Define strategic and tactical roadmaps for an evolving security program to better support current and future business models

Full Suite of Services

Cisco Security Services has a broad suite of services to support the security and risk management needs of global enterprises and the technology and service providers that support them (Figure 3).

Figure 3 Broad Range of Cisco Services

Security Strategy	Application Security	Mobile Security	Cloud Security	Risk Management and Compliance	Infrastructure Security
• Security strategy • IT governance • Security program development • Policy development	• Secure application design • Threat modeling • Application assessment • Enterprise SDLC • Code review • Developer training	• Mobile and BYOD strategy • Mobile application design • Mobile application and device assessment • Mobile security framework assessment • Mobile SDLC • Social media application assessment	• Cloud computing strategy • Cloud compliance • Cloud application assessment • Virtualization security and architecture • Secure cloud application deployment • Cloud infrastructure assessment	• PCI DDS and PA DDS • ISO 27001 and 27002 • HIPAA and HITECH • GLBA and FFIEC • Third-party risk • IT and security risk assessment • Vulnerability management program development • Incident response and forensics	• Network design review • Network security assessment • Penetration testing • Social engineering • Physical security assessment

Strengthening Cisco Security Solutions

The acquisition of Neohapsis allows Cisco to deliver even stronger security solutions to help customers address complex security challenges in the dynamic threat landscape.

Learn More

For more information visit www.cisco.com/go/securityservices.

DEC 15CS4756 04/15