Data Sheet

Symantec™ Mobile Security Assessment Suite

Mitigate the risks of enterprise adoption of today's mobile technologies

"[E]mployees increasingly want to take advantage of the productivity- enhancing characteristics of smart-phones and tablets. And, not surprisingly, they want to use their personal mobile devices while at work. This puts consi-derable pressure on organizations to institute comprehensive mobile computing device usage policies [and security controls]—which they often do too late."

John Soat
InfoSecurity Professional
Issue #14, Volume 2, 2011

The use of mobile technologies such as Android devices, the iPhone, and the iPad within the enterprise create a unique set of challenges that must be addressed in order to ensure that sensitive information accessed, stored, and/or transmitted by these devices is properly protected. These challenges have many organizations wondering:

- *How do I manage the transition of mobile devices from "a consumer device on the enterprise network" to "properly managed and protected endpoint"?*
- *How do I increase the productivity of employees and recruit top-level talent whom expect to leverage new technologies in the workplace?*
- *How do I measure and manage the risks associated with adoption and use of emerging mobile technologies?*
- *What do I need to do to prepare IT and Information Security teams to become enablers of these emerging technologies?*
- *How should I address the risks inherent in allowing personally owned mobile devices to access corporate applications, systems, and data?*
- *How do I ensure that the mobile applications created by our development teams are highly resistant to common attack vectors and do not create unacceptable risks for our customers or for the company?*

Overview

The Symantec Mobile Security Assessment Suite evaluates the capabilities of your information security program to address the unique challenges inherent in the deployment and use of emerging mobile technologies. These services evaluate security exposures from multiple perspectives: external attackers, malicious internal users, and unaware employees attempting to exploit vulnerabilities in mobile platforms and mobile applications. These assessments identify both vulnerabilities and threats to applications and infrastructure as well as gaps in your organization's policies, process, or standards.

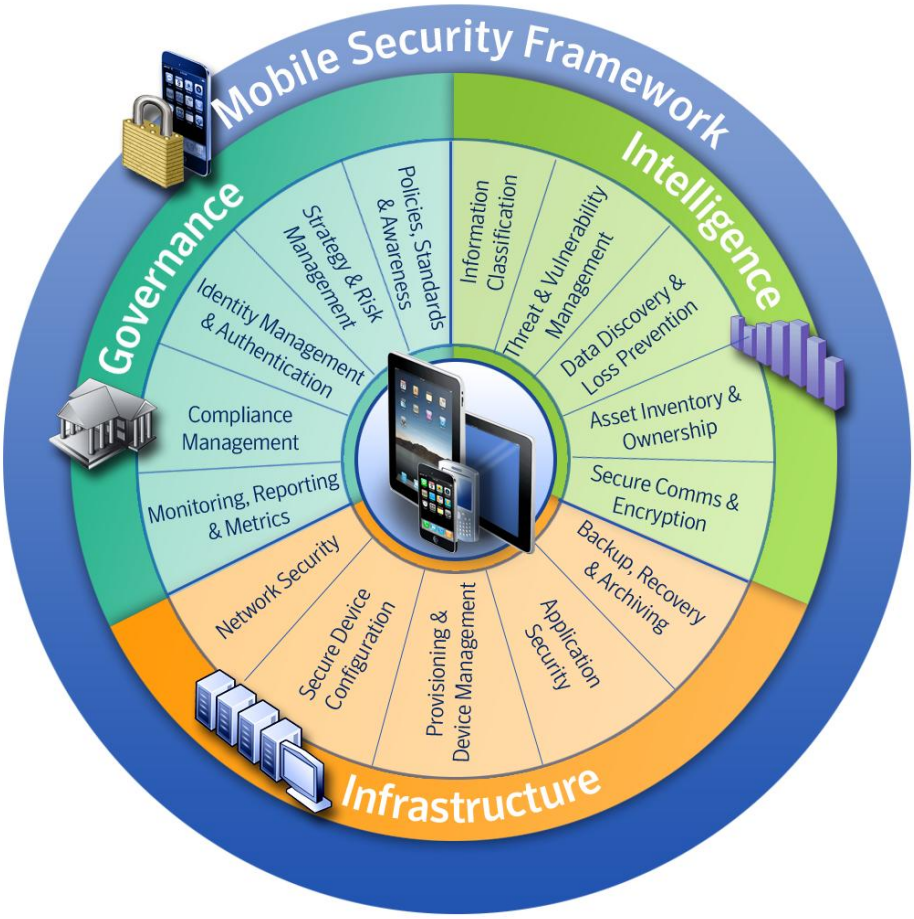
Symantec leverages its extensive knowledge base and deep technical and operational skill sets to examine the issues and challenges unique to the security and management of mobile technologies and the information these devices store and access. At the completion of an assessment, Symantec consultants provide a detailed report with strategic and tactical recommendations for secure deployment of a heterogeneous mix of mobile devices and for development of enhanced defenses against mobile threats and vulnerabilities in the enterprise.

Symantec™ Mobile Security Assessment Suite

Using a well-defined methodology and the Mobile Security Framework, Symantec consultants:

- Provide a holistic assessment of mobile security capabilities and effectiveness
- Identify strengths and weaknesses of your current approach to mobile security
- Assist with the development of a strategic roadmap for secure adoption, integration, management, and use of mobile technologies

Symantec developed the Mobile Security Framework to facilitate discussions about the various elements of your information security program that must be considered when preparing for use of emerging mobile technologies in the enterprise. As can be seen in the following figure, the Symantec Mobile Security Framework leverages an information centric approach to mobile security based on three major focus areas: Mobile Security Infrastructure, Mobile Security Intelligence, and Mobile Security Governance. These are divided into fifteen elements that apply to one or more of the focus areas to provide a holistic picture of mobile security across the organization.



Mobile Security Assessment

The Symantec Mobile Security Assessment evaluates the level of risk inherent in your organization's use of mobile computing devices, such as the Apple iPhone, iPad, or Android phones and tablets. The assessment provides an understanding of present or anticipated exposure to information security risk likely to result from gaps within the information security program based on mobile device use cases and available security controls. The service is designed to support

Symantec's broad security footprint includes:

- Services engagement with 95% of Fortune 500
- Extensive services engagements each year across Americas, EMEA, APAC, Japan
- Manage security devices in over 70 countries
- 1800 analysts, 6200 managed security devices
- 40,000 registered sensors in over 200 countries
- Over 25,000 vulnerabilities in the Symantec vulnerability database
- 120 million threat and virus submission systems

enterprise executives by evaluating, prioritizing and managing their portfolio of security controls against the unique risks inherent to use of emerging mobile technologies in the enterprise and to assist with planning for effective and secure deployments of these emerging technologies.

Using a well-defined methodology, Symantec consultants provide advice in the context of your requirements for mobile device support. Symantec leverages its extensive information security knowledge base to examine specific areas of control design through structured interviews, documentation reviews, and focused workshops conducted with both business and technical stakeholders.

Data gathered is assessed against our best practices for secure enablement of mobile technologies across all of the elements included in the Mobile Security Framework. At the completion of a Mobile Security Assessment, Symantec delivers a written report which includes an executive summary, showing the high-level analysis and findings, a scorecard illustrating the organization's mobile security readiness in each of the elements included in the Mobile Security Framework, detailed findings and recommendations for each element in the model, and prioritized action plans for closing any gaps that may exist. A sample scorecard is illustrated below.

Symantec Mobile Security Capability Scorecard	Apple iOS	Android	Blackberry/RIM	Windows Mobile	Desired Score
Mobile Information Governance					
Security Policies, Standards, & Awareness					
Security Strategy & Risk Management					
Identity Management & Authentication					
Regulatory Compliance Management					
Monitoring, Reporting, & Metrics					
Mobile Information Intelligence					
Information Classification					
Threat & Vulnerability Management					
Data Discovery & Loss Prevention					
Asset Inventory & Ownership					
Secure Communications & Encryption					
Mobile Information Infrastructure					
Network Security					
Secure Device Configuration					
Provisioning & Device Management					
Application Security					
Backup, Recovery, & Archiving					

Symantec™ Mobile Security Assessment Suite

- **How do I test mobile apps for security vulnerabilities and privacy concerns?**
- **How do I ensure 3rd-party apps do not introduce security vulnerabilities?**
- **How do you manage application security across varying platforms?**
- **How do I ensure mobile apps protect data and privacy while meeting customer demands?**

Mobile App Security Assessments

Mobile app penetration assessments test the ability of selected mobile applications to resist local exploitation as well as remote attacks originating from the Internet, carrier networks, and Bluetooth connections from the vantage point of both unauthorized and valid users. These assessments are conducted with the intent of identifying and exploiting vulnerabilities in application interfaces, existing security mechanisms, and other related services in order to gain control of the mobile device or the data stored on or transmitted to or from the device.

Symantec Mobile App Security Assessments evaluate the security of an organization's custom mobile applications against best practice criteria for mobile application security. By simulating real-world device operating system and application-level attacks, the tests provide insight into the ability of an organization's mobile applications to resist attacks from unauthorized users and to help prevent misuse by valid users.

As part of the testing, Symantec consultants gather and review available information about mobile software design, the interaction of the application's components, and security architecture. Testing can be performed onsite, or remotely via the Internet depending upon the desired approach. Consultants assess a variety of attack vectors such as Data Validation, Session Management, Access Control, Cryptography, Third-Party Components, Administration, Communications Security, Deployment Configuration, Error Handling, Network Level Access Controls, Password/PIN Length and Complexity Requirements, Data Privacy, and Session Management.

History and Experience in Security Assessment Services

Symantec is the global leader in information security, and through its acquisition of @stake in late 2004, has become the leader in network and application security and third party security assessments. Taking a solution approach Symantec Advisory Services can help you find the right combination of services for your unique requirements.

Symantec understands one of the biggest challenges that organizations face today is how to balance the operational demands for information availability with the need to adequately protect that information from unauthorized disclosure. By engaging in a Security Assessment, organizations will gain invaluable insight and visibility into their current security risks, and may proactively manage that risk in a coordinated approach.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.