HOW TO BUY A MOBILE

SECURITY SOLUTION

Lookout

Icons used in this book

Throughout this book, you'll find special call-outs to direct your attention to important information. Here's a key that explains what the icons mean:

THE DATA

The data that you'll see throughout this book is the result of a survey commissioned by Lookout and conducted by Enterprise Strategy Group, an integrated IT research, analyst, strategy, and validation firm.
The survey methodology includes:

- 150 completed online surveys with IT and security practitioners directly involved in the planning, implementation, and/or operations of their organization's mobile endpoint security and threat detection policies, processes, and/or technical safeguards
- Enterprise organizations (2,500 or more employees) in United States and enterprise organizations (1,000 or more employees) in United Kingdom
- Multiple industry verticals including financial, business services, manufacturing, and retail

Ways to learn more:

This icon means you can access another document on the topic.

This icon means you can watch an on-demand webinar on the topic.

This icon means there is a post on the Lookout blog covering the topic.

This icon will link you to more information in another part of this book.

This icon means definitions for technical terms are below.

THE EXPERTS

Craig Shumard, CISO emeritus

As Cigna Corporation's former Chief Information Security Officer, Craig developed and oversaw the implementation of a 21st century, corporate-wide strategy to safeguard information involving more than 65 million Cigna customers. He is currently a trusted advisor on a number of boards for prominent security companies.

Serge Beaulieu, Former Director of IT Security

Serge is a seasoned information security consultant whose experience includes being Director of Technical Security Strategy at Cigna Corporation. Serge is a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

Introduction

In this eBook, you'll learn what to do before you reach out to vendors, how to test vendors, and how to get your employees to use the solution you choose.

Want more?

"The Practical Guide to Enterprise Mobile Security" will answer all your mobile security questions. In it, you'll learn:

PART 1: What is mobile security

PART 2: Why mobile security should be in your top three priorities

PART 3: Six mobile security capabilities you need

PART 4: The business case for mobile security

PART 5: Buying mobile security (what you're reading)

PART 6: Lookout Mobile Endpoint Security

PART 7: The future of mobile security

GET THE FULL GUIDE

How to buy a mobile security solution

The purchase process

This guide is a practical plan that will help you get an enterprise mobile security solution into your organization, deploy it, and overcome employee privacy concerns to encourage adoption.

THE EXPERT

"First and foremost, ask yourself, 'does this mobile security solution solve the business problem I have?' You're not out there looking to buy security solutions to check-off a check box on some compliance list. There are real business issues associated with securing data on mobile devices."

Craig Shumard
CISO EMERITUS

Before you reach out to vendors:

Phase 1: Document your goals

Your existing business goals will drive your mobile security decisions, and make the case for launching this program.

They may include:

- Adopting more cloud applications
- Implementing a BYOD program or protecting your existing one
- Protecting brand reputation

USE THIS SPREADSHEET

Know your mobile inventory:
As part of your goal setting, it's helpful to document your mobile inventory. This includes: number of iOS devices, number of Android devices, what EMM/MDM you have, and if container technology is being used.

Use this simple Mobile Inventory Spreadsheet to document your devices and environment.

Phase 2: Establish your timeline

The question to answer is: When should these solutions be deployed?

Then work backwards to determine when each step needs to be complete:

1. Vendor demos
2. Your security team's technical evaluation of shortlisted solutions
3. Final decision from the buying committee
4. Your IT or Operations teams' integration of the solution with existing technologies
5. The roll-out together with HR, to ensure product adoption and that privacy concerns are quelled
6. Tracking to determine which employees have or have not enrolled

7. Initial analysis of threats found in your mobile fleet

8. Feedback on the product roll-out and how employees are reacting to its presence on their devices

Phase 3: Document requirements

The requirements your organization will need to meet depends wholly on the industry you service and the kinds of compliance standards you need to maintain. These standards may include PCI, HIPAA, or data transfer/storage laws in your country.

Make sure to assess capabilities beyond security, as the survey results show, ease of deployment and end-user support are among the most important evaluation criteria.

Phase 4: Identify who will buy and manage the solution

You'll want two teams, that may have overlapping members, as part of the mobile security vetting process. The first team should be the key decision stakeholders, who are likely to be the IT and security leaders up to the CIO and CISO level.

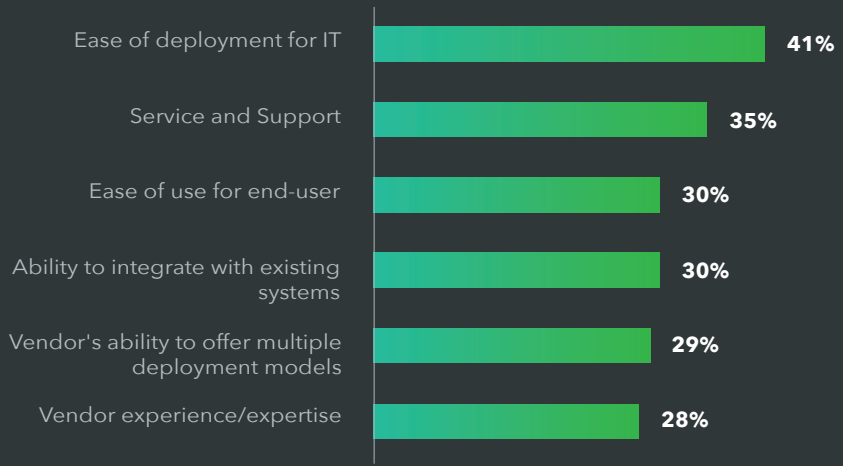
You'll also want to assemble a team of individuals who will eventually manage the solution. This might be made up of individuals on your IT, security, or operations teams. This team will be able to confirm that the mobile security solution being vetted can integrate with the existing security stack. The solution at hand should integrate easily with current solutions to reduce the cost of integration that IT, security, and ops teams naturally incur. These folks will need to be part of any technical evaluation, and will be a critical part of the enterprise-wide deployment.

THE DATA

Ease of deployment and support are key for buyers

The Question: If you were evaluating a new mobile security solution for your organization, which of the following criteria would be the most important?

The Results:



Phase 5: Assess vendors against your actual scenarios

To get the mobile security solution that's right for your company, the key thing is to get specific with each potential vendor about how they measurably reduce the specific mobile risks facing your company and industry.

Make sure you also assess:

- That the solution can integrate with your existing EMM/MDM if you have one
- The availability of support and training for your global locations
- That the endpoint app isn't a burden for end-users to adopt
- The level of effort required to deploy and manage the solution
- That the vendor can actually deliver the capabilities they promote

Focus on how each solution maps back to the business goals you documented. Try to avoid comparing checklists of features, since that could lead your evaluation away from what really matters to your company.

Phase 6: Talk with other customers

Just like a job interview, ask for customer references who can tell you how the vendor has helped them, how deployment went, and any cautionary tales.

If references aren't immediately available, ask for case studies that can educate you on real-world situations in which this technology has worked.

Here are some sample questions to ask on the call:

- What was your deployment experience like?
- If applicable: How easy was it to connect the mobile security solution with your EMM/MDM solution?
- Is the solution easy to manage on an ongoing basis?
- What is the threat detection experience like for end-users and admins?
- What is the remediation experience like for end-users and admins?
- What is your average dwell time (the time between the device encountering a threat and the moment the IT admin receives an alert)?

- What has your support experience been like?
- What feedback have you heard from your end-users?

All of these will help you confirm the solution you really need in your organization.

DOWNLOAD THIS GUIDE

Technical Evaluation Best Practices Guide: There are four stages to technical evaluation of a mobile security solution in your environment: deployment, security monitoring, threat protection, and support testing.

Get this Technical Evaluation Best Practices Guide to use as a framework for evaluating your shortlisted solutions.

Phase 7: Run a technical evaluation

There's no better way to do a technical evaluation than to deploy the solution that your team has rated the highest to a segment of your end-users – or even just your IT and security teams – to experience the solution from both the admin and user perspectives.

"People want to put an ROI to security, and I don't know that you can. What you should do is forecast the total cost of ownership over the years of the contract. Know what it costs to administer, and how that is going to be impacted by potential changes in your organization."

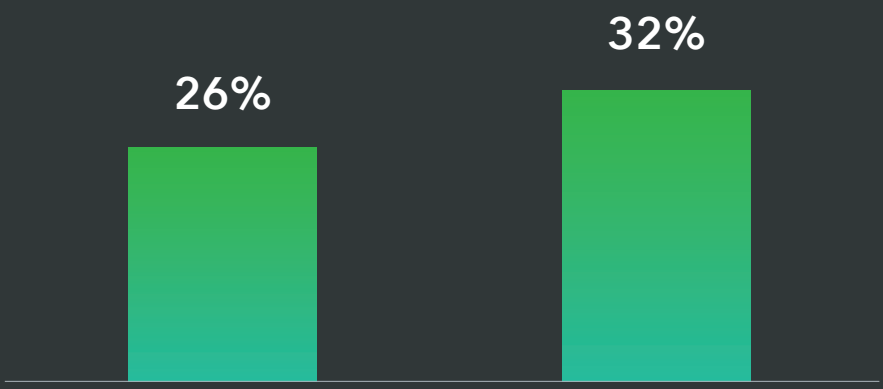
Craig Shumard
CISO EMERITUS

THE DATA

The desire for higher mobile security budget allocation

The Question: Approximately what percent of your organization's overall security budget for 2017 is, or do you expect will be, earmaked for mobile-specific security product or services? Based on how you view mobile security risk as it compares to other risk vectors (desktop security, network security, etc.) how much of the overall security budget for 2017 do you feel should be allocated to mobile-specific security products or services?

The Results:



% of overall security budget allocated, or which will be allocated, to mobile-specific products/services in 2017

% of overall security budget you feel should be allocated to mobile-specific products/services in 2017

Responses from this survey indicate that IT & security leaders think mobile security should be an even larger part of the overall budget.

Phase 8: Cost considerations

Several recent surveys indicate that mobile security is growing as a percentage of the overall security budget.

Another recent survey by the Ponemon Institute indicates that mobile security budgets could be expected to rise 37%[1] to in the next year.

Regardless of your budget, there will be a variety of factors specific to your organization that will drive the cost of your purchase. Consider the following when you're negotiating with a mobile security provider:

1. How many employees do I have? Many times you'll need to consider pricing by the number of "users" for whom you may be purchasing licenses as each employee could be using more than one mobile device to access corporate assets. This style of pricing is most relevant to companies with a bring-your-own-device policy.

2. How many devices do I manage? Some mobile security vendors may sell licenses based on the number of devices. This is most relevant to organizations with a corporate-owned-personally-enabled policy.

3. A mix. Many large organizations have a mix of corporate-owned and, BYOD devices, some of which are managed via an MDM and others that are not. If this is the case for your company, use the Mobile Inventory Spreadsheet to make sure you get the precise number of licenses you need.

Phase 9: Make a decision

Now is the time to assemble your buying committee, make your final business case, confirm that the solution works, is easy from an IT administrative perspective, and the finance team approves the costs and contract terms.

[1] https://info.lookout.com/ponemon-report.html

Phase 10: Deployment

There are two main ways to deploy a mobile security solution. The first, and most common is to use an MDM solution, such as Microsoft Intune, VMware AirWatch, or MobileIron as the deployment mechanism for the mobile security endpoint app.

If your company hasn't invested in EMM/MDM because you have a BYOD policy (or any other reason), then deployment will come in the form of an email to employees that includes a download button and a unique code to access and activate the endpoint app.

However, before you physically deploy a mobile security solution to a global workforce that can number in the tens of thousands, you have to plan for two things:

1. Your mobility policies
2. Employee education & internal communication

Your mobile security policies

Your organization will need to have policies based on your risk tolerance and the types of data you collect and store. This could include data from your product, data from your customers, and data from your employees. All three should be taken into account when setting up policies.

Mobile security policies may include "if, then" statements, such as:

- If a malicious or non-compliant app is present on the device, then block device from accessing corporate applications or services, such as email
- If an app accesses "contact information," then flag it as a "non-compliant app" to the end-user and admin – do not block access, unless other remediation instructions are set by the admin
- If a device connects to a malicious Wi-Fi connection, then block traffic from the device to corporate servers

In addition, take time to understand what really makes your company nervous. Are you uncomfortable with employee information being sent to servers outside your country? What defines a "non-compliant" app for you?

Employee education: encouraging adoption

Internal communication is very important during a global roll out, especially if your company primarily relies on employees using their own devices at work.

Employees will want to know:

- Are you watching what apps I download?
- Are you monitoring my browsing?
- How are you protecting my privacy?
- Do I need this security app on my phone?

Communicate to your employees that this solution is intended to protect their device and data just as much as it is intended to protect enterprise data.

THE EXPERT

"If it's not adopted by your users, it just won't work, and the only way it's going to get adopted is if you respect the individual's device and their data. You have to respect your end-users' privacy and communicate that to them."

Serge Beaulieu

FORMER DIRECTOR OF IT SECURITY

As far as privacy is concerned, your internal communication should clearly state that the security app is just for threats on the device, not YouTube habits. For example, the solution will be used to determine if the phone was compromised during a trip abroad to a "high-risk" country, or, more generally, if it connected to unsafe Wi-Fi.

The solution will warn them just as quickly as it will warn the admin to make sure everyone stays safe.

Finally, the bottom line is that, yes, they will need it on their phone. If they want to conduct business on their device, it's important that they are not an easy target that compromises your overall security posture.

Contact us

www.singlepointoc.com

About Single Point of Contact:

Single Point of Contact is a managed security service provider dedicated to helping businesses implement the right IT security solution. While we understand there are plenty of components in security, we will work with you to ensure you completely understand the advantages of the product or service you are considering for your firm. Our goal is to help customers reduce risk, respond to threats faster, achieve compliance and ensure data is secure. For more information on our services and how we can help avoid costly mistakes, **contact us** today.