# Smart Devices, Smart Security

## Five tips to consider in a data security strategy for smartphones and tablets

CSO
Custom Solutions Group

Voltage security

If there are any lingering doubts that mobile devices—such as smartphones and tablets—have profoundly transformed today's business, one study finds that using smart devices for productivity is "now the standard."[1] Most organizations are now commonly making line-of-business applications accessible from mobile devices.

Once mostly prohibited by IT, smartphones and tablets—such as Android-based phones and Apple iPads—are now being used by hundreds of millions of employees worldwide to access, transmit and store corporate information in today's 24x7 business environment. This "extended enterprise" introduces new challenges and complexities for IT. Not surprisingly, security has emerged as the No. 1 challenge posed by the BYOD ("bring your own device") trend.[2] When it comes to rogue smartphone and tablet use, IT organizations are concerned with device loss, data leakage and unauthorized access to corporate resources. Similar concerns have been raised about the growing use of "guest access" to corporate networks.

In response to these perceived risks, organizations have begun implementing a range of data security measures. Traditional approaches involve perimeter-based security controls such as firewalls and smart screen filters. But no amount of perimeter defense can protect data accessed by and subsequently stored on and transmitted by smartphones and tablets, especially outside of enterprise control.

### FIVE THINGS TO KNOW ABOUT MOBILE DATA SECURITY

Even as security threats loom, informed organizations have an advantage. These five tips can make or break mobile data security efforts:

**1. It's all about securing data.**

In an ideal world, sensitive data travels in well-defined paths from data repositories to a well-understood set of applications. In the real world, however, data travels everywhere, anytime, with constantly shifting applications running on an evolving set of platforms. The data lifecycle is often complex, extending beyond the container and the application—even outside the enterprise into offsite backup services, cloud analytic systems and outsourced service providers. Not to mention the onslaught of user-owned devices making their way into the fold. So although armoring applications and devices is one dimension in establishing a defensive posture, it isn't the entire answer—nor is the installation of security solutions from a wide range of vendors. There will be security gaps that eventually impede enterprise risk management and user productivity. Rather, data security is a multi-

**Data security is a multi-pronged risk challenge that requires a data-centric approach across all dimensions.**

pronged risk challenge that requires a data-centric approach across all dimensions.

### 2. Assume you've been breached.

That's the unsettling opinion of Shawn Henry, the U.S. Federal Bureau of Investigation's top cybersecurity officer. Henry, who recently left the FBI, told The Wall Street Journal that current approaches to fending off hackers are "unsustainable."[3] FBI agents increasingly come across data stolen from companies whose executives had no idea their systems had been accessed. "We have found their data in the middle of other investigations," he told the Journal. "They've been breached for many months, in some cases years, which means that an adversary had full visibility into everything occurring on that network, potentially." The challenge is only compounded by the proliferation of smartphones and tablets. Henry said companies need to make major changes to avoid further damage to national security and the economy.

### 3. You don't need an entirely separate strategy to protect your mobile data.

Mobile devices are endpoints that require the same attention that is given to PCs and laptops. Many of the same processes and policies that are leveraged for PCs and laptops are applicable to mobile platforms. Still, mobile devices are built for connectivity; the personal nature of these devices, combined with the inability to regulate or monitor user activity, means that the focus of protection must change. Simply adding another "point solution" isn't the answer. Enterprises need to make mobile data security part of their risk management strategy—consistent with desktop and laptop security—without compromising the user experience.

### 4. You don't have to forfeit usability for security.

The primary purpose of smart device adoption is to improve productivity for a geographically distributed and highly mobile workforce. Security mustn't be a barrier to productivity. Still, current mobile security solutions focus on creating boundaries within the devices on which data can be stored and accessed. When encryption is used, it's typically non-user-friendly, non-application-specific and lacks granular policy controls. Additionally, it usually relies on a traditional key management approach that requires massive investment to scale in today's environment. Security for mobile data must be as transparent as possible without losing effectiveness, and it must not intrude on familiar user experiences—yet it has to provide IT with the control it needs in order to ensure security at the data level.

### 5. Compliance doesn't equal security.

Compliance relevant to IT systems is now being extended to mobile devices—and for very sound data risk reasons. Companies must understand how these same data privacy, regulatory compliance and risk management practices should be applied to the mobile and cloud platforms. But being certified compliant or using solutions that help achieve compliance doesn't always translate into effective data security. For example, a desktop computer stolen recently from a California health care organization was password-protected but unencrypted. The theft potentially exposed the personal information of nearly four million patients.[4]

## THE "DATA-CENTRIC" APPROACH TO MOBILE SECURITY

As the adoption of mobile devices and apps continues to grow dramatically, one of the biggest challenges for enterprises has been to protect and manage the native apps and data of these devices. Over the years, companies have taken numerous approaches to mobile security. These have ranged from banning such devices altogether from the corporate network to remotely "wiping" corporate data in the event of the loss or theft of a device, to adopting a "container" approach to protect mobile apps and data. None of these approaches is satisfactory.

In a data-centric approach to mobile security, data (both structured and unstructured) is encrypted as soon as it's acquired. It remains encrypted as it is used, stored or moved across

## Case Study: Mobile Data Security Done Right

**Among Voltage Security's customers is a bank that uses encrypted e-mails to deliver documents containing sensitive data via mobile devices; those users can then decrypt and read the communications on their own mobile devices. The secure e-mail application enables consistent customer engagement and user experience across mobile and desktop systems. Customer service representatives are also able to accelerate the mortgage initiation process while protecting sensitive data.**

**From the outset, the bank faced steep challenges. It wanted to take advantage of new business relationships with customers by extending its brand to the mobile channel. That meant that data privacy mandates and regulatory compliance needed to be efficiently addressed. There was also a company mandate to "go green" by reducing reliance on paper.**

**The result is a fully compliant solution with quick ROI that fully engages the bank's mobile customers, who prize quick access to their financial information.**

data centers, public and private clouds and devices, to be decrypted only by the intended party. The goal is to devalue or "kill" data, so that even in the event of a breach, the encrypted data will have no value to cybercriminals. And data is protected without disruption of user productivity. All of which was tricky to achieve prior to recent data security innovations.

As Forrester Research observed in its "Killing Data" report of January 2012, "The advent of the extended enterprise and the ease of accessing corporate information anytime, anywhere, and on any device will create new pressures on security teams to encrypt data. Mobile devices are easy to lose and easy to steal. Enterprise-level encryption is the best hope for securing data on these devices."[5]

## PROTECTING DATA, FROM MAINFRAME TO MOBILE

Advances in encryption make it possible to combat new security threats by protecting data wherever it is used in the ever-changing IT landscape, whether in mainframes, desktops, public and private clouds or mobile devices. Technologies such as Identity-Based Encryption (IBE) and Format-Preserving Encryption (FPE) render sensitive data useless to criminal hackers, insider threats and data leaks.

The challenge in achieving this vision is twofold: to protect data at scale across millions of endpoints without increasing costs or end user complexity; and to do so within existing workflows, systems and applications—even down to the fields and data elements that attackers can access if they are not protected.

IBE enables stateless key management, so private and public keys can be generated dynamically, derived from existing identity information such as e-mail addresses. Layered with dynamic authentication, this helps organizations quickly and easily scale protection to secure data to and from mobile endpoints, desktops, servers and the cloud.

FPE provides strong, standards-based protection of structured data—such as credit card or Social Security numbers—without changing the format or structure of the data. This avoids disruption to workflows, systems and applications so that business productivity is preserved while the data is rendered useless to attackers.

Of course, one size does not necessarily fit all organizations. So with sensitive data distributed on millions of endpoints, the right technology needs to be available for the most appropriate use case.

In the end, a data-centric approach to mobile security that leverages innovations such as IBE and FPE offers the following key benefits:

- End-to-end encryption ensures that sensitive data is protected from inadvertent data loss as well as direct attacks—encrypted data is useless to hackers without the ability to decrypt or access keys.
- The compliance regulation scope is reduced by removal of sensitive data from business/merchant systems and applications—thereby also reducing costs of compliance.
- The impact on the user experience is minimal; encryption functionality is built into the application experience, which is familiar to the user and transparent to existing applications.
- Solutions built upon these technologies are nondisruptive to existing IT and business systems and extremely scalable, and they don't require key management overhead, costly servers and dedicated staff. In fact, they integrate well with existing systems, thereby extending the value of these investments.

## DATA-CENTRIC MOBILE SECURITY IN THE REAL WORLD

Every day, more and more sensitive business data is being accessed by mobile devices. Here are the three mission-critical areas in which a data-centric approach can be used to protect mobile data and the business without disrupting user productivity:

- **To protect e-mail communication that contains sensitive information and is subject to regulatory compliance.** In 2011 Forrester Research gave e-mail the No. 1 position in smartphone applications. So it's no surprise that a transparent approach to e-mail encryption is highly sought after to enable enterprises to see immediate benefits from their smartphone users—while complying with strict industry regulations. For example, the use of smartphones presents a terrific opportunity for organizations to engage their customers in real-time dialogue—whether a private electronic statement is delivered with an offer to subscribe to a new financial service or an insurance agent engages a new customer with electronic, on-the-fly enrollment.

- **To protect sensitive business data and files.** Protecting sensitive data in files, databases and applications is becoming an even bigger challenge for enterprises with the adoption of cloud storage for streamlined collaboration. The natural pairing of smart devices and cloud services puts more sensitive data at risk today. A data-centric approach protects unstructured and structured data, from the cloud to the mobile device. For example, enterprises that have adopted BYOD need the ability to securely store files in a private or public cloud and yet make them accessible and readable to mobile devices within the enterprise—and sometimes by external business partners. Only the mobile devices with policies provisioned by IT can decrypt the data.

- **To protect transaction data captured by new mobile payment methods.** New mobile payment methods are popping up all the time—whether it's customer self-service or associate-enabled payment devices that let customers skip the checkout counter. Any system touching payment data is the most popular target for hackers and subject to PCI compliance regulation.[6] To protect payment data, it must be encrypted at the card swipe—whether it's a mobile device with a card swipe attachment, a point-of-sale terminal or the Web—and remain encrypted until it reaches the processor, where it can be decrypted and processed. Given the steady proliferation of mobile payment devices, protection for payment transactions from the point of capture to authorization, settlement and beyond is a must. Otherwise, the sheer amount of payment transaction information flying through the air unprotected becomes a gold mine for hackers.

Any system touching payment data is the **most popular target for hackers** and subject to PCI compliance regulation.

## TAKE ACTION NOW

Mobile devices aren't going away, and BYOD and "the consumerization of IT" aren't fads. These trends are quantifiably improving corporate agility, but the security risk is real.

Traditional security approaches lock down the infrastructure, but that's not the target for today's cybercriminals. They want sensitive data, which is valuable; easily monetized; and increasingly on the move, into and out of IT infrastructures. And they fully understand where and when to find "data in the clear," when it's most vulnerable, and they're willing to wait.

But waiting is one thing you can't afford to do. Implementing a data-centric approach to mobile security with encryption helps keep sensitive data safe wherever it goes, however it is used and throughout its lifecycle. Ultimately, it mitigates the risk of data breaches and other threats so mobility can be leveraged to its fullest potential. And isn't that the goal of any security measure?

To learn more about Voltage Security data-centric approach to protecting mobile data, go to **voltage.com/mobile.**

**Sources**

[1] "Consumerization of IT Study," CSO, October 2011

[2] "Consumerization of IT Study"

[3] Devlin Barrett, "U.S. Outgunned in Hacker War," The Wall Street Journal, March 28, 2012

[4] "Healthcare Breach Exposes Nearly 4 Million Patients' Data," InformationWeek, November 18, 2011

[5] John Kindervag, "Killing Data," Forrester Research, January 30, 2012

[6] "2012 Data Breach Investigation Report" from Verizon