Government Business Council

Mobile Security in the Changing World of Government

April 2024

Sponsored by

verizon

Pixel for Business

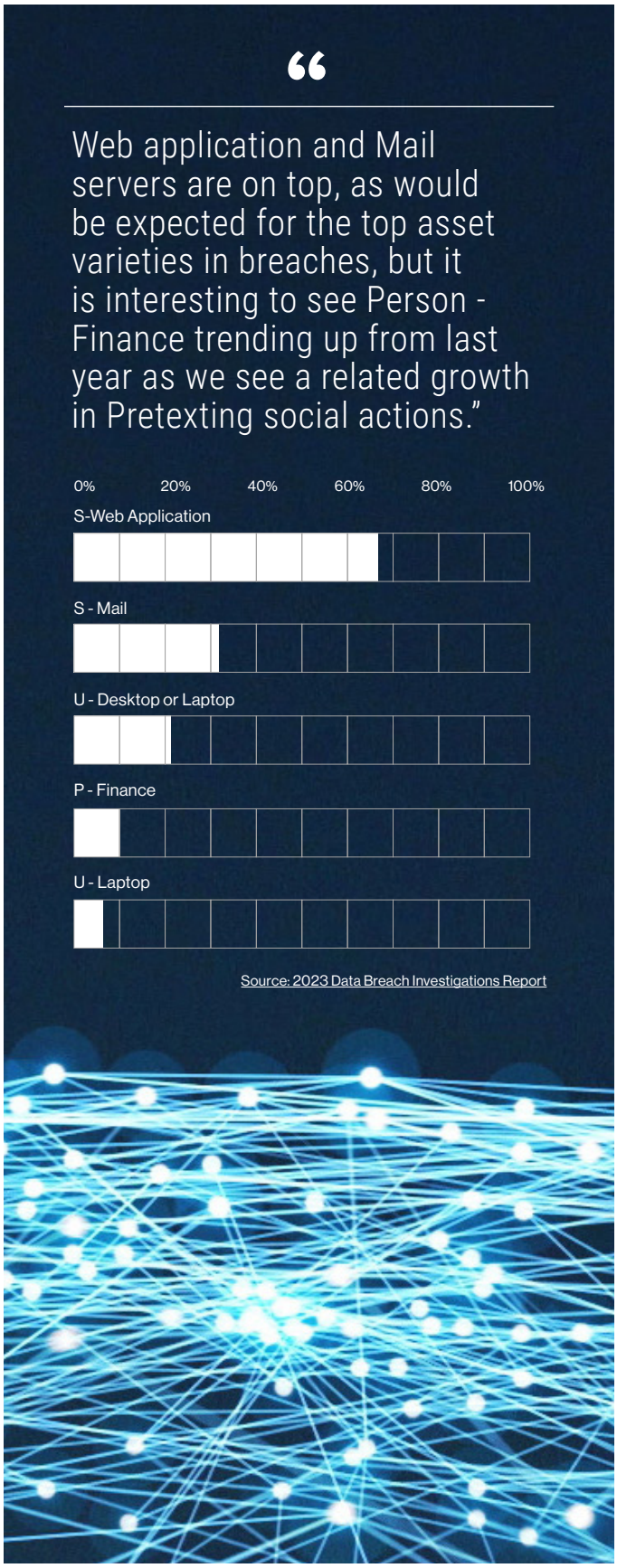
INTRODUCTION

As mobile device use has increased, so has data sharing across these devices. There are an estimated 7 billion smart mobile device subscriptions worldwide in 2024. Specifically within the federal government, there are over 600 thousand government-issued mobile devices — the Department of Defense (DoD) alone uses 550 thousand of those mobile endpoints. Mobile device usage among U.S. government workers has increased due to federal, state, and local agencies shifting to more flexible work and hybrid models, as well as additional powerful mobile technology enabling new types of work at the edge.

With mobile device technologies becoming more sophisticated, the potential for cyber-attacks increases. Those attacks are also more sophisticated and more difficult to prevent. Spam, phishing, malicious apps, and ransomware are just some of the common cyber threats that mobile device users face. The most common mobile security threats are application, web, network, and device-related. In 2023, the Verizon Data Breach Investigations Report (DBIR) states:

- **83%** of breaches involved external actors
- **74%** of breaches involved the human element
- **50%** of all social engineering attacks are pretexting incidents

Given these statistics, there are a variety of baseline security considerations and best practices that will set federal, state, and local organizations up for success when deploying a mobile fleet.



MOBILE PLATFORM SECURITY

Mobile platforms are an attractive attack vector due to the types of systems and data they have access to and because they are carried everywhere, they are more physically capable of being accessed at all times. A security-by-design approach has proven to be an effective way to deliver that security solution. Government agencies should evaluate a mobile platform’s security based on:

- Hardware-backed security
- Operating system security
- Network security
- Application security
- Security updates and patches

Hardware-Backed Security

When it comes to day-to-day business operations, securing data at the hardware level is a fundamental part of an agency's security posture. Hardware-backed security ensures that the silicon chips that make up the device are designed and implemented in a way that ensures protection for sensitive operations such as cryptographic processing.

When evaluating a mobile hardware platform, agencies should consider the following capabilities:

- Physical and/or logical separation of security subsystems
- OS booting security & integrity and frequency of security updates
- Encryption and key management solutions
- Device memory safety

Operating System Security

When it comes to day-to-day business operations, securing data at the hardware level is a fundamental part of an agency's security posture. Hardware-backed security ensures that the silicon chips that make up the device are designed and implemented in a way that ensures protection for sensitive operations such as cryptographic processing.

When evaluating a mobile hardware platform, agencies should consider the following capabilities:

- Root detection and kernel protection
- Mandatory device encryption
- Sandboxing to keep apps self-contained
- Controls or separation of work and personal data

Network Security & Data in Transit

Mobile data faces heightened vulnerabilities because it is always moving between destinations. There are approximately 328.77 million terabytes of data created each day. Wherever the data is moving, whether it be from network to network or from a local storage device to a cloud storage device, data transit security is crucial. To ensure optimal data transit security and to protect mobile data against tampering and eavesdropping, agencies need encryption and network protection capabilities to secure data and deny attackers. Both of these protection capabilities will provide appropriate

protection of data throughout the transit process. There is a need for data to be protected across all types of connections whether it be wifi, cellular, etc. In doing so, it is important to use standard basic protocols like Transport Layer Security (TLS) to protect client-server encrypted interactions.

Application Security

Mobile users are increasingly relying on apps for core productivity and communication tasks. With the uptick in usage, it is important that mobile devices provide multiple layers of protection so users can use their devices with the peace of mind that they are being protected from malware, security exploits, and attacks. Some of the most important layered solutions for application protection include:

- App scanning
- Malware and mobile threat detection
- Device integrity checks and attestation
- Protection against phishing, including harmful texts, emails, and websites
- Application signing

Software and Security Updates

Software and security updates are important in helping resolve software issues that can compromise systems. Keeping up with mobile device updates is not only about adding new features, it is also crucial in fixing bugs and improving overall security.

Software updates play a significant role in reducing cybersecurity threats while patching security flaws, protecting your data, and providing better compatibility between applications.

As agencies evaluate mobile platforms, they should consider what commitments vendors make as well as their prior track record to the software and security update process, including the overall lifetime of support, the frequency of updates, and the consistency of update delivery across device models.

OTHER SECURITY CONSIDERATIONS

Beyond selecting a secure mobility platform that meets their needs, agencies should also consider several other influencers that can affect their security posture.

Open Source Software and Mobile Operating Systems

Open Source Software (OSS) refers to any type of software, application, or program that is freely accessible to the public. The federal government recognizes the importance of using the OSSto drive innovation and is increasingly working to implement policies that will further promote the use of publicly available code in their digital services.
In the context of mobile operating systems, an open source approach allows for several advantages for government agencies, including:

- Transparency
- Flexibility
- Cost-efficiency
- Scalability
- Enhanced security

VERTICAL SECURITY INTEGRATIONS

More and more companies are starting to take a vertically integrated security approach to ensure mobile device management and government agencies can benefit from this approach. A vertical security integration approach means organizations can ensure security not only at every layer (silicon/firmware/OS/apps) but also that there is some level of integrated experience between these discrete layers. This integrated experience extends into the network layers as well because there are security elements users pass back and forth between phones and the network, such as verified identities.

Other benefits of having vertically integrated security for mobile devices are improved battery life, specialized features that require both hardware and software to function properly, improved performance, efficient use of resources, and fewer bugs present.

BEST PRACTICES WHEN IT COMES TO SELECTING A MOBILE DEVICE

Securing a mobility deployment is a multi-faceted effort: from mobile device management (MDM) selection and configuration, policy definition, enforcement and training, and ultimately, to the capabilities of the device you select. Federal, state, and local agencies regularly deploy mobile technology updates throughout their workforce to improve the efficiency of operations. Having the best security tools and processes is important. But mobile security doesn't end there. Choosing a mobile device built for security is also important. The following considerations will help your organization select the right mobile solutions:

Application and Environment Demands | What does the day- to-day working environment look like? What tools do end users need to do their jobs and how do those tools work with mobile technology?

Data Usage Requirements | How will data be captured, stored, and used on the device? Does it need to be encrypted? Will personal usage be allowed on devices and how will that data be kept private?

Data Security Requirements | What are the requirements for data at rest, data in transit, and data in use?

Training and Ease of Use | When it comes to technology in general, employees have different skill sets. The right choice of an operating system can help reduce the time needed for training to enable workers to become productive more quickly.

Security Certifications | What mobile security certifications and standards does the mobile platform adhere to? Are security claims verifiable by third-party laboratories?

Manageability, Control, and Support | What MDM policies are needed? Will they be able to support the agency's data security and application requirements? How easy is the platform to use for IT admins and end users?

Support and Repair Services | It is important to know how likely device failures are and what implications these failures may have. Additionally, agencies should evaluate what commitments vendors make regarding how long devices will be supported, including both software updates and spare parts for repairs.

Total Cost of Ownership | How much is the mobile device going to cost the agency? Is it within their budget?

With about half of government federal, state and local employees working from home or working a hybrid schedule, monitoring hardware assets is more complicated. To mitigate risks and ensure hardware security no matter where employees are working, agencies can:

- Understand the current vulnerabilities as they relate to your enterprise mobility lifecycle
- Leverage encryption solutions wherever possible
- Minimize your attack surface
- Implement adequate electronic security
- Ensure robust physical security
- Implement real-time monitoring
- Conduct regular audits

A MESSAGE FROM OUR SPONSOR, GOOGLE PIXEL

Google understands that mobile devices house your agency information and data. That is why we have made it our mission to build security into our core. Our silicon, firmware, OS, and applications are vertically integrated to keep your data private, safe, and secure. Specifically, we ensure your data is safe by making sure your data is protected by multiple layers of security, applying machine learning intelligence, managing your privacy settings of what you download, browse, and share, preparing you for any emergencies, and offering secure authentication features to ensure you are the only one with access to your phone.

A MESSAGE FROM OUR SPONSOR, VERIZON

Whether the mission takes your workforce to the field or to the office down the street, Verizon helps keep you connected and productive. Mobility and IoT solutions from Verizon connect teams at the push of a button, put drones to work, track and manage fleets, and deliver real-time data and information to power your mission and citizen services.

Within the public sector, Verizon has decades of experience supporting mobility, IT, and technology needs. Its experts understand the evolving challenges facing the government and bring new and innovative approaches to help them navigate through them. Verizon works to understand what drives each agency, and in turn, build and develop comprehensive, secure, connected communications solutions that will enable an agency's workforce, help serve citizens, and accomplish their missions, now and into the future.

ABOUT

Government Business Council

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision-makers from across government to produce intelligence-based research analysis.

For more information, email us at research@govexec.com or visit our website.

verizon

Verizon understands that federal, state, and local agencies have missions that matter. Our customers continue to rely on our decades of experience in delivering the networks and the technology that help make government work.

- Verizon Mobile Device & Endpoint Security
- Verizon Public Sector Website

Pixel for Business

Pixel is a high-performance mobility solution that works wherever your organization does, running on the flexible A ndroid platform and backed by trusted Google technology. Pixel combines strong security features, empowering organizations to reimagine the way they work and equip employees with high-performing mobile devices.

- Pixel for Business Website
- Pixel Security Certifications
- Android Security Paper 2023