Panasonic CONNECT

TOUGHBOOK®

THE MOBILE SECURITY PLAYBOOK SECURING MOBILE DEVICES FOR THE ANYWHERE ANYTIME WORKPLACE

In today's always-on world, the workplace is anywhere and everywhere. Our mobile devices have become extensions of our offices, whether it's on a factory floor, on an oil field, in an ambulance, or even a construction site. Every industry, from retailers to first responders, depends on mobile devices that workers can use to access the IT resources of their organizations.

It's critical for those workers to access resources securely, wherever they are, on whatever network. Whether data is on the move (via portable handhelds and across mobile broadband and WiFi networks) or at rest, securing sensitive information is as critical to organizations as the people who access it. That's because, even as the workplace has expanded with ever-more powerful mobile devices—from laptops for rugged mobility to equally tough handhelds—so has the threat landscape. State actors and criminal opportunists alike continue to deploy increasingly sophisticated tools of their own.

Fortunately, modern rugged mobile devices come to the table with sophisticated security features. These features can include hardware, software, and secure networks. All can enable organizations and their workforces to gain peace of mind wherever they are and whatever they do.

This e-book shows how robust device security works in three critical areas, from our perspective as the leading manufacturer of devices for rugged mobility.

Device Security
How secure hardware works to keep data both on the device and in-transit safe through encryption, authentication, and other means.

Mobile Software
How specialized software helps secure devices from the moment they power up, whether they are laptops or handhelds, using any operating system.

Mobile Connectivity Security
How mobile devices can help keep data safe through secure connectivity on both public and private networks.

Checklist
A convenient checklist also shows how organizations can bring these three elements together for a strong security posture anywhere, anytime.

PART 1: DEVICE SECURITY

In the case of enterprise handhelds, robust hardware security helps defend against intrusions from the outside. In handheld devices, the absence of a hard drive means information gets retained in memory. As a result, data tampering on these devices is practically impossible without the correct cryptographic key. Authentication through passcodes represents another line of defense. Until a user enters the correct password, all data-at-rest and applications remain encrypted. Auto-lock timeouts offer additional protection against unauthorized mobile data access.

However, laptops, with their potentially removable hard drives or solid-state drives, represent another security challenge. Fortunately, system administrators can meet the challenge with hardware-based encryption.

HARDWARE-BASED ENCRYPTION

With hardware-based encryption, data security starts with the hard drive or solid-state drive (SSD) itself. In this case, a chip on the drive encrypts all data, decrypting it only in response to a passcode.

Hard drive encryption provides several key benefits.

1. Hardware encryption is faster than software-based encryption, resulting in no noticeable degradation in device performance.
2. Users can move encrypted drives to other machines; the passcode will decrypt their data on any device.
3. Hardware encryption complies with demanding Federal Information Processing Standards for encryption.

Additional hardware encryption measures link to the unique identifier of a particular mobile device or laptop (user, model, and serial number).

These measures offer further protection on top of drive-based encryption through hardware keys that employ robust encryption standards such as Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES).

The strong baseline protection offered by hardware encryption can harden a device to brute force attacks that attempt to crack a password. Systems can even be configured to detect an attack and shut down to prevent further attempts to access data.

AUTHENTICATION

Authentication prevents unauthorized users from accessing data on a device. Contactless and insertable smart cards, fingerprint scanning, and other methods help guard identity and access rights and support privacy protection in a mobile work environment.

While password protection is commonplace for mobile devices, many government organizations and industries require multifactor authentication. This means users are required to provide an additional factor beyond a password such as a smartcard, fingerprint, or facial recognition to get into a device or network.

Multifactor authentication represents a critical second line of defense against unauthorized access to booting up a device and logging onto a secure network. It's especially important in law enforcement, the insurance, healthcare, and finance industries, where sensitive data, or proprietary corporate and customer data resides on mobile devices.

For customers in high-risk lines of work, such as law enforcement, access to data or systems must be highly secured and comply with policy or regulation such as that required for the Criminal Justice Information System (CJIS). The requirements usually entail using two or more factors for authentication. A field agent, for example, might have to insert a smart card into a laptop, enter a password, and then scan a finger to gain access to sensitive data.

Many multifactor methods depend on special hardware configurations such as high-definition cameras, fingerprint, or smart card readers.

SMART CARDS

Nearly all federal government workers have Common Access Cards (a type of smart card), which allows them to access specific endpoints or systems on the federal government network. Smart cards come in two main types.

- **Contactless smart cards** can be used by merely touching a card or fob to a reader embedded in the device. A contactless approach is user-friendly, but not as secure as using an insertable smart card. That's because when using a contactless solution, a user must remember to log off when he or she steps away, or the unit will need to timeout to safeguard data.
- **Insertable solutions** require a user to plug a card into a reader embedded in the mobile device for gaining access. Removing the card automatically logs the user off. This solution may be less convenient, but it offers greater security since, in our experience, users working in sensitive environments are more likely to take their cards with them when walking away from their computers, rather than remembering to log off.

An enhanced form of smartcard technology, employing the FIDO U2F standard, can replace passwords for internet logins. Just as a conventional smartcard can authenticate users on a device, a FIDO U2F-enabled key allows a user to log into supported email, enterprise applications, and other web-based resources. It works by generating crypto keys and storing them on the device. Users still have to establish one or more additional authentication factors for multifactor authentication.

Multifactor authentication represents a critical second line of defense against unauthorized access to booting up a device and logging onto a secure network.

Smartcards are often less finicky than biometrics, but biometrics can't get lost or stolen.

The benefit of a smartcard over a biometric solution is that the reading devices can be less finicky (less likely to reject an authorized user) and smart cards can be easier to administer, especially remotely. Biometrics, on the other hand, can't be lost or forgotten at home.

BIOMETRICS

Biometric approaches, such as fingerprint and facial scanning, represent an additional authentication feature that takes advantage of each person's unique identifying characteristics. Advanced biometrics can even authenticate users based on how they type or by voice recognition.

Biometric authentication can not only unlock mobile devices and handhelds but also help ensure the integrity of other types of transactions. In the healthcare industry, for example, some hospitals use biometric technology, such as fingerprint recognition, to identify patients and guard against patient identity theft.

Some Panasonic TOUGHBOOK models ship with built-in infrared cameras, allowing users to authenticate themselves via facial recognition even in low light conditions. This is especially useful for night-time surveillance work by law enforcement.

Biometrics are more common on units assigned to a single user who can register their fingerprints on that device. They are increasingly common in police departments seeking compliance with CJIS guidelines requiring multifactor authentication to access federal databases.

REMOVABLE MEDIA

Removable hard drives offer another effective way to protect proprietary information. If a device must be shipped for any reason, such as for servicing, a drive can be removed to comply with regulatory mandates. This can be especially important in highly regulated sectors such as healthcare, law enforcement, federal government, and the financial services industry.

Removable hard drives also make it possible for users to safeguard data by taking a disk with them if they must leave a laptop behind. Because it's always possible to lose a removable disk or a flash drive, hard drive encryption offers a valuable option for removable drive security.

TRUSTED PLATFORM MODULE (TPM)

Proving that a platform has not been tampered with as well as authenticating a laptop user are key attributes of the Trusted Platform Module (TPM) standard. Specialized chips on laptops provide TPM functionality for securely storing passwords, certificates, and encryption keys. Mobile TPM on MicroSD chip cards is also available for some enterprise-grade or rugged handheld devices.

Besides protecting logins, TPM chips can detect unauthorized configuration changes made by malware and block any access to affected applications until IT professionals can remedy the problem.

Among other use cases, TPM can enhance the integrity of digital signatures, for example, for secure email and document management. Consider a field-based insurance scenario where an auditor must assess damage to provide FEMA compensation for property damage after a natural disaster. Having a TPM chip in place helps to ensure the integrity of all remote interactions in this case.

Panasonic works closely with Intel on TPM chips for use in TOUGHBOOK computers.

LOCK SLOT

For many of our customers in industries with a remote workforce, enterprise mobile devices can be susceptible to "smash and grab" theft. That's why some devices offer the ability to physically secure hardware to an immovable object such as a table. An integrated, steel-reinforced lock slot built into the physical structure of the device lets a user attach a cable for securing the device when unattended.

PART 2: MOBILE SOFTWARE

While not impenetrable, current enterprise-grade mobile devices, by nature, exhibit a high degree of data security. That's because software encryption in both Windows 10 and the Android Operating System is automatically enabled by default.

Device manufacturers can add additional layers of security through their own software encryption or embedded technology. For example, Persistence, from Absolute Software, provides location-based protection and tracking embedded in the firmware of mobile devices, including laptops and notebooks.

ASSET TRACKING

Absolute Persistence is a software package that gets loaded onto enterprise-grade devices like Panasonic TOUGHBOOK laptops at the factory. When enabled by the IT management organization, it allows enterprises to manage and track devices after assigning them to users. If a device gets lost or stolen or even if the hard drive or SSD gets wiped or replaced, Persistence automatically reinstalls itself from the BIOS. From there, it begins reporting on device status, geographical location, and recent system hardware and software change details. It can even log keystrokes and access a device's webcam to gather forensic evidence for law enforcement.

Not only can Persistence track missing devices, but it can also activate a "kill switch" to render the device unusable and wipe sensitive data. IT departments can configure the kill switch to trip if a device leaves a specified area or a set amount of time passes without successful login. It can even reinstall other critical software if thieves try to wipe it.

The effectiveness of this type of security has resulted in some deployments gaining recognition as complying with Health Insurance Portability and Accountability Act (HIPAA) and CJIS regulations. Users should check with their device vendor for details on the availability and implementation of Persistence software to understand compliance with industry regulations,

SOFTWARE-BASED ENCRYPTION

Software encryption can be applied to any device and is relatively easy to use, upgrade, and update. Whether data is in transit or stored on different devices, software encryption—available through various applications—provides a reversible process for scrambling data and keeping it from prying eyes.

However, the flexibility of software encryption comes at a cost: it consumes more memory and CPU cycles than hardware encryption, leading to slower performance for resource-intensive applications. Increasingly powerful chipsets have helped to compensate for this limitation.

MOBILE DEVICE MANAGEMENT

Managing a large number of endpoints, i.e., mobile devices, can challenge organizations from a security point of view. Fortunately, mobile device management (MDM) application software and enterprise mobility management (EMM) systems can help.

When helping our enterprise mobility customers implement security, we regularly emphasize the importance of having an effective MDM strategy in place. MDM provides security flexibility, allowing IT to lock down device functionality remotely, monitor and limit access, track assets, and protect data via remote data wipes.

MDM takes place in three distinct stages:

- **Provisioning,** in which devices are unboxed and assigned to users, with all the associated permissions and access to applications.
- **Production,** in which IT staff can monitor devices, apply security patches and software updates, and provide support for users.

- **Decommissioning,** in which the IT department wipes sensitive data, removes user authorization and permissions, and readies devices for disposal.

Each stage involves a comprehensive set of procedures to help ensure enterprise mobile adoption goes smoothly and that IT policies are set and followed.

Windows has native MDM platforms, System Center Configuration Manager and Microsoft Intune. These MDM's are available through Enterprise licensing or monthly subscription.

Organizations managing devices running on the Android OS should deploy a third-party MDM solution.

Panasonic has partnered with SOTI for a range of MDM capabilities.

Whether managing Windows, Android devices, or a mix, MDM helps organizations deploy and manage mobile devices and applications at scale, prevent users from installing unauthorized apps, and perform other vital management and maintenance functions.

For example, MDM can prevent a logistics driver from installing unnecessary time- and battery-consuming apps on his or her enterprise handheld device, such as streaming apps and apps of questionable security. In this way, mobile devices become true work tools that run only apps published by the organization.

MDM can also flag potential security issues for IT departments, for example, a spike in data transmission that could indicate a security breach. It also gives organizations control over the frequency and scope of software updates and security patches.

This helps IT professionals strike the right balance between keeping devices up and running for mission-critical applications and plugging known security vulnerabilities with appropriately scheduled updates.

SECURE TO THE CORE

Bringing together hardware- and software-based security, Microsoft has introduced Secured-core technology developed with CPU makers and device manufacturers, including Panasonic. The technology works in three steps to secure Windows computers.

1. First, secured-core PCs use hardware-rooted security in the modern CPU to launch the system into a trusted state, preventing advanced malware from tampering with the system and attacking at the firmware level.

2. Next, as the operating system launches, the system checks every step in the process to ensure that everything operates normally. If not, it stops the process, making it impossible to use the computer.

3. Finally, once everything checks out, virtualization-based security (VBS) isolates authentication functions from the rest of the operating system. That protects logins from attack and allows only legitimate users to gain access.

The Panasonic TOUGHBOOK 55 is the first semi-rugged computing device in the most secure Windows PC category. Designed for mission-critical users in the most sensitive data industries, it makes full use of secured-core technology. The 8th-generation Intel Core i5 vPro processor, combined with Panasonic advanced components and Windows 10 Pro features, provide strong protection against firmware attacks.

When helping our enterprise mobility customers implement security, we regularly emphasize the importance of having an effective MDM strategy in place.

Secure-core technology from Microsoft and partners, including Panasonic, combines hardware and software measures to provide data security.

PART 3: MOBILE CONNECTIVITY

Along with access security, connectivity security is a critical concern for many of our mobile customers. According to Cisco's Annual Internet Report released in 2020, the number of global mobile devices will top 13 billion by 2023, up from 8.8 billion in 2018.

A growing number of those devices connect to 5G mobile networks. As 5G networks expand, they will provide the greater bandwidth needed to handle burgeoning Internet of Things (IoT) capabilities around the globe and in every major industry.

The technologies that enable the broader business capabilities of the IoT include cloud services, sensors, Machine-to-Machine (M2M) communications, and, of course, mobile networks.

While we believe 5G networks represent no higher risk for devices than 4G networks, 5G's higher bandwidth and lower latency will accelerate the growth of connected mobile devices. That in itself will introduce more opportunities for cyberattacks.

And while we consider cellular networks safer for organizations and their employees than public WiFi networks, workers will continue to need to connect to WiFi networks to do their jobs. For example, when utility technicians or transportation staff are beyond the range of cellular networks, they might rely on public WiFi to upload information. Cost, too, may compel some organizations to limit the number of mobile subscribers they support. Compromised encryption keys and intercepted traffic via faux WiFi hotspots are typical risks mobile device users can encounter.

One way to mitigate the risks of connecting to public WiFi networks is through the use of virtual private networks, or VPNs.

BOOSTING SECURITY WITH VPNS

Virtual Private Network (VPN) tools, such as mobile

VPN clients, can encrypt data at rest as well as in transit, for example, between private and public clouds. VPNs can also be configured to allow only certain apps to run online, and to restrict the sites that users can reach on the internet. Deploying a VPN product specifically designed for mobile services and cellular networks significantly reduces the high overhead present in traditional, large data-stream VPNs.

Our recommendation? Mobile-specific VPNs that maintain persistent, highly secure wireless connections regardless of where users roam. This alleviates the need for repeated logins while avoiding constant application interruptions. Data secured through VPN encryption reinforces the built-in network security provided by carriers.

We recommend all our customers take at least some, if not all, of the VPN steps described above as part of a multi-level security practice. Such a practice should also include software and hardware encryption, individual session encryption, and persistent connection security.

Organizations can go even farther in securing connections with access point name, or APN, connections.

CARRIER-BASED SECURITY WITH APNS

APNs can go a step further than VPNs in securing online connections, but they only work on cellular networks. To use them, organizations must order them from their wireless carriers.

Once set up, the APN redirects all mobile traffic to and from subscribed devices. With an APN set-up, subscribed devices do not connect directly to the internet. Instead, they connect to a server set up by the carrier for the subscribing organization. The concept is similar to proxy servers, in that users visit a special web address to access the rest of the internet. The difference here is that users have no choice; all of their traffic goes through the organization's APN server, which then routes traffic to other points as allowed.

The experience of APNs to users is seamless; users simply access the internet through a browser or other application as usual. However, the server restricts all traffic to approved sites and can constrain a range of potentially risky activities

Panasonic supports APN functionality with carrier-certified cellular modules available.

For IT departments everywhere, maintaining effective mobile security represents a constant process of staying one step ahead of the next threat. It also entails the use of several types and sometimes layers of security to provide proper mobile worker security.

A checklist of effective countermeasures can help organizations make sound choices for securing their devices, users, and networks.

APN CONNECTIONS ACT AS A GATEWAY FOR ONLY SUBSCRIBED MOBILE DEVICES TO ACCESS A CORPORATE NETWORK OR TO MORE SECURELY CONNECT TO THE INTERNET.

PART 4: THE CHECKLIST

Use this A to Z checklist as a guide to mobile device security at every level, from hardware and software to network connectivity.

- ☐ **Access point name (APN)**
  A cellular network-created service that points all internet traffic to and from subscribed devices to an organization's server for filtering and rerouting.

- ☐ **Asset Tracking**
  A feature of Mobile Device Management applications that provides real-time location and other status updates from mobile devices, even if their hard drives or SSDs are compromised.

- ☐ **Hardware Encryption**
  Data security that functions at the level of hard drives, solid-state drives, CPUs, and other hardware, typically offering faster performance than software encryption.

- ☐ **Lock slot**
  A slot in the case of a device, typically a laptop, through which to run a security cable to secure the device to a desktop docking station or in a vehicle dock mount .

- ☐ **Mobile Device Management (MDM)**
  Software application that helps IT organizations provision, manage in production, and decommission large numbers of mobile devices, and provides other benefits such as limiting access to applications, location of devices, device performance metrics and remote data wipes and tracking.

- ☐ **Multi-Factor Authentication**
  Access that depends on more than one method to authenticate a user, for example, a password in combination with a fingerprint.

- ☐ **Secured-core**
  A set of technologies offered by Microsoft in partnership with CPU and device manufacturers that secure Windows devices against malware as they boot up.

- ☐ **Software Encryption**
  Data security that depends on installed software, typically offering greater flexibility than hardware encryption, but at the cost of reduced performance.

- ☐ **Trusted platform module (TPM)**
  A chip that stores and enforces passwords and other authentication data for laptops and other mobile devices.

- ☐ **Virtual private network (VPN)**
  An encrypted tunnel to secure traffic between a device and a server.

NEXT STEPS

By considering security in these three critical areas (device security, mobile software, and mobile connectivity), enterprises will have laid the groundwork for building a coherent mobile solution management and security strategy. Such a strategy takes in data security, access privileges, connectivity security, and device security. It also takes into account business goals and the multiple ways in which mobility can transform an organization without adding unacceptable IT management risks.

Want guidance in planning your next deployment of mobile workforce solutions with proper security? Connect with Panasonic TOUGHBOOK, and we'll engage our Field Engineering & Technology Specialists. Reach us at TOUGHBOOK@US.PANASONIC.COM or 888.245.6344.

FOR MORE INFORMATION

on Panasonic TOUGHBOOK Mobile Computers Handhelds, or Tablets and our Mobile Security Services and expertise, visit us.panasonic.com/Toughbook.

Panasonic CONNECT