NETWORK BOUNDARIES HAVE GONE MOBILE

The days of an organization's network boundary extending only to the edge of their buildings is over. We live in a 24/7 world. Employees want to connect for work the same way they do in their personal lives—wherever and whenever they want.

Today's employees carry smartphones, tablets and laptops and rarely think twice about using their personal devices for work or work devices for personal activities. The mobile workforce will surpass 1.3 billion people, or 37% of the world's overall workforce, by 2015 according to IDC.[1]

Employees connect to the closest free Wi-Fi, often not caring too much about the security of the source, as long as it connects to the Internet. They download data the same way. They want information immediately at their fingertips. Unfortunately, people in a hurry are more prone to make mistakes.

With this shift, the need for mobile security has never been higher—especially when estimates say that in 2014 as many as 11.6 million mobile devices were infected.[2] While this may only represent <1% of the device population, the rate of mobile malware is expected to increase as those devices become more of an aggregation point for valuable data. Mobile applications for banking, credit card storage, and yes, corporate data are becoming prevalent making these platforms a more attractive target for hackers.

Without even knowing it, one of your employees may have accessed a malicious site, or downloaded a virus unintentionally. It only takes one virus from one infected device to move laterally and infect your entire corporate network.

The challenge is that with more device types to protect, a wider variety of software application versions and multiple operating systems to support, Information Technology's (IT) role is becoming more complex. Add to that more well-meaning but often less than vigilant employees making their own 'IT decisions' on how to connect, what to download, and where the 'safe enough' line is drawn, and IT ends up with a lot more potential vulnerabilities.

[1] IDC Worldwide Mobile Worker population 2011-2015 Forecast (Doc #232073)
[2] Annual State of the Net Survey, Consumer Reports, 2013

Mistakes will happen. Sensitive documents will end up in the wrong hands. Your network is more exposed than ever. Devices will get infected, be lost, or worse, stolen. From an IT perspective, how does one ensure the far-reaching mobile workforce is entirely protected?

A comprehensive protection approach would consider the best methods of securing all the potential touch points a hacker may pursue. The optimal implementation would be a seamless approach that protects all these assets using a single integrated solution.

TODAY'S MOBILE SECURITY APPROACHES

Many options exist today to provide security for parts of the mobile experience. There are network and device security products that protect part of the mobile experience from Good Technology, Cisco, Zscaler, Palo Alto Networks, and an array of document protection approaches offered from a variety of encryption program providers. However, they all carry with them significant limitations.

For securing remote connections, many mobile solutions consist of a basic Virtual Private Network (VPN) connecting back to the company. The VPN secures the connection as long as the data you need is within the boundaries of the office. If your data is provided on a software as a service (SaaS) site, it will not prevent your employees from accessing it from outside the VPN. It also does not protect employee devices from being exposed to malicious sites.

To protect the organization's data that may reside on a device requires implementing what is called a container. The container separates your corporate data from your personal data. While this provides a segregation of business from personal, it does not prevent the device from accessing malicious sites. It also does not prevent human errors of accidently sending sensitive data to the wrong recipient.

For documents, the typical approach is to password protect them using a solution either from an OEM or aftermarket provider. Once a document is locked, it can only be unlocked by entering a password or having the same decryption software that the sender used. Passwords are lost, forgotten and compromised all the time. And once someone has the password, they have access to that document forever.

For the device, a typical organization will implement what is called Mobile Device Management (MDM). MDM enables the organization's IT department to have control of the device. If the organization believes that device is compromised (whether it is or not), they have permission to wipe it completely. Your business and personal data will all be lost. This is true even if the device is BYOD and owned by the employee.

The problems with today's solutions can be summed up with the following shortfalls:

1. **Limited document and data protection**—Password protection approaches are set-and-forget. Assuming users remember it, anyone with the password—friend or foe—has full document access forever. As container solutions protect documents within, they do not provide protection for documents leaving the container through email or other means.

2. **Limited protection from threats**—Mobile solutions can protect data residing on the device but they do not protect against users downloading malicious content. Without threat protection, a device can still get infected.

3. **Limited network protection**—Most solutions on the market today leave security gaps or protect the network by significantly limiting employee access freedom

4. **Limited IT choices for compromised devices**—Employees are forced to accept 'full wipe policies' even on their own devices should they want to access the company network or email

KEY CAPABILITIES

- Secure access control for business resources
- Locally stored business data is sandboxed and encrypted
- Integrated encrypted communication for remote access
- Remote wipe of business data only
- Detection and prevention of rooted and jail-broken mobile devices
- Single Sign-On (SSO) for ease of use and increased security
- Supported on iOS and Android devices

Whether your current solutions have all four, two or only one of the above issues, they are still not good enough. That is because the real objective is to provide a seamless mobile experience that maximizes workforce productivity without compromising security. And none of the solutions on the market today provide network, device and data protection in a single solution.

OPTIMAL MOBILE SECURITY: SEAMLESS PROTECTION IN A SINGLE SOLUTION

Assuming equivalent coverage, every IT department would tell you they prefer to manage a single integrated solution rather than multiple individual ones. A seamless integrated solution with multiple mobile security capabilities is the preferred approach. This type of approach is important, because when managing a network, it is vital to have granular control. Granularity is the ability to zoom in to manage individual devices or documents, or zoom out to see your entire network.

Check Point recognized this and built a complete mobile security solution, called Check Point Capsule. It enables secure and easy access to your business data without interfering with your personal data or applications, extends your company's internal security policies to mobile devices, and provides seamless protection for business documents that is unmatched in the market. Check Point Capsule is built with both the user and IT manager in mind. It provides the simplicity and usage freedoms the users demand, and the management granularity and security the IT department requires. As an integrated solution, Check Point Capsule is not prone to the security gaps that typically accompany loosely integrated individual products. It is designed for complete protection.

The complete mobile security experience is what truly sets Check Point Capsule apart. The following sections describe the protection capabilities it provides. Its ease of use combined with its protection granularity will empower your organization's mobile workforce.

SECURING DEVICES

Many companies don't bother creating a separate layer of security on their employee's mobile devices. They rely on the default security provided with the mobile device. When they implement an additional layer, they typically use a Mobile Device Management (MDM) solution.

Lost or stolen phones can cause sensitive business data to be compromised. In the U.S. alone, over 4.5 million cell phones were lost or stolen in 2013.[3] The number of phones and tablets lost temporarily is likely much higher. When the device is owned by the employee and allowed to access the corporate network under a Bring Your Own Device (BYOD) policy, the employee's valuable personal data is mixed with business data on the same device. When a device is managed through MDM solutions, the entire device could get wiped if IT suspected it might be compromised. Instead, the better solution would be to protect business data without impacting personal data on the phone in a situation where it may have been lost or stolen.

Check Point Capsule is an application that provides a secure and encrypted environment for business data on mobile devices. This prevents data leakage between personal and business data. It is accessed via a personal identification number (PIN) that is separate from the phone's lock screen PIN. Once entered, the user has access to their corporate email, calendar, and contacts as well as secure documents, web-based applications and their organization's secure intranet.

[3] Juniper Research, December 2013

KEY CAPABILITIES

- Secure documents by default upon creation
- Access documents without passwords
- Create document access authorization by group or individual
- View and edit documents on personal computers, iOS and Android smartphones and tablets
- Permissions can be set to: read, edit, print, change classification, remove protection, modify authorized users, print screen, and copy/paste
- Encryption to protect sensitive data
- Monitor document access and use history

Check Point Capsule is simple to install, configures automatically and works on any iOS or Android mobile device. In the case of a compromised device or employment termination, all data and access enabled through the application can be erased remotely without impacting any of the employee's personal data.

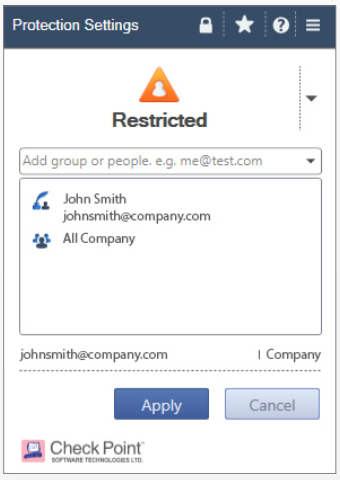
Organizations implementing the Check Point Capsule benefit from the increased productivity that comes with mobility without compromising on device security.

SECURING DOCUMENTS

Most organizations today either opt to not protect documents at all, or protect them using basic password protections. Besides having to remember them, the downside of passwords is that once someone has them, they have access to that document forever.

Sharing documents with coworkers, partners, and customers is a daily activity in business today. On average, sensitive data is sent outside organizations every 49 minutes.[4] Almost 85% of organizations have used Dropbox to share business documents.[5] Think about the several means of sharing data today and number of security gaps they leave. Sensitive documents get attached to emails, shared on cloud sharing sites, transferred via FTP or put on USB thumb drives and exchanged every business day. Once a document leaves the organization, there is typically no insight or control over WHO is accessing it and HOW else it is being shared.

Check Point Capsule provides a complete document security solution. Users establish security when they create documents. They can encrypt sensitive documents, as well as define who can access that document and what they can do with it. Authorized recipients can seamlessly access and use documents without the need to remember passwords. On premise management enables organizations to verify and audit who has shared documents, review usage history, and remotely revoke access. Check Point Capsule also provides document tracking and controls throughout the document's lifespan. Documents can be shared with confidence, because security follows the document wherever it goes throughout its life.



[4] Source: Check Point 2014 Security Report
[5] Source: Check Point 2014 Security Report

KEY CAPABILITIES

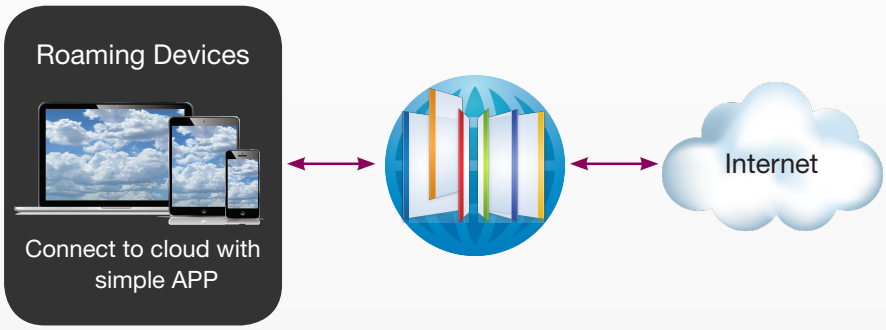
- Extends the corporate security to mobile devices anywhere using one single policy
- Includes IPS, Application Control, URL Filtering, Antivirus, Anti-Bot, and Threat Emulation
- Data centers located across the globe to provide best latency and performance
- Supported on iOS, Android, Windows, and MAC platforms
- Logs can be pushed and stored locally or viewed online
- Active Directory integration for identity awareness

PROTECTING MOBILE DEVICES AND YOUR NETWORK FROM THREATS

Your employees with mobile devices want to access the same kinds of information as employees sitting at their desks in your headquarters. At the same time, it is critical to provide mobile employees with the same level of security as your employees sitting within your office building. Today, 93% of organizations have mobile devices accessing their network and 79% have reported mobile security incidents in 2014.[6]

The objective is to extend your organization's security policies to protect mobile devices everywhere they go. Check Point Capsule creates a secure connection from your mobile device. It provides seamless access and directs all traffic through the secure cloud for full protection by leveraging the same policies as your corporate network. This would prevent devices from accessing malicious files and websites, and protect devices from bot damage and other cyber threats. Anti-bot, antivirus, application control, URL filtering, threat emulation and intrusion prevention system (IPS) protect mobile users from threats as if they were in your corporate headquarters.

Check Point Capsule enables organizations to provide security across their business operations, providing always-on, always up-to-date protection for mobile users outside your organization's security perimeter. Check Point is considered best in class in network security protection performance as rated by NSS Labs in their latest 2014 competitive review.[7] These same corporate security policies protecting your organization will be extended to your mobile devices with Check Point Capsule. Monitoring the network and device management is integrated and simplified through the Check Point Security Management system.



[6] Check Point Mobile Security Survey Report 2013
[7] Next Generation Firewall (NGFW) Security Value MapTM (SVM), Comparative Analysis Reports, NSS Labs, 2014

MANAGING MOBILE SECURITY

Complete mobile protection is comforting, but it would be far less so if each feature required its own monitoring and management software. Managing a complete mobile solution using multiple software tools would be complicated and costly for an organization, and would likely lead to security holes.

With Check Point Security Management, IT has a single interface from which they can monitor and control all aspects of their Check Point Capsule deployments. The security policies of the entire organization are managed from the same SmartDashboard. If the organization is using Check Point security gateways on premise, they get the additional benefit of pushing the same consistent corporate security policies to the cloud, and applying a single security policy across the entire organization. If they are only using Check Point Capsule, then an easy-to-use web interface is available to configure the policies.

Check Point Capsule offers complete mobile protection in a single, integrated experience. With Check Point Capsule, employees on the move will have the same protections as employees in the office. Mobile devices will be secure. Documents will be protected within devices and even when they leave the devices, without having to send or share passwords. Most importantly, your corporate network remains secure even when accessed by tens, hundreds or even thousands of mobile devices.

SUMMARY

The mobile revolution is here. The global mobile workforce is set to increase to 1.67 billion in 2018, accounting for 41.8% of the global workforce according to Strategy Analytics.[8] Usage patterns between corporate disciplines and personal freedoms are blurring quickly. Proactively protecting your organization by securing the mobile workforce is becoming more important.

IT needs to secure the mobile network, protect against mobile device attacks and infections that are becoming more prevalent, and protect their organization's documents both now and in the future.

Check Point Capsule combines all these protection capabilities in a single integrated solution. Check Point Capsule creates a secure mobile environment that protects mobile devices from threats everywhere and secures business documents wherever they go. Finally, a solution that offers complete mobile freedom without compromising security.

[8] Global Mobile Workforce Forecast Update 2012-2018, Strategy Analytics, 2014

CONTACT CHECK POINT

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com