



Handheld Wireless Security

Business-critical devices face new security threats

Contents

Introduction	3
Rise of handheld wireless communication devices	3
Security a critical enabler for businesses with handheld devices	4
Handheld wireless communication devices and platforms	5
Wireless communication devices present special security challenges	6
Secure remote network access for handheld wireless devices	7
Virus and malware protection	7
Endpoint security policy compliance.....	8
Data security for handheld wireless devices.....	8
Security deployment and management for handheld wireless devices	9
Conclusion	9

Introduction

Smartphones are rapidly becoming an indispensable communication and computing tool for the world's expanding mobile workforce. Worldwide Smartphone sales topped 32 million units in the second quarter of 2008. Incredibly, they have begun to outpace sales of laptop PCs, and market research firm In-Stat forecasts Smartphone sales to grow at more than a 30 percent compound annual growth rate through 2013. As Smartphones and other handheld wireless communication devices become an integral part of the modern business landscape, the advances in flexibility, power, and mobile access come with a risk. Popular features such as email and Internet connectivity, still-maturing protocols and practices, and expanded access to corporate networks and confidential information expose Enterprises to a vast and growing array of security threats.

Malicious activity, once the province of isolated hackers who sought notoriety, is now carried out by organized cybercriminals who seek to exploit corporate IT vulnerabilities for financial gain. The cyberattacks themselves have become more complex and sophisticated, including blended threats that can enter and infect multiple areas of an enterprise's network. Protecting one part of a corporate network—for example, the network gateway—without protecting endpoint devices, such as handhelds, is a prescription for a security incident. Hackers have always sought out new vulnerabilities and lapses in security coverage, so it is not surprising that handheld devices, a new frontier, have become a growing target for malicious activity.

With the vast amount of information that enterprises consume, process, and store, the stakes are higher than ever. A security breach can lead to enormous costs associated with loss of critical data, including damaged reputations, reparations to customers and partners, and fines paid to government regulators. To be successful, a business must allow workers to access needed resources remotely, while at the same time ensuring that confidential information and assets are not compromised. A comprehensive security solution is a critical enabler of modern business practices and a mandatory element in protecting any enterprise.

Rise of handheld wireless communication devices

Of all handheld communication device categories, Smartphones—with their PC-like computing capabilities—are the fastest growing segment, as well as the most vulnerable to security risks. Smartphones combine cellular phone capabilities with basic tools such as address books and contact lists, additional functionality found on feature phones, like Bluetooth, MMS, and streaming video, plus more advanced features such as “push” email and Web access.

Smartphone users typically access corporate information, files, and resources over the Internet using software specially designed for remote access and smaller user interfaces. With the growth of Web applications—applications designed for access via Web browsers—workers have access to an increasing amount of critical corporate resources and information. For example, business travelers can now review and make travel plans, check warehouse inventory levels, conduct online banking transactions, communicate with co-workers, and access customer relationship management (CRM) applications while on the road.

Given the changing business environment and ever-increasing capabilities packed into Smartphones, it is no wonder that they are rapidly becoming an indispensable part of business. According to forecasts from industry research

firm Gartner, Smartphone sales for 2008 will reach 173 million units, representing an increase of 42 percent over 2007 sales. North America continues to be one of the fastest growing markets: unit sales grew 75% in the second quarter of 2008 compared with the same period in 2007. Smartphone sales are growing as part of the overall handheld device category. According to a study by ABI Research, the Smartphone market is projected to grow from 10 percent of total handheld device sales in 2007 to over 30 percent in 2013.

Future growth will be driven by several factors including an expanding set of features and functions, an increasing number of applications designed for Web-based access, and faster wireless Internet connections and technologies. The growing popularity of Software-as-a-Service (SaaS)—a model in which host companies store business information on servers accessible over the Internet via a browser or simple Smartphone interface—will enable workers to perform even more functions when on the go.

Last year was a breakthrough year in the industry. Smartphones outsold laptop computers for the first time. This trend is likely to continue. A Wall Street Journal article indicates that workers are increasingly leaving their laptops at home in favor of the smaller, lighter devices. While only a few mobile workers currently do all of their work on Smartphones, a survey from research firm In-Stat reveals that over 50% envision using Smartphones as their sole computing device in the future. Security solutions must be in place to protect enterprises from vulnerabilities associated with this growing segment.

Security a critical enabler for businesses with handheld devices

Handheld wireless communication devices deliver real business value, allowing users to access information and applications like never before. But here's where it gets challenging. With features such as Bluetooth, MMS, email, and Internet access, handhelds are becoming a backdoor into corporate networks and a new target for malicious activity. Protecting the security at an enterprise perimeter level is not enough, not when endpoints such as handhelds can be used as an entry point for attacks or as a mechanism for spreading malicious activity.

Already over 400 different mobile viruses have been reported. Security experts and industry analysts expect this number to grow in much the same way that malware affecting PCs has grown over the past ten years. The types of handheld threats are already broad, exploiting the different vulnerabilities associated with use of such devices. For example, the Symbian Cabir worm, along with its 15 variants, infects Symbian Series 60 Smartphones by sending itself over Bluetooth connections, taking advantage of vulnerabilities in the unsecured and still-evolving, protocol. Mabir, a related worm, listens for incoming MMS and SMS messages sent to the victim's phone and then sends a copy of itself in an MMS response.

Commwarrior and Beselo exploit the victim's local address book and send randomly named files to avoid recognition and cover its tracks. Skulls, a major family of Trojans aimed at handheld devices, overwrites all of the device's applications with non-functional versions. A spyware program variant of Skulls records voice calls and SMS text messages, and relays that private information to an outside server. A pocket PC trojan copies itself to the Startup folder, emails the victim's IP address back to the author and then exposes the device to remote commands

issued by the hacker. Earlier this year a new WinCE trojan emerged, packed inside legitimate installer programs such as Google Maps. InfoJack disables Windows Mobile's installation security so that other malicious applications can be installed without a user knowing.

The relative immaturity of mobile phone and wireless protocols, user practices and protection are leaving workers and corporate networks more exposed than many realize. These backdoors to the corporate network must be closed. Access to sensitive corporate data, often over unsecured wireless access points and networks, leaves businesses vulnerable to unauthorized access, loss or theft of data, including intellectual property and confidential customer information, and associated non-compliance with security regulations. Applications like online mobile banking and email expose users to the same types of threats facing PCs. Analysts estimate that there will be 280 million mobile mailboxes by the end of 2008, and Smartphones are being used more and more to surf the Internet. This means handheld users will confront adware, spyware and phishing attacks in increasing numbers.

Currently, the greatest threat to enterprises deploying handheld devices occurs when data stored on devices falls into unauthorized hands. An alarming number of devices are lost or stolen every year, and research shows that the vast majority contain confidential business data.

Unfortunately, several trends are making handheld wireless communication devices an increasingly desirable target for cybercriminals:

- A growing population of handheld users means a bigger and more lucrative target for hackers
- An expanding set of features, including email and Internet access, exposes users to an increasing set of threats and many of the same ones associated with PCs, including viruses, trojans, worms, denial-of-service, and phishing attacks
- As Smartphone operating systems standardize and consolidate, hackers will be able to have an even greater impact for the same level of effort
- A low level of risk awareness leaves enterprises unprotected and vulnerable

Handheld wireless communication devices and platforms

Handheld wireless communication devices are built on many different operating system (OS) platforms, but four are most common. Symbian, an open OS found on Nokia devices, dominates the market. Symbian accounted for 57% of total Smartphone sales in the second quarter, 2008, down from 66% in 2007. Windows Mobile is a compact OS integrated into a suite of applications designed for mobile devices based on the Microsoft Win32 API. Windows Mobile runs on multiple hardware platforms including Pocket PCs, Smartphones, Portable Media Center, and automobiles. Palm OS is a proprietary, embedded operating system used on some mobile devices. Palm was a pioneer in Smartphones with the introduction and popularity of the Treo. Research In Motion (RIM) Blackberry devices, among the most popular in the market for Smartphones, use a proprietary multi-tasking OS and place special focus on email capabilities.

Two newer operating systems are entering the scene. Apple's iPhone runs on a mobile version of its Mac OS X operating system. The iPhone software has built-in support for a VPN client and supports a range of Wi-Fi Protected Access (WPA) protocols. The iPhone focuses on multimedia features. Also, Linux operating systems for mobile phones are on the rise. Google's G1 Smartphone, available on T-Mobile devices, runs the Linux-based Android OS.

Wireless communication devices present special security challenges

Handheld wireless communication devices operate over a variety of communication protocols and networks. These include CDMA (code division multiple access), TDMA (time division multiple access), GSM (global standard mobile), 802.11X (Wi-Fi), 802.16X (WiMAX). The two major standards for third generation (3G) networks are W-CDMA (also known as UMTS) and CDMA2000 1x EV-DO technology. These reflect technology advances in speed, standardization, range, and access.

As handheld wireless communication devices become an indispensable part of an enterprise's network, enterprises must respond with appropriate safeguards, ideally deployed as part of an overall, comprehensive security plan. Malicious entry into any part of an enterprise's network architecture can be lethal, and in the face of coordinated, blended threats, a comprehensive view is critical. Comprehensive security means addressing vulnerabilities across the entire enterprise network and protecting all endpoints, including PCs and handheld devices.

There are five primary components to handheld wireless communication device security: secure remote network access, virus and malware protection, endpoint security policy compliance, data security, and centralized management.

Secure remote network access for handheld wireless devices

Enterprises face two risks when they allow handheld devices to connect to corporate resources over unsecured networks and via Wi-Fi hotspots: unauthorized persons or servers may access the corporate network, and data may be compromised during transmission. If either of these occurs, an enterprise is left wide open to damage. Thankfully there is a straightforward solution. Enterprises can protect against these risks by deploying a network access control (NAC) solution and encrypting data in transit.

A NAC solution, simply put, ensures that users are who they say they are—before being allowed to access corporate resources. At the gateway, enterprises can define NAC rules and verify authorization before a user is allowed to connect over a VPN. Handheld devices support a variety of authentication methods, including passwords, tokens, certificates and shared secrets. A strong secure remote network access solution will support a broad range of industry standards and should include WPA2, a secure wireless authorization protocol designed for enterprises and mobile devices operating over Wi-Fi networks.

Once access is authorized, the data must be protected in transit. The most popular secure wireless communication protocols are IPSec, IPSec over L2TP, PPTP, SSL and TCP/IP. While TCP/IP is the basic communication protocol of the Internet, the others represent different methods of creating a virtual private network (VPN), a secure "tunnel" for safe transmission of information across the Internet.

The most popular forms are IPSec and SSL VPNs, and newer Smartphones use industry standard protocols for both. Whereas IPSec VPNs require a client loaded onto the endpoint device, SSL VPNs afford the most flexibility because they are clientless. Users of handheld devices typically access the SSL VPN via a simple Web browser. A strong SSL VPN solution will provide mobile workers with transparent, uninterrupted connectivity, allowing them to easily traverse firewalls, proxies, and network address translation (NAT) devices without the disruption of having to constantly re-authorize as they roam across multiple cellular and Wi-Fi networks.

Virus and malware protection

Regardless of secure transmission protocols deployed, the chosen VPN should include a firewall. The firewall protects the network from unauthorized access by outside, unknown networks and unauthorized users. Deploying personal firewalls on handheld devices helps block malicious traffic and prevents the propagation of worms and the potentially harmful effects of spyware, such as Flexispy, a variant of the Skulls Trojan. Firewall protection on both the endpoint and the gateway are consistent with multi-layered security, a recommended practice for strong protection. Ideally, firewalls should be integrated into other security technologies such as the VPN, NAC and NAT and should include intrusion prevention, antivirus and web content filtering capabilities. A unified security architecture with centralized management can allow enterprises to administer and deploy security policy from a single console.

Endpoint security policy compliance

Since IT administrators do not have direct access to handheld devices and may not be installing bundled software or VPN clients, they do not have as much direct control over the devices as they would like. This is a significant concern because handhelds, like other endpoint devices, can be used as an entry point of attack or to spread an existing virus or threat.

In the PC realm, there has been a dramatic rise in spyware including keystroke loggers, Trojan horses, and malware designed specifically to automate financial crime. These threats are now beginning to target handheld devices. Malware threatens information confidentiality, endangers system passwords and increases the risk of data loss or compromise. A strong handheld endpoint security solution protects against threats by ensuring that a device complies with an enterprise's security policy before a user is allowed to access the network. Prior to granting access, endpoint security solutions ensure that anti-malware software is up to date, devices patches and updates are in place, and real-time threat updates are received.

Endpoint security for handhelds should be tailored to a device's unique characteristics such as computing power and screen size. Malware scanners should employ signatures and rules that identify malware targeting the device's specific operating system. Virus signature updates should take into account the different Smartphone interfaces, such as SMS, MMS, and ActiveSync. Security providers are just beginning to develop anti-virus and anti-malware scanning tools to address these differences.

Since most malware is conveyed via unsolicited messages, endpoint security for mobile devices should include interface blocking utilities; the ability, for example, to turn on or off SMS/MMS or Bluetooth capabilities. Such utilities should include

granular device settings so that IT administrators can apply different rules to different groups, and interface blocking should be configurable centrally within an enterprise for maximum visibility.

Data security for handheld wireless devices

Analysts agree that lost or stolen devices currently pose the greatest threat. A device usage survey conducted by Check Point found that 22% of mobile device owners had lost their devices, and a staggering 81% of these devices had no protection such as encryption. What's more, 37% of these devices contained sensitive information, such as passwords, corporate data and bank account details.

Research shows that the vast majority of lost or stolen mobile devices contain company communications and confidential business information. Because handhelds are often used by the most senior-level managers and by those accessing critical customer and financial data, the risk is enormous. Two solutions protect data on the devices from falling into the wrong hands: data encryption and device access control.

To protect against data loss or abuse, all data stored in files, folders and memory cards on the handheld device should be encrypted. A good solution should be transparent and simple, encrypting files on the fly without interrupting workflow. Handheld owners should be required to enter an access code or other authentication procedure before being allowed to access device features and stored data. With both of these protections in place, IT staff can sleep better at night knowing that data stored on the devices is protected. As an additional safeguard, enterprises may adopt technology allowing IT administrators to remotely wipe a phone clean in the event that it is reported lost or stolen.

Security deployment and management for handheld wireless devices

Most enterprises have a formal security policy in place, outlining their overall security and risk strategies. A good handheld device security solution allows an enterprise to monitor and protect devices within the context of this overall security strategy. It should offer centralized management of handheld devices, including policy management, monitoring, and enforcement, and should enable an integrated view of security status across the entire enterprise.

With centralized management, IT administrators can deploy security policies such as access rights, encryption settings and interface blocking rules, deploy patches and device updates, and distribute security threat updates and alerts. Centralized configuration and maintenance of security solutions for handhelds allows an enterprise to configure resources and policies more consistently and provides administrators with greater visibility into policies and status.

A security management tool allows an enterprise to build an audit trail of the performance and events associated with handheld devices and delivers critical information needed to spot security threats and aid planning. Network attacks have become increasingly complex, often involving blended threats. A sound handheld security solution should integrate into an overall, unified security management solution for the enterprise so that administrators can correlate security threats across all products and solutions to quickly identify potential attacks. For example, being able to see a user attempting to login to IPSec and SSL VPNs from different locations is an easy way to spot a potential login violation.

Conclusion

To stay competitive in a changing business world, enterprises must leverage technology to meet the needs of workers while ensuring the security and stability of information and network assets. Handheld wireless communication devices are becoming an indispensable part of business. As workers continue to adopt and use handheld devices to check email, surf the Web, and access corporate resources, the potential for devastating security breaches will also increase. If enterprises do not quickly address the vulnerabilities posed by handheld wireless communication devices, they risk loss of data, damaged reputations, disrupted operations, and costly reparations.

Cybercriminals, a new breed of criminals specializing in malicious activity for financial gain, are beginning to target vulnerabilities associated with handheld devices. Already over 400 different mobile viruses have been identified, and experts warn that the number of threats will rise significantly. Meanwhile, awareness of the level of risk associated with handheld devices has been low. To protect against costly security breaches, enterprises need to accomplish four aims: protect the data on physical handheld devices so that it is not compromised when lost or stolen; secure data in transit and provide strong authorization; ensure device compliance via endpoint security tools; and implement centralized security deployment and management.

Check Point offers total security solutions that meet an enterprise's comprehensive security needs. Two solutions—Check Point SecureClient Mobile™ and Pointsec® Mobile—specifically safeguard handheld wireless communication devices and are designed to fit into an overall enterprise security plan. SecureClient Mobile provides secure and uninterrupted remote network access for handheld devices, while Pointsec Mobile safeguards data on Smartphones and other handheld devices using encryption and access controls. Both products can be centrally managed and integrate seamlessly into Check Point's unified security architecture. For more information on these and other products and solutions, please contact a Check Point representative or visit www.checkpoint.com.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

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

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.