

“We have peace of mind now with Check Point Full Disk Encryption, and we know that the information on our laptops is safe and protected.”

*Jim Thornton
Senior Systems Architect
Memorial Health Services*



CUSTOMER NAME

Memorial Health Services

INDUSTRY

Health Care

CHECK POINT PRODUCTS

- Check Point Full Disk Encryption™

CUSTOMER NEEDS MET

- Provided peace of mind by protecting confidential information
- Delivered quick and simple configuration and deployment
- Enabled transparent, automatic, and enforceable full disk encryption

Memorial Health Protects Patient Information with Check Point Full Disk Encryption

ABOUT MEMORIAL HEALTH SERVICES

Memorial Health Services (MHS) is a nationally recognized, not-for-profit health care system with five hospitals located in Southern California, in both Los Angeles County and Orange County. MHS focuses on evidence-based, best practice medicine, thereby gaining widespread recognition for its distinctive approach to medical care. Known for its high standards, MHS is continually recognized for its governance and safety practices by several leading accreditation bodies in the United States. By practicing ground breaking and innovative health care methods, MHS Medical Centers repeatedly exceed state and national averages, remaining a leader in the health care industry.

THE MEMORIAL CHALLENGE

With media coverage surrounding the exposure of confidential patient information becoming more prevalent, MHS became quite concerned and did not want to suffer a data breach that could compromise the security or confidentiality of patient information. “Around the time we began to think about encryption solutions, there was a lot of publicity about missing laptops,” says Jim Thornton, senior systems architect at MHS.

As one of the top hospital organizations in the country, MHS is responsible for large amounts of confidential patient information. With a growing number of employees working remotely and regulatory drivers such as the Health Insurance Portability and Accountability Act (HIPAA) and SB 1386, a California law regulating the privacy of personal information, MHS needed a comprehensive data security solution that could be deployed quickly and transparently to secure the personal health information of its patients.

THE CHECK POINT SOLUTION

During this time of intensive media coverage, several other providers in the health care industry began to evaluate similar solutions. According to Thornton, Check Point Endpoint Security Full Disk Encryption™ was the leading product rec-

ommended by other companies. These companies shared their experience with Check Point Full Disk Encryption's quick and simple deployment and the fact that it supports any PC or laptop running Windows or Linux.

"We looked at what the new Microsoft Windows Vista operating system was offering as far as its BitLocker drive encryption feature, but we were afraid that it might require hardware changes or new laptops," says Thornton. "We wanted a quick turnaround and a solution that we could test."

After validating the recommendations from other organizations with information from Gartner's Magic Quadrant, which has positioned Check Point in the 2007 leaders' quadrant for mobile data protection seven years running, MHS felt Check Point Full Disk Encryption was the only solution robust enough to meet its growing need for data security.

"We gave other solutions a cursory look but did not evaluate them because Check Point Full Disk Encryption was the obvious choice," says Thornton. "We bought an enterprise license for all of our hospitals and have completely deployed on our inventory of laptops."

THE BENEFITS OF CHECK POINT SECURITY

For MHS, the primary advantage of deploying Check Point Full Disk Encryption was the realization of complete and total patient data protection. Regardless of whose hands a missing or stolen laptop may end up in, MHS is confident that the information on that laptop is safe and secure.

Peace of mind

Check Point Full Disk Encryption eliminates the concern of losing the private and personal details of a patient's medical history. In the event of an actual theft, Check Point Full Disk Encryption ensures that all data is "locked down" and secure. It is a simple, strong, and enforceable solution that protects MHS's privileged patient data wherever it goes.

"We have peace of mind now with Check Point Full Disk Encryption, and we know that the information on our laptops is safe and protected," says Thornton.

The current policy at MHS is to encrypt any new laptop that is deployed. "It's just like installing virus protection or anti-spyware protection," says Thornton. "It's just another layer of security that we add on to a laptop before we give it to a user."

Easy-to-use, easy-to-manage

Check Point Full Disk Encryption runs in a completely automatic, transparent mode to the user and ties in seamlessly with MHS's

current IT infrastructure. Administrators did not have to change any procedures or burden staff with hours of training.

"We realized it was a fairly easy solution to install and manage, and once we installed it, we really didn't have to go back and do any maintenance," says Thornton. "We had a Check Point engineer come out and do a one-day overview of how to install Check Point Full Disk Encryption and what our options were; it is a simple solution."

According to Thornton, it was also very important that the solution be unintrusive from the user's perspective. MHS utilized the Windows Integrated Login feature of Check Point Full Disk Encryption to keep the user experience recognizable and familiar.

"We did not want to add another layer of authentication or change the way that someone is used to authenticating," says Thornton. "So implementing the Windows login seemed more appropriate."

Complete data security protection

Check Point Full Disk Encryption provides MHS with the highest level of security by combining strong full-disk encryption with access control and the ability to support all common smartcards and tokens. Only authorized users with the correct logon and password can gain access to a computer. And if the machine is turned off or goes into standby mode, the entire hard drive remains encrypted, protecting all the contents.

"Every feature of Check Point Full Disk Encryption is appealing, the core, the entire scope of the product," says Thornton. "The single sign-on, preboot authentication, full-disk encryption, ease of deployment, broad platform support—it all appealed to us."

The Check Point Full Disk Encryption product family has been in widespread use for more than 10 years, and Check Point Full Disk Encryption has the most and highest levels of certifications in the industry, including FIPS 140-2, Common Criteria Evaluation Assurance Level 4, and BITS.

THE FUTURE OF MEMORIAL HEALTH SERVICES

Currently, MHS is consulting with Check Point regarding other data security concerns relating to data leakage, such as USB ports on PCs and the proliferation of USB flash drive usage. Check Point Media Encryption offers complete port and storage device management, preventing unauthorized copying of sensitive information from enterprise desktops and laptops through port control, content filtering, and optional media encryption.

CONTACT CHECK POINT

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-575-9256 | 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 | www.checkpoint.com

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, 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, INSPECT XL, 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, 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, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, 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, 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.