

“One of the requirements that we have built into our 2005 security policy manual is that all vendors accessing our network will also need to have some type of Integrity client.”

*Mark Schaefer
Information Security and Windows
Infrastructure Group Manager,
Edwards Lifesciences*



CUSTOMER NAME

Edwards Lifesciences

INDUSTRY

Healthcare

CHECK POINT PRODUCTS

- Integrity™ endpoint security
- VPN-1® Pro™ gateway

CUSTOMER NEEDS MET

- Compliance with HIPAA, SOX, and other government regulations
- Attack protection for thousands of desktops
- Access policy enforcement to ensure PCs meet trust criteria for network access
- Ease of management

Edwards Lifesciences secures endpoints with Integrity

ABOUT EDWARDS LIFESCIENCES

Defeating cardiovascular disease is the life’s work of the more than 5,000 men and women of Edwards Lifesciences, a global leader in products and technologies for treating heart and circulatory problems. Every year, 70,000 people in the United States alone receive new heart valves—the vast majority made by Edwards. In operating rooms and intensive care units the world over, Edwards brand monitoring devices measure heart pressure and blood volume. In 2004, 80 percent of the company’s nearly \$1 billion in sales came from its market-leading products.

Edwards has a presence in 100 cities, with its main data center in Irvine, California, and a regional hub in Horw, Switzerland. Connection to the corporate WAN is provided for employees and business partners in various ways. Many offices and remote users connect securely through the Internet via Check Point VPN-1® Pro™ gateways.

THE EDWARDS CHALLENGE

As a U.S. healthcare company, Edwards Lifesciences has to comply with many federal and state regulations to protect information. It must adhere to the security requirements of the Federal Drug Administration and the Health Insurance Portability and Accountability Act (HIPAA), as well as those of the Gramm-Leach-Bliley Act, the Sarbanes-Oxley (SOX) Act, and the California Security Breach Information Act. “We are a very regulated environment. Every other month someone audits our security,” says Mark Schaefer, the information security and Windows infrastructure group manager for Edwards, who cites SOX and stage-two HIPAA compliance as his company’s most immediate security concerns.

For regulatory compliance, Edwards needs to demonstrate that all its endpoints connecting to the network are safe and adhere to the company’s security policies. “We have been effective at stopping attacks coming from outside the perimeter, only to find that employee devices are often the source of worms, spyware, and other problems,” Schaefer says.

THE CHECK POINT SOLUTION

Five companies offering endpoint security solutions were invited by Edwards to demonstrate their products. “We gave each vendor basically a checklist of items and the same amount of time to install their solution, deploy it to five clients, and teach us how to roll out a basic security policy with it,” Schaefer says. Some failed the test

for lack of required functionality. Others took days to implement even on the small scale of the demonstration. Check Point Integrity™ was the only solution to provide the security required with the ease of use and management demanded for a large-scale global deployment. “For installation, administration, and ease of use, Integrity was by far the best,” he says.

After selecting its endpoint security solution, Edwards implemented Integrity on 2,000 desktop computers throughout the enterprise. The Integrity product family safeguards enterprise networks from worms, penetration attacks, Trojan horses, spyware, and other exploits with proactive protection for every network endpoint. Integrity’s Stateful Inspection firewall blocks all unsolicited inbound traffic, and endpoint PCs are completely invisible to hackers. With Integrity, Edwards is able to centrally manage security policies and enforcement for every desktop in the company, no matter where in the world they are located.

THE BENEFITS OF CHECK POINT

Deployed worldwide to thousands of desktops, Check Point Integrity is helping the Edwards IT organization support the communication needs of the business while complying with myriad government regulations.

Regulatory compliance

HIPAA, SOX, and other regulations all have certain requirements in common that Integrity helps Edwards meet.

“Integrity gives us a second layer of firewall and protocol protection, required by both the FDA and SOX,” Schaefer says. Integrity enables Edwards to meet the common regulatory requirement to limit and control user access to information by providing control over how, when, and with which resources endpoints can communicate. “We are able to control access more effectively and with more granularity at the desktop level with Integrity than at the router level,” explains Schaefer. Integrity also ensures that endpoints have the latest versions of applications, patches, and service packs and that they are not running any prohibited programs before they are allowed access to the network.

“All the regulations require us to prove that we are enforcing our security policies,” Schaefer adds. “We use the Integrity logs and monitoring features to provide that information in both real-time and historical formats.”

Access for trusted endpoints only

With Integrity’s policy enforcement, Edwards now has the confidence that only trusted endpoints have access to the private and proprietary information on its network. The Edwards security administrator creates policies that define the conditions under which PCs and other devices may be granted access to the network. These conditions include the specific operating system patches, antivirus updates, and application versions that must be present. Endpoints can also be denied access if they are running prohibited programs, like peer-to-peer file sharing applications.

Schaefer has found modifying the policies extremely easy to do. “I can roll out an antivirus update or software patch and within three or four minutes everyone online has the update and anyone offline gets it when they boot up. With Integrity, I know in real-time who has the update and can quarantine anyone who does not receive it,” he says.

Superior security at lowest risk

Integrity also reduces risk. “I can apply a policy all the way down to an individual computer or user without affecting the rest of the company,” Schaefer explains. “This significantly reduces the risk of applying a general change to our physical infrastructure that could impact the network and result in down time and lost revenue.”

He singles out one other security advantage that Integrity has over other products. “Once Integrity is installed, users cannot remove or uninstall the Integrity client, which means no nasty endpoint security surprises.”

Reduced costs

Before Integrity, Edwards had to hire a desktop support partner to inventory every computer for necessary patches—a process that took months and thousands of dollars to complete. “Now with Integrity, I can see that information myself in just few minutes at the Check Point management console,” Schaefer says.

THE EDWARDS LIFESCIENCES FUTURE

For Edwards, Integrity is the foundation for endpoint security on all its desktop and laptop computers. “One of the requirements that we have built into our 2005 security policy manual is that all vendors accessing our network will also need to have some type of Integrity client,” Schaefer concludes.

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

©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, 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, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, 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, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, 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 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.