



# Lock Manufacturer Protects its Network Against Internet Intrusions

A case study in network security

## BACKGROUND

InstaKey is a physical security company with an innovative, patented product and critical secrets to protect. The Denver-based company manufactures high-security locksets with up to 12 factory-preset key configurations. Each lock can be re-keyed at any time, without calling in a locksmith or removing either the key core or the lock from the door.

For this company, protecting physical security and safeguarding network security go hand-in-hand. A web application in the data center tracks the serialized keycodes and allows InstaKey customers to manage their key sets. The customers include everyone from theft-conscious retail chains to security-sensitive government agencies. To protect the InstaKey network - and customers - the company called on Accelerated Network Solutions (ANS), an IT-support services company with a solid reputation in the Denver area. ANS, in turn, called on WatchGuard®.

## CHALLENGE

According to Scott Taylor, IT Director at InstaKey, “With our online key management software package, our customers are able to manage who has what keys, which doors they open, the pinning, type of keyway - pretty much every bit of information about the key configurations. We need solid network security because of our government contracts, and the regulations that go along with them.”

“We had a couple of Cisco PIX firewalls that just did not have the failover we needed, did not have an interface that was easy to manage... they just didn't fulfill our needs at all,” recalls Taylor. So he asked ANS to make a recommendation on replacing the Cisco units with a high

availability solution. Greg Cann, co-founder of ANS, was quick with an answer: “As a WatchGuard partner, we said, ‘yes, of course we can do that’.”

One of Cann’s first recommendations was to run a Qualys security audit to assess the Cisco security posture and establish a baseline. “The report returned about 50 pages of security vulnerabilities against the servers and firewall itself,” recounts Cann. There were 94 vulnerabilities in all. Most were security holes that could expose information that could be useful in a further attack. But 16 were of immediate concern, classified as “confirmed vulnerabilities,” and 5 were deemed to be serious.

## **WATCHGUARD® SOLUTION**

Cann recommended and installed a WatchGuard high availability solution. “For the size of their network, the Firebox® X Core™ 550 e-Series was the right model for the job,” he says. “We installed two of them, working in secondary failover mode.”

The installation itself “was a breeze, because I was able to pre-build the configuration at our offices. We used our standard, rule-of-thumb WatchGuard security set, based on our past work with WatchGuard sales engineers. I don't think I spent more than 45 minutes customizing the security policies for the various proxy agents that InstaKey needed. We were able to create a very secure environment pretty much out of the box.”

## **BENEFITS**

Customers simply expect that, as a security company, InstaKey has no open holes in its own security. Declares Taylor, “The biggest thing for us is that we can now very truthfully and confidently say to our customers, ‘our web servers are secured against any kind of intrusion, so no one's going to break in and steal your data’.”

## **Security Improvements ‘Like Night and Day’**

About a month after installing the WatchGuard solution, Taylor and Cann reran the Qualys scan and compared it to the earlier scan performed when InstaKey was using Cisco PIX firewalls. It flagged just four security notices compared to a previous 94, all at the lowest of the 13 threat levels recognized. “Frankly, I was shocked by the difference,” says Cann. Comparing the Cisco and WatchGuard results was “like total night and day... opposite ends of the security spectrum.”

## **Why InstaKey is ‘Thrilled with the Product’**

According to Taylor, the WatchGuard solution is a perfect fit. “I'm thrilled with the product. For a small company that doesn't have the money to train people on every little thing, it's vital to have a product in here that's easy to manage and that we don't have problems with. We have not had a single solitary hiccup.

“I love the user interface. It's intuitive. Since Greg did the initial configuration, we've been revamping our environment pretty drastically, and I've had to do quite a bit of reconfiguration: opening ports, monitoring them, closing some things down, adding new services. I've done some network security in the past, but not in a long time. I was able to pick it up on my own. You don't have to be a network security guru to understand what the WatchGuard appliance is doing and what needs to be done.”

InstaKey also makes extensive use of WatchGuard VPN. Plus, Taylor is looking at other ways to simplify the task of protecting InstaKey’s desktop users, such as replacing his current web proxy, anti-virus, and anti-spyware solutions with extensible threat management (XTM) security subscriptions offered by WatchGuard.

### **‘WatchGuard is Extremely Good to Our Bottom Line’**

For Cann and ANS, the ease-of-management provided by WatchGuard devices has been an essential business advantage. “It’s a very intuitive user interface, straightforward and easy to take care of - much better than what WatchGuard’s competitors have. I’d estimate that we have over 300 WatchGuard units in service, both Edge and Core appliances. In some cases the clients do the management themselves. In others, we handle it and WatchGuard lets us easily manage multiple devices.”

When it comes to proposals, says Cann, “the products sell themselves. The spamBlocker, WebBlocker and Gateway AntiVirus options help customers who are on the fence realize that, ‘Whoa, I am vulnerable; I do need this kind of protection.’ And the zero day security isn’t just marketing. It’s real, ready to go out of the box, and nobody else offers it.”

Concludes Cann, “WatchGuard is extremely good to our bottom line. They’re priced correctly, they’ve got the right feature sets, and we’re very happy with the relationship. In fact, we rarely lose a firewall opportunity when we recommend a WatchGuard.”

---

**ADDRESS:**

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

**WEB:**

[www.watchguard.com](http://www.watchguard.com)

**U.S. SALES:**

1.800.734.9905

**INTERNATIONAL SALES:**

+1.206.613.0895

**ABOUT WATCHGUARD**

Since 1996, WatchGuard Technologies has been building award-winning network security solutions that combine firewall, VPN and security services to protect networks and the businesses they power. These fully extensible threat management (XTM) solutions feature reliable, all-in-one security, scaled and priced to meet the unique security needs of small businesses to medium sized enterprises. Our products are backed by 7000 partners and 450 employees representing WatchGuard in 120 countries. More than a half million signature red WatchGuard security appliances have already been deployed worldwide in industries including healthcare, education, and retail. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Firebox are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE6660\_072409