

Community Bank Secures Data and Streamlines Regulatory Compliance

Premier Valley Bank uses a Self-Defending Network and 24-hour monitoring from HEIT to create an adaptable, end-to-end defense system.

EXECUTIVE SUMMARY
<p>PREMIER VALLEY BANK</p> <ul style="list-style-type: none"> • Industry: Financial Services • Location: Fresno, California, United States
<p>BUSINESS CHALLENGE</p> <ul style="list-style-type: none"> • Protect sensitive financial data and customer information • Block Internet attacks that could compromise data and reduce network performance • Develop more efficient, automated auditing and reporting capabilities to meet regulatory requirements
<p>NETWORK SOLUTION</p> <ul style="list-style-type: none"> • Deployed a Cisco Self-Defending Network to provide intelligent network- and host-based intrusion prevention capabilities • Enlisted services from HEIT for advanced FFIEC auditing and reporting
<p>BUSINESS RESULTS</p> <ul style="list-style-type: none"> • Attacks blocked before they can damage the network or reach customer data • Dramatic reduction in time and resources required for auditing and reporting • Greater peace of mind through tighter control over access to financial data

Business Challenge

Protecting against network attacks makes good sense for any business, but for financial services companies, it's not just a good idea—it's the law. State and federal regulations require banks to demonstrate that they have solutions in place to block network attacks and protect customer information at all times. These requirements help safeguard financial data, but they also can present a significant challenge for banks—especially for smaller institutions with limited IT resources. Premier Valley Bank (PVB), a leading community bank with eight locations in Central California, was no exception.

PVB must comply with a broad range of information security regulations from the Federal Financial Institutions Examination Council (FFIEC) and the California Department of Financial Institutions. In periodic audits, PVB must demonstrate that it has deployed strong network defenses and must provide

detailed records documenting every security event that the bank encounters, as well as the response. Although PVB's previous network security solutions provided an acceptable level of protection, the reporting capabilities were sorely lacking, making preparations for regulatory audits a time-consuming, cumbersome task.

"We had a firewall solution in place, but it didn't provide very good documentation of what events took place, when they occurred, and what we did about them," says Carl Goodman, information technology manager at PVB. "I had to spend about an hour every day manually reviewing logs just to understand what was happening in our environment. When we had audits, pulling the meaningful information out of the logs to prepare reports could take eight to nine hours."

Beyond the reporting inefficiencies of the security solutions, PVB leaders were also concerned that security itself was not as robust as it could be. The bank largely relied on perimeter defenses. Although the bank's firewall blocked most threats, some attacks did manage to make their way into the network. The system also provided little visibility into the real-time security state of the environment, and included very few tools for recognizing attacks in progress. In addition, even

when malicious threats were blocked, the attacks could sap network performance and impede the banking applications upon which PVB customers and staff rely.

“Every few months, we would have malicious programs trying to attack our network multiple times a day, which could really slow down our traffic,” says Goodman. “It could affect our network for several days, or as long as a week. It was a real problem.”

Ultimately, PVB needed a more proactive, intelligent, and comprehensive network security system.

“We haven’t had any issues with attacks reaching our network or slowing down our performance since we adopted this solution. They don’t even get past our first layer of defense.”

—Carl Goodman, Information Technology Manager, Premier Valley Bank

Network Solution

After weighing several options, PVB leaders turned to HEIT to help them overhaul the network defenses. HEIT—recipient of the Cisco® Financial Services Partner of the Year Award in 2006, 2007, and 2008—offered a complete managed security service that included assistance with deploying new security technology, as well 24-hour remote monitoring. HEIT has been a longtime leader in the financial services industry, and its technology recommendations are based on years of industry experience and a comprehensive understanding of financial regulatory compliance requirements. At HEIT’s recommendation, PVB deployed a Cisco Self-Defending Network.

Instead of providing security services through a single device or a single point in the network, the Cisco Self-Defending Network model integrates security throughout the environment. In this way, the entire network becomes an intelligent defense system, capable of recognizing, preventing, and adapting to threats automatically.

“Providing defense at the network edge is fine, and that’s what most other manufacturers are doing,” says R. Zaid Akhter of HEIT. “But if you want to prevent attacks at all levels of your network, no one has anything close to the Cisco solution.”

Patrolling the Network Perimeter

With HEIT’s assistance, PVB deployed a Cisco ASA 5500 IPS Solution to provide robust firewall and intrusion prevention system (IPS) services. The IPS solution builds on conventional intrusion detection system (IDS) technologies by not only recognizing malicious attacks, but taking steps to actively block them. And, by integrating industry-leading firewall technology, multivector threat protection, and robust policy enforcement mechanisms into a single device, the solution provides an unparalleled tool for recognizing and responding to suspicious network activity in real time.

As part of the HEIT service, remote technicians monitor the Cisco IPS solution at all times. With detailed, up-to-the-minute threat information, HEIT can rapidly determine whether an incident is legitimate traffic or a genuine attack, and when necessary, use the powerful Cisco IPS mitigation capabilities to halt attacks in progress.

“Before, our firewall would block some traffic coming in, but the Cisco IPS solution actively detects threats and circumvents them,” says Goodman. “That capability alone gives us 24-hour armor.”

Locking Down Desktops and Servers

To extend visibility and defense capabilities beyond the network perimeter, PVB deployed Cisco Security Agent on all desktops and servers. A host-based IPS solution, Cisco Security Agent goes beyond conventional antivirus systems by monitoring actual operating system (OS) behavior, instead of simply looking for signatures of known attacks.

“With a signature-based system, it’s always possible that a new attack won’t be recognized and will make it through your defenses,” says Akhter. “That’s why Cisco Security Agent is so valuable. Even without identifying a specific virus, it can recognize if a process is trying to overwrite data on the hard drive, or log keystrokes, or send information out over the Internet, and immediately block that activity.”

In addition to protecting the desktop or server on which it’s deployed, Cisco Security Agent also communicates with the Cisco IPS system at the network perimeter to alert it to any new attack it has encountered. Together, the solutions create an environment that is able to continually adapt to changing threats.

“There are a lot of other IPS solutions out there, but they can’t provide that kind of proactive communication between the network level and the desktop level,” says Akhter. “That’s an extremely powerful capability, and I’m not aware of anything else that can do that.”

With the ability to monitor the behavior of any desktop PC—and by default, any user of that PC—Cisco Security Agent also provides Goodman with new tools for enforcing corporate security policies and protecting customer information.

“Windows security prevents users from installing software on their own, but sometimes a program running in the background might try to install something,” says Goodman. “Cisco Security Agent blocks all of that. It also prevents users from saving data to any floppy disk, CD, or flash drive. It gives me much more control over the desktop than I had before.”

Managing Security Information

To bring all of the security information in the environment together and provide more sophisticated reporting capabilities, PVB uses the Cisco Security Monitoring, Analysis, & Response System (MARS). Cisco Security MARS aggregates and synthesizes the massive amounts of security data generated in the network, and uses sophisticated event correlation and validation intelligence to help HEIT engineers appropriately identify and respond to threats. The solution provides intuitive topology maps to track attacks in real time and integrates with PVB’s Cisco routers, switches, and security systems to block attacks in progress.

In just one month in December 2007, PVB’s Cisco Security MARS evaluated more than 29 million events. The solution filtered that down to nearly 18,000 suspicious incidents, eliminated thousands of false positives, and blocked the rest automatically.

Business Results

Today, PVB has much stronger, more proactive, and more intelligent network defenses. The bank can easily demonstrate compliance with all state and federal information security regulations, and more importantly, can protect customer information better than ever before. In fact, with the sophisticated Cisco solutions and 24-hour monitoring from HEIT, the bank has virtually eliminated attacks compromising the network.

“We haven’t had any issues with attacks reaching our network or slowing down our performance since we adopted this solution,” says Goodman. “They don’t even get past our first layer of defense. The minute a hacker tries to scan a port, that port gets shut down immediately. HEIT sees what’s happening right away, and they block that IP address and keep us going.”

The key to this improved defensive capability is the fact that all of the Cisco solutions work together as a single, intelligent system.

“The Cisco solution isn’t just providing one component that PVB needs, it’s providing an end-to-end solution that extends from the network perimeter to the desktop,” says Akhter. “In the past, their security solutions operated independently, each in its own way. Now, we have the capability to bring all of the pieces together into a single, adaptable system that can communicate and take whatever measures are required at any time.”

Beyond the improved protection, the biggest benefit to Goodman’s team is the ability to maintain a universal view of the network, and to generate detailed, customized reports for any regulatory or audit requirement.

“The Cisco Security MARS pulls all of the meaningful information out of all of the device logs, and creates a report that almost anyone can read,” says Goodman. “Instead of spending hours collecting information for auditors, I can just print out a customized report and hand it to them. I’d estimate that the man hours we’re saving from that capability alone saves us US\$10,000 annually.”

The expert, continuous network monitoring capabilities provided by HEIT also make it much easier for Goodman’s team to manage the network and its security, and to respond to any problems that arise.

“The HEIT staff is very well trained, and we have a direct line to a technician for any situation we might encounter,” says Goodman. “We’re not calling a national number somewhere and getting routed somewhere else. When we talk to their technicians, they know us personally, and they know our network inside and out. It’s like having an extension of our internal staff.”

Ultimately, the managed service from HEIT and the Cisco Self-Defending Network provide greater peace of mind for Premier Valley Bank and its customers.

PRODUCT LIST

Routing and Switching

- Cisco 2800 Routers
- Cisco Catalyst® 3560 Series Switches

Security and VPN

- Cisco ASA 5500 IPS Solution
- Cisco IOS Intrusion Prevention System
- Cisco Security Agent
- Cisco Security MARS

Unified Communications

- Cisco Unified Communications Manager
- Cisco Unity
- Cisco Unified IP Phones 7941 Series

“Our customers can feel confident knowing that we have one of the leading security companies in the world protecting them,” says Goodman. “We’re protected 24 hours a day, seven days a week, and we can respond to any issue to better protect their information.”

For More Information

To find out more about Cisco IPS solutions, Cisco Security Agent, and the Cisco Self-Defending Network, visit <http://www.cisco.com/go/security>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)