

Arbor Peakflow X Provides Cost-Effective Security for Investment Bank Thomas Weisel

Customer

Thomas Weisel Partners (TWP) is an investment bank specializing in the growth sectors of the economy including the technology, healthcare and consumer sectors. Its nearly 600 employees include Investment Banking, Brokerage and Equity Research groups that serve U.S. and international emerging growth companies and institutional investors.

Challenge

TWP's IT staff was spending too much time in often unsuccessful attempts to identify and block a growing number of worms, viruses, Botnets and other malware, including zero day attacks.

Solution

Arbor Peakflow X has given TWP's IT staff a better view into network traffic. This allows the IT team to detect and block attacks, and to shut down unauthorized network use, without the need for multiple, costly point solutions or added workload for the IT staff.

Results

Arbor Peakflow X provides TWP's IT staff the in-depth network traffic details and visibility it needs to identify and block viruses, worms and other malware in far less time and at far less cost than before. Arbor Peakflow X has also allowed the IT department to identify and stop unauthorized network use such as rogue instant-messaging accounts and peer-to-peer file sharing.

Peak Performance for Fast-Growing Customers

Like the fast-growing companies it serves, TWP prides itself on having an entrepreneurial, performance-oriented culture. Its core values are high ethical standards, a strong client-first and team mindset and meritocracy in the workplace. In addition, TWP must meet ever-stricter and more comprehensive rules and regulations governing the security of its information systems, and the financial transactions conducted over them.

Those goals were threatened by a series of malware attacks in the spring of 2005 that reduced user productivity, disrupted systems, and created a massive workload for TWP's IT staff. When one particular worm hit, "We had most of our staff working on the problem to figure it out. It took easily 100 man-hours," remembers Chief Security Officer Beth Cannon... "People were here until 1 am...with an IT department of 34 people, and a lot of other things not getting done, it wasn't good."

Defending the TWP network from attacks was so difficult because, "We didn't have a good way of looking into what was going on in our network—who (the attack) was hitting, where it was going, how it was getting in. It was like chasing your tail," said Cannon. While TWP did employ sniffer software to monitor and analyze network traffic, "We didn't have it up all the time and we didn't have workforce or time to monitor the log file all the time," she added.

Evaluating Security Solutions

TWP had initially considered a network IDS system, but found it would have been too expensive to install the necessary hardware probes throughout its network, and the company didn't want to incur the staff expenses needed to monitor and tune them. Moreover, TWP needed tools to view the inside network activity as well as intrusion activity.

"Finding a single tool that can provide a view into all critical network traffic flow is one of the hardest challenges for a security manager today," says Cannon.

Arbor Peakflow X provided that view. "The first day we deployed it we found machines that were running peer-to-peer software, spyware and adware," she says. "It also found users who were violating TWP's network usage policies, such as one who had installed the Skype voice over IP application on their PC."

Without Arbor Peakflow X to provide a view of critical network traffic TWP would have had to get a single point solution from another vendor to identify and stop the Skype application, with additional cost and requiring more time of the IT staff, says Cannon.

Arbor Peakflow X also allows the IT staff to identify rogue applications such as Instant Messenger (IM) that bypass the company's secure proxy server. That is crucial for TWP because regulations require all IM traffic be logged and archived.

"Finding a single tool that can provide a view into all critical network traffic flow is one of the hardest challenges for a security manager today. Arbor Peakflow X provides that visibility."

Beth Cannon, Chief Security Officer,
Thomas Weisel



Corporate Headquarters

430 Bedford Street
Lexington, Massachusetts 02420

Toll Free +1 866 212 7267

T +1 781 684 0900

F +1 781 768 3299

Europe

T +44 208 622 3108

Asia Pacific

T +86 10 8529 8885

www.arbornetworks.com

Copyright ©1999-2007 Arbor Networks, Inc.
All rights reserved. Arbor Networks, the Arbor
Networks logo, Peakflow and ArbOS are
all trademarks of Arbor Networks, Inc.
All other brands may be the trademarks
of their respective owners.

CS/THOMAS WEISEL/US/0407

Conclusion

Companies that serve entrepreneurial customers need to be nimble. Investment bank Thomas Weisel Partners must provide its fast-growing clients with financial services on time and securely, while complying with complex regulations, and do so with a solution that doesn't bog down its budget and its IT staff with overly complex or costly appliances.

TWP has learned the hard way how quickly viruses and network worms can spread, inhibiting productivity on critical systems. Just as important as time is the need for straightforward solutions that provide a view into network traffic and security threats. As Cannon says, "You don't want 20 point solutions that give you a lot of information," but rather a platform that monitors for all threats and provides the necessary information to help Cannon's IT staff improve network performance.

And just as with its start-up clients, TWP must purchase cost-effective solutions. With an intrusion prevention system, says Cannon, you need probes on every switch. The cost-benefit of Arbor Peakflow X is that it can take in all this data from many different areas of the network without adding a lot of additional infrastructure.

For TWP, Arbor Peakflow is a part of a layered security approach. While the company maintains its perimeter defenses, a lot of what goes on and what we fight day in and day out comes from inside, such as threats which enter through laptop notebooks, says Cannon.

Arbor Peakflow X "helps us to catch things that get around the rules," she says, and allows TWP to focus on its core mission of helping growing companies prosper.

Why Arbor?

With the potential to inflict millions of dollars in damage and lost revenue worms and insider misuse are the most troubling threats faced by network operators today.

Arbor Networks network behavior analysis combats these next-generation network threats. Built on the proven Peakflow Platform, Arbor's solutions provide accurate, real-time awareness of behavior across the entire network, enabling organizations to better secure and more efficiently operate their networks.

Unlike perimeter security tools, Arbor Peakflow X must operate in environments with proprietary protocols and run over core mesh networks with hundreds of distribution and access layer devices. Nowhere is this more important than on the top global financial networks, which are the most advanced and demanding networks in the world.

Arbor Peakflow X allows financial organizations to preserve business continuity and solve the internal network security threat.

About Arbor Networks

Arbor Networks® provides network security and operational performance for the world's global business networks—protecting networks from the service provider cloud to the enterprise core. Arbor Peakflow® products deliver unmatched network-wide visibility, anomaly detection and scalability to defend against current and future threats, including worms, data theft, botnets and more. Arbor Peakflow products enable businesses to harden their networks, maintain business continuity and prevent the loss of customer confidence. Arbor is headquartered in Lexington, MA, with a research and development office in Ann Arbor, MI, and overseas headquarters in London and Beijing.