



Customer Solution Case Study – Extrusion Prevention

Telecom Service Provider Achieves Total Network Control with innovative Data Security Solution.

Overview

Country or Region: Israel

Industry: Telecom Service Provider

Customer Profile

Headquartered in Rosh Haayin, Israel, and operating globally, 013 Barak is the leader in Israeli business telecom. With an integrated service provider model, Barak provides co-location, Internet access, managed network, international voice, Global VPN and pre-paid services.

Business Situation

Service provider security directly impacts the customer's security. Barak needed to mitigate attacks on the network operation in order to minimize the damage to customer retention.

Solution

Extrusion prevention system installed between the public Internet and the internal network. A single XPS sensor running on an IBM x-Series server protects the operation.

Benefits

- Real time response to violations
- Polite learning curve, incremental policy development lifecycle
- Integration with NOC using Nagios
- Powerful event management & forensics
- Capacity to process more traffic
- No additional manpower required

“The built-in accuracy and performance of XPS, means Barak network operations now has a real-time picture of privacy, customer data and network abuse violations.”

Moti Landes, Director, IT Infrastructure and Security, 013 Barak

013 Barak is one of the standout success stories in the liberalization of Israel's telecom industry in recent years. A fiercely competitive market and high-tech-oriented business environment required the provider to see how it could protect its customer information assets from competitors and criminals. After a live pilot on the network backbone, Barak decided to upgrade its internal network security with an extrusion prevention solution based on Fidelis XPS. The new system was implemented and operates 24x7 with no additional manpower. The real-time event handling enables immediate remediation without foot-dragging and bureaucracy.

XPS™ and Extrusion Prevention™ are registered trademarks of Fidelis Security Systems Inc.

Situation

France Telecom, Deutsche Telecom and Sprint established 013 Barak in 1997 together with the Israeli companies ClalCom and Matav as a joint venture into a newly privatized Israeli telecom market.

Barak quickly established a leadership position in international voice services with 36% market share providing international direct dialing and toll-free, video and audio conferencing, post and pre-paid calling cards. Barak went on to become the first international operator to provide Internet services and is a specialist in high-speed business Internet connectivity, co-location, and managed services. As the exclusive partner of Equant in Israel, Barak provides global private virtual network solutions to many Israeli businesses.

After a tumultuous period of growth and change in the wake of privatization, IDB acquired the majority holding (over 80%) in 013 Barak in 2005.

There are multiple network threats and vulnerabilities at any service provider and especially so for a highly diversified and integrated provider such as Barak:

- Network operations security directly impacts the customer's security
- 92% of all end-points have Internet access.
- Unprecedented technology awareness of employees in 24x7 network operations and customer support.

- Widespread usage of removable USB
- 30% of workstations are "hot seats" with multiple profiles
- 60% turnover of customer service staff
- 30% of all head count are temps

- Negative PR affects the operation immediately.
- Legal and regulatory exposure for customer privacy breaches

Therefore, when Open Solutions introduced the Fidelis Extrusion Prevention System, the Barak IT infrastructure group was eager to begin using this internal network security solution to see if it would meet their objectives for protecting key digital assets:

- Business plans
- Operational and performance reports
- Customer data
- Prepaid codes
- Mail and calling card passwords

Barak realized that they were lacking visibility and control of their internal network channels. Director of IT infrastructure and network operations, Moti Landes likes to say: "Extrusion is like a water leak, you don't know how much it costs until you get the bill".

The Barak team quickly grasped the power offered by XPS, and recognized how this technology could provide them with the tool they required to

mitigate vulnerabilities of extrusion, data and network abuse.

The fundamental requirement for the Proof of Concept project that ensued was to disprove what Moti Landes was to later call “the four deadly myths”:

- Stopping hackers protects me
- If I only grant access to employees, I’m protected.
- There are no threats on authorized channels
- There no threats to authorized systems

A Practical Solution

In late summer 2004, Barak began testing and developing policies using XPS on the internal network backbone. The proof of concept project, which lasted 3 months, was driven by a frugal IT management philosophy:

- Don’t be on the bleeding edge of technology; use proven systems
- Pay modest prices for technology.
- Acquire tools and internal capabilities as opposed to developing long-term dependence on consultants.
- Leverage internal knowledge
- Respond to change quickly
- Be transparent to general management

At end of 2004, Barak VP technologies – Nati Perry approved the production implementation.

The proof of concept deployed a sensor attached to a port mirror on a Cisco switch on the internal network backbone. The sensor, a single CPU commodity P4/512MB box, met the

performance objectives of 30GB/hour. In the course of the POC, the team evaluated multi-protocol support, collected feedback, working closely with Open Solutions and building a win-win relationship with the partner.

As Moti Landes explains, “We felt the system might struggle with the challenges of our targets for performance and protocol support, but we found that the protocol decoders and content analyzers worked well out of the box and we were able to put our theories into practice. Granularity of control is excellent: We can detect and control with fine granularity – down to a single PNG file transferred in a MSN Messenger IM session”.

In the course of the POC, a number of violations were detected using out-of-the-box rules for compliance and content monitoring:

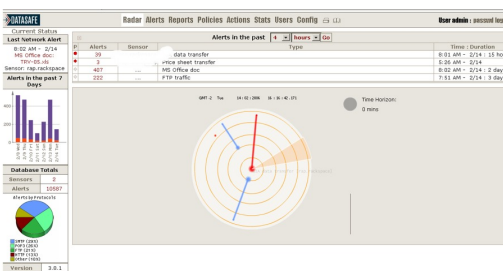
- Unauthorized transfer of Personal data
- Suspected transfer of passwords
- And more...

In January 2005, the solution was deployed using XPS running on an IBM x-Series dual processor server (the sensor).

A second server was deployed for the Command Post™ Apache Web based management and database server. MySQL 4 is used as the event analytics database.

Benefits

The accuracy, flexibility and performance built into the Fidelis



Command Post Radar Page

Extrusion Prevention System deliver a robust tool for mitigating a wide variety of internal network attacks.

Enabling Effective Communication
The Command Post event analytics, combined with the powerful capabilities of MySQL database, enable rapid remediation by reducing the overhead typically associated with tracking progress, reporting status, and monitoring the violations.

As Moti Landes explains: “The Fidelis event database is unique in its simplicity and power to show related events and forensics. The original file can be downloaded from the Web-based Command Post™. It’s a great advantage for us to be proactive, route an event to the security officer and be able tell a user exactly what they did on the spot.”

“The key strength of this technology is the extensible Fidelis protocol decoder and content analyzer architecture.”

Moti Landes, IT infrastructure 013 Barak

Managing the Policy Development Lifecycle

The tightly integrated and extensible lifecycle tools offered increase the productivity of the policy development process. Barak use the system in a continuous cycle of measurement, corrective action and policy refinement.

“As we use it, the Command Post policy development feeds on the results of the sensor and events collected,” says Landes.

Barak could not afford a large enterprise project with multiple stakeholders to meet the company's requirement for content monitoring and filtering.

Landes explains, “We didn't want to bite off more than we could chew and we believe that good development tools are better than a grand integrated strategy of network and content. In the Fidelis solution, no changes to network were needed. The installation was short and sweet; with no need to register content”.

XPS policies are based on logical rule combinations in two dimensions: network channels and content. Using MCP (Multidimensional Content Profiling) the analyst builds metadata descriptors of structured data such as billing reports or prepaid code files. When combined with the network channel rules, high rates of precision (low false positives) and recall (low false negatives) in excess of 99% are attained.

Mapping business processes to XPS policies

While other CMF/ILP systems are based on classification, tagging, registration and detection of content; Fidelis XPS is based on mapping business processes to network channels and content.

For example, the Barak team created channel and content policies to monitor and alert on exceptions in business processes:

- New customer provisioning
- Transfer of billing files to other service providers
- Transfer of account information to business clients.
- Customer support using MSN Messenger

Building an Extensible Security Platform

XPS is a powerful assistant to Barak's firewall and inbound content filter proxies. For example, users who bypass the enterprise Web proxy or users who elevate privilege to obtain SSH access to a production document exchange server are quickly identified.

Moti Landes, enthusiastically explains, “The key strength of this technology is its extensible protocol decoder and content analyzer architecture”. For example,” Landes continues, “as Web mail applications evolve, the engineering team can create an updated 'network channel' fingerprint used by the Webmail disclosure control rule in our enterprise policy. When you change a fingerprint, the policy automatically inherits the change”.

Gaining Powerful visibility and granularity of control
Suspected violations display immediately and clearly. The Command Post employs an ANN (Adaptive neural network) to classify and compress events by three orders of magnitude, solving the “event flood” challenge endemic in IDS systems. Using the built-in event workflow, a suspected violation of AUP can be routed immediately to the corporate security officer for corrective action.

Ensuring project success
Barak agreed that the information collected from the POC was crucial in building the business case and ensuring project success. Moti Landes summarizes 5 steps to ensure a successful implementation of an extrusion prevention solution:

- Look at your own network for threats and vulnerabilities; you’ll be surprised by what you find.
- Collect live-fire examples from the Fidelis XPS™ sensor
- Show some examples to the decision makers
- Start small & start early; allocate money and act quickly
- Do the implementation in “baby steps”

For More Information

For more information about Fidelis products and services, call the Fidelis Sales Information Center at 1-(800) 652-4020.

Acquire XPS

In Europe, the Middle East and Africa please contact Open Solutions Israel at +972-3-610-9750 or sales@opensolutions.co.il

To access information using the World Wide Web, go to: www.fidelissecurity.com

Fidelis XPS-Extrusion Prevention system

XPS provides bi-directional analysis and active control of client/server application connections. Key benefits are:

- Quick implementation, to effectively enhance existing IT security capability.
- Real-time visibility to channels, including tunnels and embedded content
- Deep, format-independent analysis of intercepted content in over 150 file formats.
- Wide range of content analysis methods - keywords in context, embedded pictures, file fingerprints and many more.
- Active countermeasures for a wide range of attacks such as: Trojans injected through back channels and physical CD-ROM's, IM file transfers, Web mail, elevation of privilege and rogue encrypted channels.

Software and Services

■ Open Solutions eRisk customer data audit system.

■ Technologies

- Fidelis XPS: Extrusion Prevention System
- IBM X-Series servers

Business Partner

– Open Solutions Israel
www.opensolutions.co.il

■ Operating System

- Red Hat Enterprise Server 3
- MySQL 4
- Apache 2

© 2006 Fidelis Security Systems. All rights reserved. This case study is for informational purposes only. FIDELIS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Fidelis, XPS, CommandPost, and Extrusion Prevention System are either registered trademarks or trademarks of Fidelis Security Systems in the United States and/or other countries. All other trademarks are property of their respective owners.

Document published April 2006