



“Bezeq International’s prime security concerns are around data integrity and compliance with the regulations that surround data integrity. BIG-IP ASM delivers on both counts.”

Ami Hoffman, Information Security Director. Bezeq International

## Bezeq International Protects Customer Data and Adheres to Regulations Using F5 Solutions

**Bezeq** is Israel’s largest telecommunications group. Bezeq International, a subsidiary organization of the Bezeq Group, is an ISP and hosting provider with more than 1 million customers, ranging from small businesses to large enterprise and government organizations.

By using F5® BIG-IP® Application Security Manager™ (ASM), Bezeq International has been able to protect sensitive information that is exchanged between the company and its customer base and also comply with a variety of industry and legal requirements concerning data integrity.

### Business Challenges

Bezeq International’s decision to review security for its web properties was driven by regulatory need as well technology issues, specifically related to maintenance and product roadmap concerns.

Securing application transactions involving credit cards was a key requirement, due in part to industry, national, and international regulatory requirements. The Payment Card Industry Data Security Standard (PCI DSS), which includes requirements for security management, policies, and procedures, as well as the provisions of the Sarbanes-Oxley Act, dictate the company’s security stance to a great degree. Local Israeli banking

and insurance regulations and the Health Insurance Portability and Accountability Act (HIPAA) also affect Bezeq International’s data security actions.

In addition, Bezeq International aimed to reduce the amount of manual maintenance required to keep security at an acceptable level and provide more protection for the company’s web servers to guard against SQL injection and denial-of-service (DoS) attacks.

### Solution

A total of six F5 BIG-IP ASM devices running on the BIG-IP 6400 platform were

## Overview

### Industry

Telecommunications

### Challenges

- Adhere to industry regulatory requirements
- Reduce security maintenance time
- Defend against data integrity attacks

### Solution

- BIG-IP Application Security Manager

### Benefits

- Enabled PCI DSS and Sarbanes-Oxley compliance
- Reduced server infrastructure by 25%
- Secured data integrity
- Maintained fast application response times

deployed in two locations: in a data center that is mainly devoted to the Bezeq core telecommunications business and in a facility dedicated solely to Bezeq International's hosting business. Both are based in Petach-Tikva.

Bezeq International uses tools to scan application source code for vulnerabilities and employs penetration testing to assess the strength of the company's defenses.

BIG-IP ASM forms part of a multi-layered defense of Bezeq International's approximately 30 web properties. The types of applications protected include marketing sites and customer self-service web portals, where sensitive data is frequently sent and received. Bezeq International employs very few off-the-shelf applications; most are developed by the company's in-house team using Java and Microsoft .NET.

"We use the latest 10.2 version of BIG-IP software," said Ami Hoffman, Information Security Director at Bezeq International. "Our web properties are very dynamic and always changing. The new automatic policy builder features of version 10.2 mean we can adjust our security stance to reflect these changes very easily, which is enormously beneficial in maintenance terms."

Bezeq International also uses F5 iRules,<sup>®</sup> an event-driven scripting language that allows for direct control and management of IP application traffic. As a testament to their flexibility, iRules are used at Bezeq International for debugging, access control, HTTP header filtering, traffic redirection, as part of the company's DoS defense, and much more.

"The contrast between our previous web application firewall and BIG-IP ASM is marked in many ways," said Hoffman. "Deployment was trouble free, and in terms of ongoing administration, there is

no comparison. BIG-IP ASM is much less demanding in that sense."

### Benefits

BIG-IP ASM has helped Bezeq International rapidly patch web application vulnerabilities so that the company can comply with government and industry regulations such as PCI DSS and HIPAA.

"Bezeq International's prime security concerns are around data integrity and compliance with the regulations that surround data integrity," said Hoffman. "BIG-IP ASM delivers on both counts."

Bezeq International's web properties are scanned hundreds of times on a daily basis, mostly by attackers conducting sweep scans to look for open ports to try to identify the software applications the company uses. Following this, more advanced techniques like SQL injection are employed to try to exploit web server vulnerabilities. Most attacks are filtered out immediately, and any that make it to BIG-IP ASM are generally dealt with through policy rules.

"I'm happy to say that, during my time at Bezeq International, we never suffered from a major compromise," said Hoffman. "Not even one case where a DoS attack or defacement was successful. BIG-IP ASM has played its part in ensuring that we faced only minor issues that were identified easily and handled within BIG-IP ASM policy."

Further, the BIG-IP 6400 devices have also delivered top performance. Bezeq International uses BIG-IP platform application traffic compression, acceleration, and SSL offload capabilities to reduce CPU load on its application servers. This has enabled the company to reduce its server count by about 25 percent, saving on power, space, and financial outlay. The performance capacity of the 6400 devices

means BIG-IP ASM isn't a drag on application response times either.

Finally, the flexibility of iRules has enabled the company to use multiple custom methods of controlling and managing web application traffic. One of the simplest, implemented at a cost only in time and requiring no application code tweaks, addresses DoS attacks. When a threshold number of connections comes in from a DNS or mail server, an iRule recognizes that the threshold has been breached and blacklists the server for a short period of time, before moving it back into the pool automatically. If these unwanted characteristics continue to be displayed, the server will again be blacklisted.

Having introduced BIG-IP ASM to Bezeq International, Hoffman is now responsible for all F5 projects within the company. Following the success of BIG-IP ASM, BIG-IP<sup>®</sup> Local Traffic Manager<sup>™</sup> devices have been brought into Bezeq International to replace the previous load balancing solution.

"We've worked hand-in-hand with F5 as BIG-IP ASM has been developed over a number of years," concluded Hoffman. "We bought into F5's vision, and it's been an excellent decision for us."

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.  
Corporate Headquarters  
info@f5.com

F5 Networks  
Asia-Pacific  
apacinfo@f5.com

F5 Networks Ltd.  
Europe/Middle-East/Africa  
emeainfo@f5.com

F5 Networks  
Japan K.K.  
f5j-info@f5.com

