



Sergey Khimanych
Information Security Expert
MegaFon

TELECOMMUNICATIONS LEADER MEGAFON PROTECTS WEB SERVICES WITH POSITIVE TECHNOLOGIES APPLICATION FIREWALL

THE CHALLENGE

Protect 12 key web applications that service 60,000 user requests per second

To stay competitive, MegaFon has to move quickly to meet the growing demands of its more than 70 million mobile subscribers. In response to its customers' need for more convenient services, MegaFon has developed and launched several new self-service Web and mobile applications, and it expects to roll-out many more applications in the near future.

To deliver these applications quickly and stay flexible to changing customer requirements, MegaFon adopted collaborative software development methods such as DevOps and Agile. While these approaches have helped MegaFon's development team stay nimble, they leave little time for security analysis of the developing code or implementation of other recommended secure software development lifecycle (SSDL) practices. The situation is further complicated by the pace of MegaFon's business, which leaves developers little time to even address the vulnerabilities that have already been identified. And in many cases, application code has been inherited through acquisition and cannot be fixed to eliminate known security flaws.

"As a services company, we must be sure that our clients and web resources are well protected", says MegaFon information security expert Sergey Khimanych. "The world is changing and threats are growing. Like other companies our size, our web services are constantly under attack, from port scanning to attempts to hack into our client's personal accounts. We have to be confident that our web resources are always reliably protected."

COMPANY PROFILE:

- + Industry:
Telecommunications
- + Customers: 70 million
mobile subscribers
- + Revenue: USD \$5.6 billion
(2013)
- + Corporate Structure:
Privately held. Key
shareholders include AF
Telecom and TeliaSonera
- + Established: 2002 (formerly
North-West GSM)

MegaFon needed a Web application security solution that would be:

- + Highly performing, efficient and fault-tolerant
- + Rapidly adaptable to changes in protected applications, ensuring stability of security levels
- + Capable of working across geographically distributed systems
- + Compatible with its existing protection mechanisms such as IPS, DLP and Anti-Virus technologies
- + Able to mitigate security flaws even when source code could not be changed
- + An early warning system against evolving security threats by identifying unusual behavior by users or applications

THE SOLUTION

Positive Technologies Application Firewall

After a rigorous vendor selection process, MegaFon chose Positive Technologies Application Firewall™ to protect 12 separate web and mobile applications that receive up to 60,000 user requests per second. In addition, PT Application Firewall has been integrated with the MegaFon's existing Security Information and Event Management (SIEM) solution.

"We can see what is going on with our web services and in case of an alert we can change the system configurations to improve our security levels."

Sergey Khimanych
Information Security Expert
MegaFon

HIGHLIGHTS

- + Blocked zero-day attacks and obtained early warning of fraud through behavioral analysis
- + Quickly neutralized known vulnerabilities with virtual patches
- + Secured obsolete and third-party applications where source code could not be changed
- + Reduced false positives with self-learning and automatic correlation of vulnerabilities

PT Application Firewall's virtual patching feature allows MegaFon to quickly close security holes exposed by vulnerabilities that are detected by MegaFon's existing security tools, including the MaxPatrol™ vulnerability and compliance management solution from Positive Technologies. PT Application Firewall's virtual patches maintain application security levels while the company's development team eliminates the vulnerabilities. Additionally, virtual patches provide long-term protection for legacy and third-party applications where MegaFon cannot update the source code.

PT Application Firewall also plays a key role in the early detection of web fraud attacks by using behavioral analysis to identify unusual client behavior and unauthorized activity by network bots.

Sergey Khimanych says MegaFon wanted to be sure it was entering into a long-term partnership: "We selected Positive Technologies because we trust that they will continue to develop their product and keep an open dialogue with companies like us to satisfy our specific requirements and features sets."

PT Application Firewall can be supplied either as a hardware appliance or on a software-only basis for customers who prefer to procure their own hardware. MegaFon opted for the hardware appliance in order to optimize performance.

THE BENEFITS

Provide early warning of attacks, secure legacy applications, control costs

"With Application Firewall we can now detect and track attacks as they happen," says Khimanych. "We can see what is going on with our web services and in case of an alert we can change the system configurations to improve our security levels."

MegaFon has been able to improve efficiencies and control costs within their Information Security department thanks to PT Application Firewall's self-learning mechanisms and its automated verification and correlation of attacks and vulnerabilities. Together, these capabilities drastically limit the number of false positives and filter and prioritize risks. This lets MegaFon's security specialists concentrate on tackling high-priority events quickly rather than spending countless hours manually sifting through mostly insignificant data.

"My company is a longtime customer of Positive Technologies", says Khimanych. "We have been co-operating together and successfully using their products for years. As usual, the experts at Positive Technologies were open to hearing about our specific needs and we were very satisfied with the quality of their results."

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit www.ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of \$20M+.

© 2015 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.

