



TrafficShield™ Internet Technology Company Relies On F5's TrafficShield To Protect Their Critical Application Data

Executive Summary

An Internet Technology firm relies on a web application that consists of a large variety of internally developed ASP pages running on IIS web servers. The ASP pages themselves interact with a SQL server database back-end, and are used to quickly track and view customer and employee data and ultimately provide better customer support.

Protecting this IT company's high value customer data, as well as their internal employee data, was key. Other goals included:

- The people supporting the application did not write it and didn't know how it worked - they required a tool to give them a greater understanding.
- Providing a checks-and-balances system for Development before any changes were made. This meant validating the input of data and placing restrictions on those inputs.
- Lowering the security responsibilities, duties and associated costs for Developers with a device that automatically enforced pre-defined security policies.

Challenge Vulnerabilities in the web server or the application could potentially be used in an SQL injection attack. This company had a series of perimeter firewalls in place but on the intranet it relied upon the built-in security features of the various software applications they used in-house. And since the web application itself was housed on the intranet, anyone who hacked into the intranet (or a rogue employee on the inside) could gain access to the application - and from there tunnel into more sensitive data.

Vulnerability scanning was done on the application to assess the security exposure - and, in addition to the known vulnerabilities, a Denial of Service vulnerability was found - but the company's IT department elected not to try to fix those and other vulnerabilities via their Development team because of limited time and resources.

"It was basically a cross-your-fingers approach that nobody bad was on the inside or that no outside hackers gained access to our internal network," stated one network engineer.

Solution The Company discovered F5's TrafficShield, an application firewall that provides comprehensive, proactive, application-layer protection against both generalized and targeted attacks.

TrafficShield is a hardened appliance that sits in front of servers, protecting them from attacks and ensuring that only valid responses get through. Even the most sophisticated attacks can be efficiently identified, isolated and eliminated without impacting legitimate application transactions. And because it includes a variety of mechanisms for automatically generating and enforcing application security policies, it reduces manual processes while improving overall security.

By running TrafficShield in 'passive mode', the company's IT personnel were able to gain a greater understanding of the application.

"It gave IT a better understanding of what the application was doing, what it was supposed to be doing, and more importantly, what stuff was going through that shouldn't be," said the network engineer.

When TrafficShield was in its active blocking mode, it allowed IT to ensure that a developer did not add functionality that might introduce a new vulnerability into the network.



"The developer could not put new code and functionality on an application without first following specific pre-defined policies," said the network engineer. "In this way it prevents 'rogue developers' from putting more stuff up without any checks and balances. Nothing can go through that you didn't already pre-define."

In addition, TrafficShield also played an important role in helping the Development team find previously non-disclosed bugs in the network. For example, extensive TrafficShield logging capabilities helped diagnose which links were not working. Previous to TrafficShield, everyone was blind to this knowledge.

"Their might be a bug in the application that nobody bothered to tell us about," said the network engineer. "TrafficShield now informs us, allowing us to fix the problem more proactively."

TrafficShield's logging capabilities also helped overcome a problem associated with accessing data through BlackBerry devices. The browsers of these devices are very "chatty", and those clients were exceeding the input limits in TrafficShield. The problem was very easy to diagnose and overcome using the TrafficShield logs, and then fine tuning the configuration.

"We might have issues with browsers acting in ways we didn't expect," said the network engineer. "But with TrafficShield, we can constantly re-tweak our idea of what is and what isn't appropriate coming from our clients."

TrafficShield is also ideal for the company's developers who often don't have time to delve deeply into myriad security issues.

"Our busy application developers are very happy that they don't spend their hours being so security conscious," said the network engineer. "With TrafficShield, they can just point-n-click, and all the data is as it should be. The security responsibility now rests with TrafficShield."

Recent vulnerability testing has already proved TrafficShield's worth for this company. They were able to see in the logging that TrafficShield was pro-actively blocking the kind of hits to the server that are well-known Windows/IIS vulnerabilities. The IT department is now satisfied that developers are unable to make unplanned changes to the application that wasn't supported by policy, ultimately improving the company's overall security posture. They have a complete view into the application - what it's doing, and what might be going through that shouldn't be.

And thanks to the F5's TrafficShield Professional Services team - the support network behind the product -the company was able to quickly set up various policies and understand all that TrafficShield had to offer.

"They did an excellent job of guiding us through," said the network engineer.

About F5 F5 enables organizations to successfully deliver business-critical applications and gives them the greatest level of agility to stay ahead of growing business demands. As the pioneer and global leader in Application Traffic Management, F5 continues to lead the industry by driving more intelligence into the network to deliver advanced application agility. F5 products ensure the secure and optimized delivery of applications to any user - anywhere. Through its flexible and cohesive architecture, F5 delivers unmatched value by dramatically improving the way organizations serve their employees, customers and constituents, while lowering operational costs. Over 9,000 organizations and service providers worldwide trust F5 to keep their businesses running. The company is headquartered in Seattle, Washington with offices worldwide.