



“F5’s Application Security Manager is critical to our risk management model ... No other technology let us do this level of traffic. It is a great product, and I am a huge proponent.”

Mark Nagiel  
VP of IT and Information Security,  
InCharge Institute, Orlando, FL

## InCharge Institute Uses F5 Application Security Manager to Control Risk Management Strategy

### Industry

Personal finance education and credit counseling

### Challenges

- Traditional risk of unmonitored port 80 and port 443
- Security and protection of sensitive data in the system
- Challenge of integration with internally-developed and third-party applications

### Solutions

F5 BIG-IP® Application Security Manager, version 9.1, build 29.0

### Benefits

- Enhances ability to manage risk
- Provides us insight and knowledge of the DMZ
- Shows type of traffic and the risk

### Overview

Based in Orlando, Florida, [InCharge® Institute](#) of America is a national non-profit community organization specializing in personal finance education and credit counseling. Under its umbrella are several businesses:

- Brightscore.com helps clients monitor and get current up-to-date information from credit agencies
- InCharge Educational foundation offers educational products and services that support the personal financial literacy needs of consumers nationwide
- InCharge Debt Solutions which offers confidential and professional credit counseling, debt management, financial education programs
- InCharge radio network broadcasts financial education programs in nearly 400 markets

Together, these organizations are committed to helping financially distressed families and individuals pay off their debts—and learn to use credit responsibly.

As a financial organization, InCharge Institute is very protective of its customers and the sensitivity of their financial records, so it is essential for the organization to have an aggressive risk management program in place.

### Challenges

Mark Nagiel, vice president of IT and information security, oversees ‘all things IT’ at InCharge Institute, including traditional networks, the web environment, back-end and front-end support, business continuity, and software development, both internal and third party. Fifty individuals are part of the IT staff.

With a mature information system architecture, InCharge has several key applications that have been internally developed. The primary application, called *Freedom*, allows InCharge to process and support individuals with counseling, and allows interaction with customers, and is a web-based model.

For InCharge Institute, protecting sensitive customer data is a major concern. “We take a holistic approach, providing security measures at the presentation layer, SSL to client, to our back-end database. We have to protect the perimeter of the system internally.” Risk types include cross site scripting, cookie poisoning, SQL/OS injection, and the traditional risk of an unmonitored HTTP (port 80) interface facing environment.

When Nagiel first joined InCharge, he’d audited the IT environment. Their standard port 80 and HTTPS (SSL/TLS at port 443) traffic was open/negotiable, and InCharge needed the ability to close the loop. “We went through a thorough





analysis before making our product selection,” said Nagiel. “Because our applications are internally developed, our challenge is to wear both the IT and security hats.”

I proposed to the board that we needed to enhance our ability to manage risk, and they considered a critical need,” he said. “InCharge has a large portfolio of individuals, and it is due diligence for us to protect that asset,” said Nagiel.

### Solution

Previously having worked with F5’s BIG-IP solutions when he was other organizations, Nagiel included BIG-IP Application Security Manager (ASM) in his search for a solution for InCharge Institute that would enhance its risk management program.

F5’s Application Security Manager delivers comprehensive protection for web applications and operational infrastructure. BIG-IP ASM employs an auto-adaptive approach to application delivery security, where the security policy is automatically updated based on observed traffic patterns. This simplified approach to configuration makes implementation and maintenance easier, reducing the overall total cost of ownership. BIG-IP Application Security Manager is available as a product module for BIG-IP, but is also available as a standalone appliance, which is how it is implemented at InCharge.

“F5’s Application Security Manager allowed us to fill that need to complete our risk management model,” said Nagiel. “It is adaptable—and we know we can rely on this solution for the long-term,” he added. “This project helps us close the loop in our security infrastructure, so our management and board of directors have been very supportive of this mission.”

Application Security Manager allows InCharge to see the type of traffic and the risk. “In addition to giving us insight and knowledge on our DMZ, Application Security Manager is a tool that also teaches us how to better write code,” Nagiel said. Application firewalling is a pre-requisite for InCharge. “This is a common, very basic methodology to control the environment,” said Nagiel. “We will see an embedding of security into procedures, because more and more organizations are realizing it enhances risk management.”

Nagiel believes Application Security Manager ASM is a tool that can help transition to security in the development stage. “We presume that development focuses on functionality rather than security—it is difficult to reprogram developers to embrace a security focus,” said Nagiel. The Application Security Manager firewall helps manage security for the long- and short-term. “We are inserting security-related checks into both our development and quality assurance components,” explained Nagiel.

InCharge Institute operates in every state, but regulations can vary—or be non-existent. “We have very efficient processes for the different states,” Nagiel explained. “In New York, for example, we are considered in the same category as a bank, so examiners audit and review our processes, just as they do with any large banking organization,” noted Nagiel. “Application Security Manager helps us show our ability to demonstrate due diligence.”

Once the order was placed, it took 45 days, including training, to deploy Application Security Manager. “We have quite a sophisticated internal IT crew, but we did use the opportunity to bring F5 onsite for consulting and tutorial help,” Nagiel said. “It was

very useful, and a fabulous opportunity for us to gain more knowledge. F5 support has been outstanding, with good follow up,” he added. The ongoing integration process is getting easier, as InCharge implements the solution at its second and third sites, according to Nagiel. “It does get easier. We understand the functionality, so we are more efficient. This is not a trivial application, because we wanted a robust solution,” he said. “But our initial investment in time has paid off.

In terms of requirements, InCharge has standards for encryption and monitoring. “When it comes to credit cards and websites, we follow standards because they are best practices,” said Nagiel. The Credit Bureau audits the InCharge environment every year. “The first year, they spent time on our DMZ and IAS environment,” he continued. “Last time, after we implemented Application Security Manager, they spent no time on it—they felt that covered any vulnerability.”

Nagiel explained that calculating the return on investment is difficult. “The way we view risk is simple: to us, there is nothing more expensive than an incident,” he added. “The cost to purchase and maintain Application Security manager is a small price to pay to minimize the risks. With the inherent nature of port 80 and port 443, no other technology lets us do this level of traffic.”

Putting in a strong perimeter and back-end is essential, according to Nagiel. “If you are not doing this, you are not doing due care. Having port 80 and port 443 exposed is no longer an option,” he said. “I admit I am a ‘belts and suspenders’ guy, meaning I am not willing to take risks or a chance—so this is all worth the effort and cost,” Nagiel said. “F5’s Application Security Manager is a great product. I am a huge proponent.”

**F5 Networks, Inc.**  
**Corporate Headquarters**  
 401 Elliott Avenue West  
 Seattle, WA 98119  
 (206) 272-5555 Voice  
 (888) 88BIGIP Toll-Free  
 (206) 272-5556 Fax  
[www.f5.com](http://www.f5.com)  
[info@f5.com](mailto:info@f5.com)

**F5 Networks**  
**Asia-Pacific**  
 +65-6533-6103 Voice  
 +65-6533-6103 Fax  
[info.asia@f5.com](mailto:info.asia@f5.com)

**F5 Networks, Ltd**  
**Europe/Middle-East/Africa**  
 +44 (0)1932 582 000 Voice  
 +44 (0)1932 582 001 Fax  
[emeainfo@f5.com](mailto:emeainfo@f5.com)

**F5 Networks**  
**Japan K.K.**  
 +81-3-5114-3200 Voice  
 +81-3-5114-3201 Fax  
[info@f5networks.co.jp](mailto:info@f5networks.co.jp)