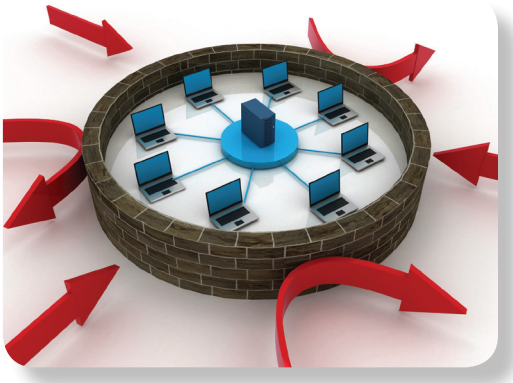
nBreach℠

FIACIA™

Financial Service companies present cyber criminals with lucrative targets of choice. While the industry faces increased regulatory and consumer pressure, individual banking institutions continue to fight against cyber threats such as network breaches, loss of data via malwares (viruses, worms, trojans etc), victimization by botnets, and insider attacks which are twice as likely in Financial Services as in other industries.



It's time for a new approach to securing financial networks, applications, and, most importantly, sensitive financial data.

According to the U.S. Secret Service Data Breach Investigations Report, over 90% of data records compromised belong to the financial sector.

New attacks and methods of exploitation show us that Financial Services companies are migrating from being targets of opportunity to targets of choice for deliberate and skilled attackers. Existing security solutions improve on the shortcomings of past products and services, but fall short.

Wanted: Protection Against Advanced Persistent Threats

According to a study cited in SC Magazine, two-thirds of Financial Services companies say they plan to implement at least one new security technology in the next year. The question is which one(s) ... and why?

Some shortcomings of current technologies:

- Web security proxies are vulnerable to port and protocol-agile threats.
- DLP tools cannot detect embedded malware or defend non-standard ports.
- Firewalls cannot detect content-based threats.
- Intrusion prevention solutions are blind to inside or multi-faceted attacks.
- Anti-virus products miss unknown threats, averaging only a 50% detection rate.

The reality is that there are no silver bullets. Cyber attackers will keep plotting, innovating, and probing your networks. The FIACIA AA6000 and the nBreach(sm) service provides superior protection against hackers' attempts to exploit vulnerabilities in badly configured business servers, applications and networks.

Tailored Solutions:

Our solution has been tailored to meet the needs of most Financial Service companies (banks, brokers, insurers etc) irrespective of their size. At a fraction of the cost, a team of analysts responds to security incidents and sends the appropriate Breach Notification(s) in the event of a breach, to the appropriate parties (affected individuals, Government mandated recipients and the media) as defined by the respective statues governing Network/Cyber security.

Features: of our Managed Network Security solution:

- AA6000 - Unified Threat Management product.
- Managed Firewall Services - Intrusion detection & Intrusion prevention, Data Leakage
- Managed VPN services - Promotes secure virtual private network access for remote users.
- Provides 24/7/365 network monitoring by a team of certified, Security Engineers operating in a Secure Operations Center (SOC).
- Leverages FIACIA's Enterprise class, Unified Threat Management hardware [AA6000]
- Compliance Regulations - FIACIA's NBreachSM solution helps you adhere to the FFIEC, GLBA, FACTA, Sarbanes-Oxley and ITI TF intrusion prevention requirements.
- Monthly Report - a monthly report summarizing all security incidences and detailed resolutions or proposed resolutions.
- Security Bulletins - a notification of a policy change in relation to the network environment.
- Vulnerability Bulletins - a notification of a new security vulnerability or exploit.
- Network Penetration test - a monthly simulated attack to try and breach the protected network. This is an uncoordinated test.
- Log monitoring and retention - a 3 year rentention of the network logs indicating a breach occurred.
- Breach Notification - a notification sent to all affected individuals in the event of a network breach resulting in protected Financial data being compromised.
- Global Network Community Watch - FIACIA is a member of the DShield global cooperative network community watch program. With millions of sensors deployed worldwide working together, security events occurring can be seen as they happen and proactive changes are then made to the Healthcare providers security policy to protect the protected network against emerging threats.

FIACIA Corp
3525 Piedmont Rd NE,
7 Piedmont Center, Ste 300,
Atlanta GA 30305, USA
T: 404.364.1830
E: info@fiacia.org
I: www.fiacia.org