

RFA - DEFENDER



Network Security

Defender is a tiered data protection solution. It is the first line of defense that goes beyond attack signatures for detecting and blocking malicious executables. This powerful, comprehensive solution ensures network security and can be applied separately or collectively to suit your needs.

DEFENDER COMPRISES FOUR KEY ELEMENTS:

1.) MANAGED SECURITY SERVICE

Managed Security combats security threats and meets compliance auditing requirements. This service collects and correlates event data from a variety of network devices including routers, switches, firewalls, VPNs, IDS/IPS systems, proxy servers, antivirus software, spam and spyware filters, content filtering, Web security, Windows, Unix and Linux servers and workstations.

FEATURES

- Automated report generation and distribution
- Automated log archiving for compliance and forensic analysis
- Compliance monitoring
- Intrusion and rule-based reporting

BENEFITS

- Eliminates false positives
- Identifies breaches and corporate violations

2.) MANAGED DATA LEAK PREVENTION

Prevent leakage of sensitive information from data ports, channels and networks with our comprehensive offering. The product combines end point-based enforcement fingerprinting.

FEATURES

- Real-time enforcement by RFA's 24/7 Network Operations Center (NOC)
- Complies with privacy regulations

BENEFITS

- Most comprehensive network wide management of operational risk
- Protects against identify theft

3.) INTRUSION DETECTION

Crime ware and malicious threats are eradicated from the network. RFA's solution protects networks against crimeware and botnets that have evaded antivirus security.

FEATURES

- Protection against crimeware, botnets, hackers, malware

BENEFITS

- Low false positives
- Highest accuracy

4.) E-MAIL SECURITY

RFA provides proactive e-mail protection that detects zero-day threats, targeted attacks, first-instance malware variants and blended threats not detected by traditional security measures

FEATURES

- Observes behavior of suspect messages in virtual environment
- Two layers of antispam filtering

BENEFITS

- Lists unknown threats before pattern-file availability

TOP TIPS

1. Lock down your endpoints where information can get out, such as laptops, USBs, BlackBerrys, etc.
2. Educate your users on best security practices, strong passwords and report lost equipment
3. Look for easy-to-use intuitive tools to alert you to security and compliance violations
4. Update your virus and spyware detection definitions regularly via automation

BOSTON, MA
Inquiries
617.951.4562

PURCHASE, NY
serving
Westchester &
Connecticut
Inquiries
914.729.7401

NEW YORK, NY
Inquiries
212.328.6260

Inquiries@rfa.com
www.rfa.com