

Nokia Intrusion Prevention with Sourcefire 3D Network Security for Nokia IP390

Nokia for Business

Product Description

Nokia Intrusion Prevention is a new security solution that combines hardened, purpose built Nokia IP Security Appliances with "best in class" intrusion prevention technology provided by the Sourcefire 3D System of Define, Determine, Defend. Nokia Intrusion Prevention complements firewalls and allows organizations to add an additional layer of defense to their enterprise security deployments. Based on the successful Nokia IP390 platform in combination with the Sourcefire 3D System, Nokia Intrusion Prevention brings together policy, behavior rules, technology, and automation to protect network entry points, systems, applications and data all the time.

What are the Key Features?

Sourcefire Intrusion Sensor™ for Nokia - Running on Nokia IP390 appliances, Sourcefire Intrusion Sensors inspect incoming traffic for known and unknown anomalies and generate alerts, block traffic altogether, or even replace malicious code with benign code based on pre-defined security policies.

Sourcefire Real-time Network Awareness™ (RNA) Sensor for Nokia - RNA Sensors utilize Nokia IP390 appliances for intelligent network monitoring through a combination of passive network discovery, behavioral profiling, and integrated vulnerability analysis to deliver the benefits of real-time network profiling and change management.

Sourcefire Defense Center™ for Nokia - The heart of the 3D system, Sourcefire Defense Center is capable of handling hundreds of millions of events for identification of long-term security trends, while also allowing in-depth forensic analysis down to the individual packet level.

Why Offer Nokia Intrusion Prevention?

Today the network perimeter is dissolving, introducing new exposed points of access within corporate networks. Additionally, attackers have moved beyond exploiting insecure networks to exploiting vulnerabilities in applications, driving enterprises to adapt a "defense-in-depth" strategy. Still yet, many enterprise exploits come from within the corporate network. Nokia Intrusion Prevention enhances Nokia Firewall/VPN Appliances, providing sophistication and intelligent network security for medium to large organizations, remote campuses and large branch offices.

Who Is The Target Audience?

Nokia IP390 is ideal for small to mid-size enterprises, remote campuses, and large branch offices that need intuitive and flexible, purpose built plug-and-protect appliances to enhance their overall network security deployment.

For additional information on Nokia Intrusion Prevention, contact your Nokia Account Manager or visit: <http://www.nokia.com/connect>.

Nokia Intrusion Prevention At a Glance...



Value Proposition

Nokia Intrusion Prevention features Nokia IP390, a high performance and easy to manage security appliance with Sourcefire Intrusion Sensor and RNA Sensor software. Nokia IP390 is designed specifically for the demanding performance of medium-sized to large enterprise customers, remote campuses or large branch offices. The versatility of Nokia IP390 for monitoring network segments actively (inline) or passively and the choice of throughput performance makes it an excellent choice for deployment throughout the core to defend one or multiple network segments.

Talking Points

Nokia Intrusion Prevention

- Market-leading security and manageability with Sourcefire 3D Network Security
- Purpose-built Intrusion Prevention appliance from Nokia
- Hardened IPSO-LX Operating System
- Supports up to 2 Dual Fail-Open Network Interface Cards (copper or fiber)
- Two throughput versions - 250 Mbps or 400 Mbps
- Nokia First Call - Final Resolution Support for both hardware and software
- Fully Integrated advanced Intrusion Prevention technology

Nokia Security for Enterprise Networks

- Firewall/VPN, Integrated Security, IP VPN, SSL VPN, and Intrusion Prevention appliances
- Purpose built, hardened and secure
- Over 8 years of appliance and networking technology innovation
- Securing the worlds most demanding networks