Today’s enterprise endpoints face more sophisticated attacks than ever, especially when they are outside the corporate network and no longer protected by multiple layers of security. In addition, point of sales devices and networked devices with embedded operating systems are difficult to update and patch. To keep your business fully protected from breach or targeted attack, all types of endpoints require a blended approach to protection that secures data and applications from hacking attempts, web threats, and the increasing threat of vulnerabilities being exploited.

As a plug-in for OfficeScan, Intrusion Defense Firewall provides earlier, stronger endpoint protection by supplementing highly effective OfficeScan client-level security with pro-active virtual patching. A high-performance, deep-packet inspection engine monitors incoming and outgoing traffic for network protocol deviations, suspicious content that signals an attack, or security policy violations. Intrusion Defense Firewall shields vulnerabilities from being exploited with easy and fast to deploy filters, providing full protection before patches can be deployed. Together with Intrusion Defense Firewall, OfficeScan provides the industry’s most secure platforms for protecting endpoints, whether they are on the network, mobile, or remote.

**Key Features**

**Defends Against Advanced Threats**
- Blocks known and unknown vulnerability exploits before patches are deployed
- Automatically assesses and recommends required virtual patches
- Dynamically adjusts security configuration based on the location of an endpoint
- Protects endpoints with minimal impact on network throughput, performance, or user productivity
- Shields endpoints against unwanted network traffic with multiple protection layers
- Protects systems that hold sensitive data, critical to regulatory and corporate policy compliance

**Removes Bad Data from Business-Critical Traffic**
- Applies application control filters to alert/block specific traffic such as instant messaging and media streaming
- Ensures delivery of business-critical communications with low false positives
- Uses deep packet inspection to identify content that may harm the application layer
- Filters forbidden network traffic and ensures allowed traffic through stateful inspection

**Provides Earlier Protection**
- Provides protection before patches are deployed using attack blocking and vulnerability shielding
- Shields operating system and common applications from known and unknown attacks
- Detects malicious traffic that hides by using supported protocols over non-standard ports
- Blocks traffic likely to damage at-risk components using vulnerability-facing network inspection
- Prevents networking backdoors from penetrating into the corporate network
- Blocks all known exploits with attack-facing network inspection
- Defends custom and legacy applications using custom filters that block user-defined parameters

**Deploys and Manages within Existing Infrastructure**
- Leverages plug-in architecture for instant, live deployment to previously installed OfficeScan clients
- Easily deployed and managed from previously installed OfficeScan central management console
- Shortens the deployment cycle by eliminating the need to redeploy the entire solution

**Key Benefits**

- Eliminates risk exposure due to missing patches
- Reduces down-time for recovery with incremental protection against zero day attacks
- Allows patching on your own terms and timelines
- Lowers potential legal exposure by improving data security compliance
- Enhances firewall protection for remote and mobile enterprise endpoints
- Lowers management costs by using the common OfficeScan infrastructure
OfficeScan protects your physical and virtual desktops and laptops—on and off the network—with an innovative blend of world-class anti-malware and in-the-cloud protection from Trend Micro Smart Protection Network. File Reputation frees endpoint resources by moving pattern files into the cloud. And Web Reputation blocks access to malicious websites. A flexible plug-in architecture, Device Control, Behavior Monitoring, virtualization-awareness, and extended platform support all help lower management costs and increase flexibility.

Systems Requirements for Intrusion Defense Firewall

**Server Plug-in Requirement** - OfficeScan 10.0 & above
- Memory: 4GB recommended
- Disk Space: 4GB for install files, 4GB to 40GB for database
- Operating system: please refer to the deployment guide
- Browser support: Microsoft IE 7, IE 8 and IE 9. Note: IE 10 and IE 11 works best when used with IE compatibility view settings

**Client Plug-in Requirement** - OfficeScan 10.0 client & above
- Memory: 1GB recommended
- Disk Space: 200MB recommended