

Features Guide

Features Guide

Características

Funcionalidades

Versión

SYSTEM PROTECTION	DYNAMIC POLICY	DEVICE CONTROL	DATA ENCRYPTION	ENTERPRISE	PREMIUM
-------------------	----------------	----------------	-----------------	------------	---------

Sistema de Prevención de Intrusos (Host- Intrusion Prevention System)

- Protección del sistema de software dañino (gusanos, troyanos y virus).
- Defensa de programas espía (troyanos, spyware, keyloggers, rootkits).
- Protección a los medios críticos del sistema operativo de reinicios no solicitados por el usuario, uso excesivo de la CPU, archivos, carpetas y registros del sistema.
- Prevención de desbordamientos de memoria (memoria estática y memoria dinámica).P

✓				✓	✓
✓				✓	✓
✓				✓	✓
✓				✓	✓

Firewall Dinámico (Stateful Firewall)

- Posee un firewall de red basado en el kernel del sistema operativo.
- Filtro de tráfico entrante y saliente a nivel de host

✓				✓	✓
✓				✓	✓

Control de Aplicaciones (Application Control)

- Control de instalación y ejecución de aplicaciones.
- Implementación tanto de listas blancas como de listas negras de aplicaciones.
- Prevención de la detención de aplicaciones, por parte de un usuario no autorizado para ello.

✓				✓	✓
✓				✓	✓
✓				✓	✓

Características

Funcionalidades

Versión

		SYSTEM PROTECTION	DYNAMIC POLICY	DEVICE CONTROL	DATA ENCRYPTION	ENTERPRISE	PREMIUM
<p>Control de Aplicaciones (Application Control)</p> <ul style="list-style-type: none"> Control centralizado de archivos. Control sobre los procesos activos (procesos del sistema, antivirus, bases de datos, etc.) Análisis sobre las actualizaciones de firmas y parches. Control de acceso a la red. Posibilidad de ejecutar scripts para la solución de problemas. Desactivación remota y segura del agente. 		✓				✓	✓
<p>Protección de Red (Network Access Control)</p> <ul style="list-style-type: none"> Monitoreo de accesos no autorizados a una estación de trabajo o a una red mediante el IDS (Sistema de Detección de Intrusos). Filtro avanzado de tráfico (protocolos múltiples sobre IP, TCP/UDP/ICMP y Ethernet, y filtro de direcciones MAC/IP). Revisión de la integridad del protocolo, y protección de la red contra el escaneo de puertos. Verificación de procesos en ejecución, archivos de firmas y actualizaciones de software. Implementación de políticas de control de acceso a la red NAC (Network Access Control) basadas en los requerimientos del usuario final. Implementación de acciones encaminadas a garantizar la compatibilidad automática interoperativa con Juniper UAC, Microsoft NAP, Cisco, NAC y muchos otros desarrolladores de la VPN (Virtual Private Network). 		✓				✓	✓
<p>Aplicación Dinámica de las Políticas (Stateful Policies Enforcement)</p> <ul style="list-style-type: none"> Definición de políticas de seguridad de acuerdo con las necesidades de su organización (por tipo de conexión de red o por el ID del usuario o del sistema) Integración completa con las herramientas de dispositivos móviles (VPN, 3G). Control de acceso a la red. Análisis de los procesos activos (procesos de sistema, antivirus, etc.) Análisis de las actualizaciones de firmas y de software. 		✓				✓	✓

Características

Funcionalidades

Versión

SYSTEM PROTECTION	DYNAMIC POLICY	DEVICE CONTROL	DATA ENCRYPTION	ENTERPRISE	PREMIUM
-------------------	----------------	----------------	-----------------	------------	---------

Aplicación Dinámica de las Políticas (Stateful Policies Enforcement)

- Posibilidad de ejecutar scripts para la solución de problemas.
- Desactivación del agente de manera segura y remota.



Monitoreo de Puntos Finales (Endpoint Monitoring)

- Control de compatibilidad de las políticas con el punto final, dependiendo de los criterios específicos de cada organización.
- Implementación de acciones correctivas para puntos finales incompatibles, tales como la actualización de los programas de antivirus y de Windows.
- Implementación contextual de políticas, considerando los riesgos de seguridad de cada entorno organizacional.



Control de Dispositivos Móviles (Wireless Security)

- Permisos de acceso a dispositivos removibles de almacenamiento, considerando tipo, modelo, número y serial. Control de quemadores de CD/DVD.
- Control de permisos de lectura y escritura de acuerdo con el tipo de archivo.
- La implementación de la herramienta se realiza de manera automática y transparente para el usuario.
- Gestión y recuperación centralizada de llaves de encriptación de dispositivos.
- Los dispositivos de almacenamiento pueden ser restringidos, sin bloquear el funcionamiento del puerto USB/Firewire.
- Auditoría permanente de dispositivos conectados y desconectados.
- Monitoreo de operaciones en archivos, incluyendo el volumen de los datos copiados, así como todos los procesos llevados a cabo por la aplicación.
- Configuración de los niveles de autenticación.
- Control de la conectividad Wi-Fi, incluyendo sus modos de infraestructura y ad-hoc, así como la conectividad Bluetooth.



Características

Funcionalidades

Versión

SYSTEM PROTECTION	DYNAMIC POLICY	DEVICE CONTROL	DATA ENCRYPTION	ENTERPRISE	PREMIUM
-------------------	----------------	----------------	-----------------	------------	---------

Control de Dispositivos Móviles (Wireless Security)

- Control de la conectividad Wi-Fi, incluyendo sus modos de infraestructura y ad-hoc, así como la conectividad Bluetooth.
- Control de la conexión a redes de acceso inalámbrico de acuerdo al tipo de autenticación y encriptación WiFi (Abierta, WEP, WPA, WPA2)
- Administración de listas blancas y listas negras de puntos de acceso inalámbrico, de acuerdo con la dirección MAC o SSID.
- Aplicación de políticas dinámicas de acceso a dispositivos y comunicación móvil.

		✓		✓	✓
		✓		✓	✓
		✓		✓	✓
		✓		✓	✓

Encriptación de Archivos y Carpetas (File and Folder Encryption)

- Encriptación transparente para el usuario de forma inmediata.
- Encriptación /desencriptación de los archivos con acceso inmediato a ellos.
- Protección de datos en modo de hibernación.
- Eliminación y limpieza automática de archivos SWAP.
- Posibilidad de solicitar una contraseña de autenticación secundaria, con el fin de aumentar el nivel de seguridad de sus puntos finales.
- Definición de una contraseña para desencriptar información contenida en archivos auto-extraíbles.

			✓		✓
			✓		✓
			✓		✓
			✓		✓
			✓		✓
			✓		✓