



Proteja sua infra-estrutura informática das ameaças à rede, protegendo os dados, arquivos importantes e informação confidencial da sua organização.

Benefícios

- Disponibilidade 24x7 e integridade nas estações dos usuários.
- Implementação das novas aplicações e ferramentas de produtividade.
- Proteção dos ativos corporativos, dentro ou fora das instalações da companhia.
- Tranquilidade dos usuários de TI, quando os “patches” precisam ser instalados.
- Disponibilidade do ponto final as novas regras corporativas.

Características

- Proteção atualizada e permanente.
- Controle de acesso à rede.
- Controle de instalação e acesso a uso das aplicações.
- Controle de dispositivos removíveis de armazenamento.
- Controle de comunicações móveis.

Atualmente as redes de trabalho estão mais ou menos protegidas pelas tecnologias de segurança. Por isso os hackers informáticos trocam suas estratégias e agora os ataques são dirigidos aos pontos finais das empresas (servidores, estações de trabalho e notebooks). Os pontos finais são as fraquezas dos sistemas de segurança.

A forma mais comum para os ataques às redes é a Web, devido ao rápido e ilimitado acesso a Internet. Conseqüentemente o uso inapropriado, perigoso e improdutivo dos meios informáticos tem aumentado; por exemplo, com descargas multimídia, P2P, mensageria instantânea, spywares, etc.

Os sistemas de reconhecimento das assinaturas das ameaças informáticas (signature-based systems) são a primeira camada de proteção para os pontos finais nas organizações, mas sem dúvida não são suficientes para destruir as novas ameaças, porque os ataques são mais rápidos e diversos.

Enquanto isso, a organização é atacada por novos vírus, vermes informáticos (computer worms), troianos, transbordamentos de memória e intromissões na rede, já é muito tarde para que os sistemas baseados na detecção de assinaturas das ameaças informáticas atuem.

Por conseqüência, uma companhia deve ser capaz de garantir a produtividade de seus usuários e salvaguardar sua informação; agora a defesa dos pontos finais e a prioridade para a organização e nossa missão principal.

A única solução efetiva

Aranda 360 ENDPOINT SECURITY apresenta uma nova e radical solução para proteger as organizações dos ataques externos, e das falhas nas políticas corporativas de segurança, para o uso das estações de trabalho.

Este é o primeiro sistema de defesa que é pro - ativo, automático, e com muitas camadas em tempo real. **Aranda 360 ENDPOINT SECURITY** não precisa atualizações de assinaturas para proporcionar uma proteção completa e integrada das estações de trabalho.

Um agente é responsável de reforçar o perfil de cada política nas estações de trabalho, sem importar onde e quando são usadas (dentro ou fora das instalações da organização, on-line ou off-line). O agente desenvolve esta tarefa sem necessidade de interromper o trabalho de cada usuário.

Benefícios estratégicos para sua organização

- Aplicação das políticas de segurança informática para toda a organização.
- Baixo custo de propriedade (TCO), porque A360 utiliza um agente, uma console, e uma implementação para resolver muitas situações que possam afetar a segurança informática em sua empresa.
- Integração imediata com a infra-estrutura TI (aplicação, antivírus, e vigilância).



- Controle total da segurança em suas estações de trabalho.
- Sua organização terá um alto nível de segurança informática, gerando confiança no registro da informação.
- Informação crítica e/ou confidencial da companhia permanentemente segura e protegida.
- Aumento da produtividade, uma vez que os recursos encontram-se sempre disponíveis.

Funcionalidades

Proteção de Arquivos e Aplicações (Standard & Enterprise Edition) Files and Applications Protection

Controle as aplicações dos usuários mediante o acesso as listas de permissão ou bloqueio (whitelists and blacklists) e o acesso aos diferentes tipos de arquivos. Desta forma, A360 limita os processos de descarga e restringe arquivos multimídia.

Estabelece permissões de acesso detalhadas para cada aplicação, para os registros e os arquivos. Permite a configuração das permissões de acesso na rede. Além disso, controla a instalação das aplicações e evita a contaminação binária das aplicações existentes.

Suporte aos Dispositivos (Standard & Enterprise Edition) Multiple Devices Control

Permite o controle dos dispositivos de armazenamento removíveis, como por exemplo, USB, câmeras digitais, reprodutores MP3 ou discos rígidos externos, garantindo o controle sobre quem te acesso a que e sob que condições.

Além disso, A360 bloqueia os dispositivos de armazenamento sem travar as portas e controla o dispositivo conforme o distribuidor, o serial ou o modelo.

Sistema Controle de Dispositivos Móveis (Standard & Enterprise Edition) Wireless Security

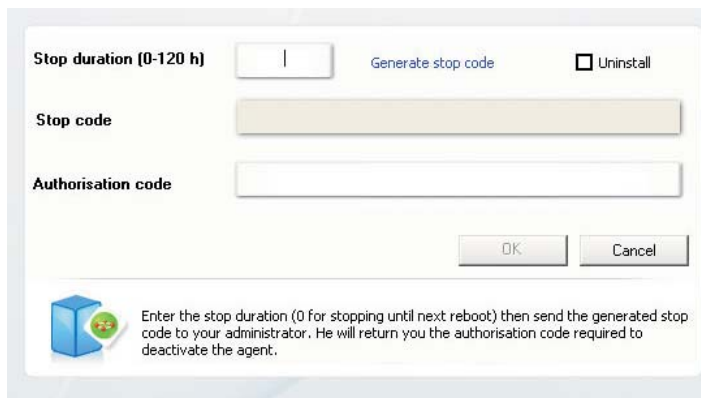
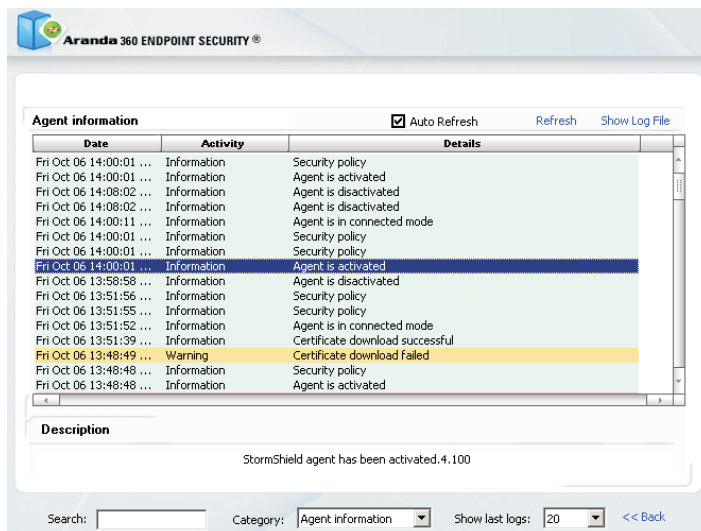
Protege o sistema ao criptografar a informação (data encryption) mediante diferentes métodos (WEP, WPA, WPA2) e definindo os pontos de acesso autorizados (SSID, MAC). E mediante técnicas de análise dos comportamentos são detectados intromissões ou bloqueios às solicitações de serviço.

Administra e controla os dispositivos moveis (wireless security). Por exemplo, desligar ou apagar as conexões WiFi e Bluetooth.

Control e centralizado (Standard & Enterprise Edition) Centralized Control

Permite estabelecer políticas particulares que uma organização precise, além de controlar e gerar relatórios permanentemente. **Aranda 360 ENDPOINT SECURITY** é uma solução gerenciada conforme o perfil designado do usuário e permite executar todas suas funções desde uma console de gerenciamento de maneira centralizada.

Adicionalmente, a solução identifica um ponto final com o diretório ativo, o endereço IP ou o nome do computador.





Proteção do Sistema (Enterprise Edition) System Protection

Proteção dos ataques que podem gerar um transbordamento de memória, que é a primeira etapa para entrar no sistema e instalar um troiano. Além disso, defende os meios críticos do sistema operacional, por exemplo, reinícios provocados por intrusos, uso excessivo da CPU, arquivos, pastas, e registros do sistema.

Também bloqueia automaticamente as tentativas de programas espíões para capturar a digitação do teclado (keylogger). Desta forma, A360 protege o sistema operacional de instalação dos rootkits que podem ter acesso aos documentos, arquivos, e pastas de uma estação de trabalho.

Proteção de Acesso à Rede (Enterprise Edition) Network Protection

A360 ativa um filtro no sistema operacional, quando o tráfego de informação entra no ponto final (múltiplos protocolos sobre IP, TCP/UDP/ICMP e Ethernet, e filtro de MAC/IP); adicionalmente, complementa o firewall da rede, criando regras de comunicação para esta em cada aplicação.

Detecta os acessos não autorizados no computador ou na rede, mediante o IDS (Sistema de Detecção de Intrusos), e protege a rede do escaneio(monitoração) das portas.

Aplicação Dinâmica das Políticas (Enterprise Edition) Stateful Policies Enforcement

A instalação de aplicações é controlada, para proteger o sistema da execução de software não autorizado, incluso para usuários com direitos administrativos, e não só isso se protege também as aplicações do uso inadequado, salvaguardando sua integridade.

Três mecanismos de proteção

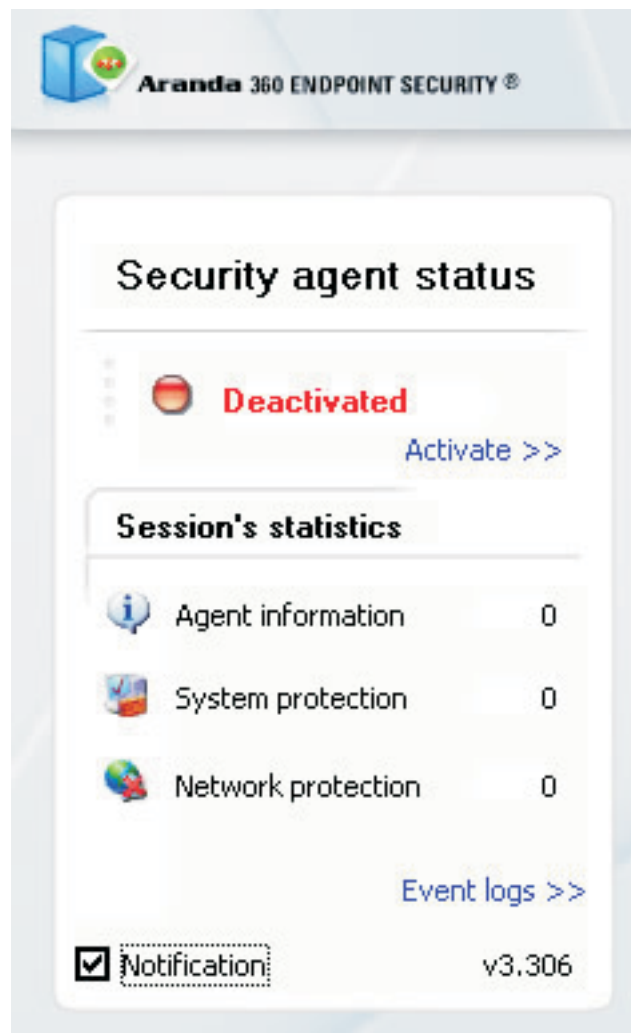
Aranda 360 ENDPOINT SECURITY incorpora três tipos de mecanismos de proteção que suportam o nível mais alto de segurança na estação de trabalho:

- Proteção baseada em regras.
- Proteção automática
- Proteção controlada baseada no perfil.

Proteção Baseada em Regras

Este mecanismo permite definir os privilégios ou permissões da proteção baseada em regras, assim como estabelecer privilégios associados com as aplicações das estações de trabalho, registros e a comunicação na rede.

Uma política de segurança explicita pode ser implementada por distintos grupos de estações de trabalho. Aranda 360 ENDPOINT SECURITY, tem regras predefinidas, e as políticas podem ser aplicadas imediatamente pelo administrador. Embora as regras de omissão possam ser modificadas em qualquer momento para ser adaptadas as políticas que uma organização particular precise.





Proteção Automática contra Qualquer Atividade Suspeita

A proteção automática cobre todos os mecanismos de **Aranda 360 ENDPOINT SECURITY**, detectando e bloqueando qualquer tipo de atividade suspeita. Este tipo de proteção não precisa de uma configuração por parte do administrador, mas pode definir o grau de desta.

O produto tem duas categorias de proteção automática. A primeira abrange as atividades do sistema e da aplicação; esta protege a estação de trabalho contra tentativas de corromper arquivos executáveis ou acesso a serviços do sistema, e dados específicos.

A segunda categoria é um sistema de proteção de Intromissões (Host Intrusion Protection System), e a estação de trabalho se pode proteger exatamente assim de ataques da rede. Os mecanismos implementados para detectar ataques do sistema ou da rede, por ser o sistema de proteção automática estão ativos permanentemente.

O tratamento que **Aranda 360 ENDPOINT SECURITY** tem diante os eventos pode ser controlado pelo administrador. Dependendo do tipo de evento, o sistema enviará um alarme ou implementará ações definidas automaticamente desde o principio do processo.

Proteção Baseada no Perfil

O último mecanismo de defesa é uma proteção automática baseada no perfil. Este depende da capacidade de controlar sistemas mediante ligações de cada aplicação. Durante a aprendizagem, estas ligações são memorizadas para criar um perfil padrão da aplicação. As ações desempenhadas por uma aplicação que esta rodando são comparadas com seu perfil para detectar qualquer possível discrepância que possa surgir.

A proteção baseada no perfil é a terceira linha de defesa que esta organizada para prevenir ataques e novos vermes informáticos (computer worms). Qualquer ataque baseado em aplicações ou serviços de sistema operacional corrompidos são totalmente bloqueados, sem importar se um mecanismo de detecção de assinaturas ou outro meio para defender o sistema de intromissões se encontra ou não disponível.

Requerimentos

No Cliente

Sistema Operacional	Windows 2000 SP4, XP
Processador	SP1/SP2, Pentium III 600 Mhz
Espaço Disponível no HD	20 MB

No Servidor

Sistema Operacional	Windows 2000, XP, 2003
Processador	Pentium III 850 Mhz
Espaço Disponível no HD	50 MB

Na Consola

Sistema Operacional	Windows 2000, XP SP1/SP2
Espaço Disponível no HD	15 MB

Solicite mais informações sobre este ou outros produtos da Aranda Software no e-mail infobrasil@arandasoft.com, consulte seu distribuidor autorizado ou visite o nosso site na internet www.arandasoft.com