

1. Pontos Gerais

Que tipo de ameaças põem em perigo a infra-estrutura de meu PC?
Como Aranda 360 protege a infra-estrutura da minha PC?
Posso usar Aranda 360 sem um antivírus?
Posso usar Aranda 360 sem um firewall pessoal?
Como obter mais informação acerca do Aranda 360? Como posso adquirir esta solução?

2. Segurança

Como Aranda 360 protege meu PC de vermes do computador?
Com quais mecanismos Aranda 360 protege de troianos e tentativas de ter controle da estação de trabalho?
Como Aranda 360 protege de tentativas de roubo de informação confidencial?
Como Aranda 360 protege a estação de trabalho de ataques à rede?
O usuário é notificado quando Aranda 360 bloqueia uma operação na estação de trabalho? A ferramenta consulta ao usuário para autorizar ou proibir ações suspeitas?
Quando Aranda 360 é usado, não se devem instalar "patches"?
Aranda 360 protege-se contra ataques?
O usuário pode desinstalar ou deter Aranda 360?

3. Políticas de Uso

Que é uma política de uso?
Pode-se proibir o uso de dispositivos de armazenamento removíveis?
É possível proibir o uso de arquivos específicos?
É possível proibir o uso de aplicações específicas?

4. Distribuição e Integração

Como se implementa Aranda 360?
De que forma pode ser implementada uma política de segurança com Aranda 360?
Aranda 360 é compatível com Windows XP SP2? Aranda 360 é compatível com o firewall SP2?
Com que antivírus foi testado o Aranda 360?

5. Configuração e Administração

Quanto tempo toma configurar Aranda 360?
Que conhecimentos são indispensáveis para utilizar o produto?
Existem alguns modelos de configuração disponíveis?
Por que alguns produtos não necessitam de configurações prévias para proteger Pcs?

6. Arquitetura

Quais são os pré-requisitos de Aranda 360?

Quais são os componentes da solução?

Qual é o tamanho do executável do agente?

É possível instalar o servidor num equipamento que é utilizada para outras tarefas, ou é necessário ter um servidor dedicado para esta aplicação?

É necessária uma base de dados? Pode ser usada uma base de dados já existente?

Que banda deveria ser destinada para a comunicação com os agentes de Aranda 360? É possível administrar e otimizar esta comunicação?

Como escala Aranda 360 ENDPOINT SECURITY? Quantas estações pode proteger?

7. Desempenho

Que impacto tem o Aranda 360 no desempenho da estação de trabalho?

Que banda deveria ser destinado para a comunicação com os agentes de Aranda 360? É possível administrar e otimizar esta comunicação?

Como escala Aranda 360? Quantas estações pode proteger?

8. Atualizações

Aranda 360 requer de assinaturas para funcionar?

Existe alguma maneira de verificar se um agente de A360 foi atualizado na estação de trabalho?

9. Verificação

Que informação específica é registrada na console?

A informação de segurança é enviada imediatamente para a console de administração?

Aranda 360 tem funções integradas para segurança e criação de relatórios?

É possível gerar alertas e ações nas consoles de verificação da rede?

Os dados de segurança podem-se utilizar com outras análises e ferramentas de relatórios, como por exemplo. Objetos de negócios ou Crystal Reports?

1. Pontos Gerais

Que tipo de ameaças possam em perigo a infra-estrutura de meu PC?

As estações de trabalho são os pontos mais inseguros dos sistemas de informação na rede. Sem dúvida alguma, essas estão expostas a qualquer tipo de ameaça e são cada vez mais vulneráveis, por situações como, por exemplo, a facilidade de mobilidade de Pcs, a conectividade móvel, e muitos elementos de comunicação.

Os novos ataques são atualmente muito mais agressivos difíceis de detectar, e mais rápidos que antes (de tal forma que os sistemas de reconhecimento de assinaturas de ameaças informáticas não têm tempo suficiente para reagir).

Os ataques não estragam somente a estação de trabalho, ou sua capacidade dentro da rede. Pelo contrario, tomam o controle do PC, para fazer espionagem industrial, transferência ilícita das contas bancárias, apresentação de Pop-Up de publicidade, etc.

Além disso, os usuários autorizados também facilitam a perpetuação destes ataques e de outros problemas legais quando usam suas estações de trabalho para ações como, por exemplo: carregar aplicações de conteúdo perigoso, aplicações vulneráveis, transferência de documentos de tipo legal, etc.

Como Aranda 360 protege a infra-estrutura da minha PC? de mi PC?

A360 protege de maneira pró-ativo e independente sua infra-estrutura informática contra ataques conhecidos ou desconhecidos. Pró-ativo, significa que a solução não depende de assinaturas, parâmetros ou outras atualizações para bloquear um novo ataque. Independentemente, esta ferramenta não necessita intervenção do usuário ou um administrador para bloquear atividades que são perigosas.

Por isso, esta é uma solução de defesa autônoma que em tempo real usa uma combinação de técnicas inovadoras para detectar e bloquear todas as ações que ameacem a integridade do sistema, as aplicações ou a comunicação numa estação de trabalho com seu ambiente. A360 é uma solução de tipo empresarial, porque a console de administração central pode definir e aplicar políticas, de uso e de segurança para grande número de Pcs.

Posso usar Aranda 360 sem um antivírus?

A360 pode proteger sua infra-estrutura informática de ataques ocasionados por vírus. Porém, esta solução é complementar ao sistema de detecção das assinaturas de ameaças informáticas. O antivírus elimina cada um dos sinais do ataque de vírus numa máquina que esteja infectada.

Na maioria dos casos, bloqueia um vírus conhecido antes que afete qualquer estação de trabalho. Apesar de que o A360 bloqueia muitos tipos de ataques, assim como operações perigosas que um antivírus não pode deter; dentro deles encontramos novos vírus que não tem assinaturas detectadas, ataques sigilosos, ataques à rede que usam vulnerabilidades de protocolos, operações de usuário proibidas por as políticas da companhia, etc.

Posso usar Aranda 360 sem um firewall pessoal?

Aranda 360 têm um firewall pessoal que controla a comunicação na estação de trabalho; o uso do firewall adicional é por este motivo é desnecessária. Esta ferramenta oferece uma solução completa e eficiente, mediante uma proteção mais sólida que a proteção oferecida por um firewall pessoal.

Primeiramente, um firewall pessoal se pode desinstalar, durante um ataque. Adicionalmente, se pode desconfigurar por aplicações que estabelecem comunicação com a rede de trabalho. Finalmente, um firewall é estático, e por esta razão sua eficiência depende das configurações pré-estabelecidas por o administrador.

A360 é protegido de qualquer possível tentativa para deter-lo ou desinstalar-lo. A solução preserva a integridade dos executáveis, evita a criação de portas de entrada encobertas estabelecidas normalmente em programas que estão autorizados para ter comunicação com a rede.

Além disso, o firewall do A360 está interconectado com vários mecanismos de detecção de intrusos e anomalias, que bloqueiam qualquer comunicação perigosa.

Como obter mais informação acerca de Aranda 360? Como posso adquirir esta solução?

Contate nosso equipo de vendas, enviando um e-mail para: infobrasil@arandasoft.com.

2. Segurança

Como Aranda 360 protege meu PC de vermes do computador?

Um verme informático é um tipo de vírus que pode ser espalhado automaticamente através da rede, sem precisar uma ação dos usuários. Os vermes do computador exploram as debilidades dentro do software da rede, como por exemplo, as fraquezas que existem na recepção de e-mails, nas bases de dados, e no sistema operacional.

A360 bloqueia que vermes informáticos se espalhem mediante os seguintes mecanismos: proteção da integridade do software em cada estação de trabalho, prevenção de códigos mal intencionados, assim como o bloqueio das ações destes vermes, antes que se espalhem dentro da rede.

Adicionalmente o A360 monitora o tráfego da rede para cada aplicação da estação e detecta automaticamente qualquer atividade suspeita. O firewall integrado desta ferramenta pode ser ativado para bloquear o tráfego ilícito, mediante a prevenção tanto para a corrupção dos executáveis, quanto para a comunicação da rede. Sem duvida, o Aranda 360 oferece uma ótima proteção contra vermes informáticos.

Com quais mecanismos Aranda 360 protege de troianos e tentativas de ter controle da estação de trabalho?

Um Troiano é um software que oculta operações maliciosas, baixo a aparência de uma aplicação de usuário comum ou de entretenimento. Os troianos permitem que um intruso tenha o controle remoto da estação de trabalho. Para receber ordens do atacante. O troiano instala-se de maneira permanente na estação e posteriormente comunica-se como um servidor da rede. A360 oferece três níveis de proteção contra os troianos: proteção das chaves de registro que iniciam automaticamente as aplicações; prevenção contra qualquer uso ilícito dos serviços do sistema operacional; finalmente, bloqueio de qualquer comunicação de rede que não esteja autorizada.

Como Aranda 360 protege de tentativas de roubo de informação confidencial?

A estação de trabalho é o objetivo de um número cada vez maior de ataques, desenvolvidos para obter e roubar informação confidencial: senhas de entrada, segredos industriais, sobre atividades bancárias, entre outros. Quando você enfrenta este risco o filtro de tráfego de rede é útil, mas nem sempre suficiente, inclusive se um firewall pessoal estivesse instalado na estação de trabalho.

Para garantir uma proteção absoluta, esta aplicação tem mecanismos de proteção específicos contra espionagem e captura de informação armazenada o computador: neutralização de captura da atividade do teclado, proteção de zonas do sistema onde as senhas são salvas regras de uso de dispositivos de armazenamento removíveis, limitação de acesso aos arquivos que são críticos, etc.

Como Aranda 360 protege a estação de trabalho de ataques à rede?

O A360 tem um Sistema de Detecção de Intrusos (SDI) que bloqueia todos os ataques quando estes intentam afetar a estação. Quando um ataque é dirigido para uma vulnerabilidade desconhecida, o sistema de proteção da ferramenta toma o controle e evita a execução de qualquer código malicioso.

O usuário é notificado quando Aranda 360 bloqueia uma operação na estação de trabalho? A ferramenta consulta ao usuário para autorizar ou proibir ações suspeitas?

O A360 é uma solução de proteção autônoma e independente. Esta ferramenta não atrapalha a atividade normal do usuário. Embora esta ferramenta advirta ao usuário quando um comportamento perigoso ou uma ação não autorizada são bloqueados. Esta notificação é apresentada temporariamente numa janela na tela. O sistema de notificação pode ser desativado se o usuário assim o desejar.

Quando o Aranda 360 é usado, não se devem instalar “patches”?

Um “patch” é uma atualização do software que repara um erro do programa; os patches de segurança bloqueiam fraquezas identificadas que podem ser aproveitadas durante um ataque. O A360 protege os sistemas sem patches de ataques que podem usar essas vulnerabilidades.

Quando as vulnerabilidades são identificadas, um ataque pode-se apresentar enquanto o patch ainda não está disponível. Incluso, quando o patch está disponível, instalá-lo em muitas estações de trabalho é muito complicado. Por isso, uma defesa pró-ativa é necessária.

Os patches de segurança são de muito benefício e o A360 não exclui a importância de sua implementação. Porém, esta aplicação é complementar aos patches, porque protege o sistema durante períodos de vulnerabilidade, permitindo ao usuário usar-los de forma controlada.

Aranda 360 protege-se contra ataques?

A360 protege-se contra ataques criados para deter, desativar ou desinstalar o produto. Esta ferramenta sempre continuará operando, já que seus mecanismos principais estão localizados ao interior do núcleo do sistema operacional, fazendo-os inacessíveis a qualquer tipo de ataque.

Esta proteção também aplica configurações instaladas na estação de trabalho, para manter as políticas de segurança sob o controle do administrador.

O usuário pode desinstalar ou deter Aranda 360?

O administrador do A360 pode autorizar ou proibir a desinstalação ou desativação desta solução. Esta regra funciona também quando o usuário é o administrador da estação de trabalho.

3. Políticas de Uso

Que é uma política de uso?

Uma política de uso é um parâmetro que regula a forma de uso das estações de trabalho. Desta forma, se reforçam as políticas de segurança da organização, proibindo comportamentos perigosos como, por exemplo, o uso de aplicações que são particularmente vulneráveis a ataques.

Uma política por se próprio pode proibir qualquer comportamento incompatível com um ambiente profissional em particular, como a descarrega de conteúdos multimídia.

Pode-se proibir o uso de dispositivos de armazenamento removíveis?

Simplicidade, cautela e uma grande capacidade, são as características que fazem que um dispositivo de armazenamento removível (USB, Ipods, etc.), sejam o meio perfeito para roubar informação. Estes meios podem também ser usados para introduzir programas perigosos, assim como informação proibida na rede de trabalho, sem que sejam detectados pelas defesas de segurança da estação. O A360 pode ser usado para bloquear o uso de USBs removíveis, sem necessidade de bloquear o acesso de outros periféricos que usam este tipo de conexão, como o Mouse, a impressora, etc.

E possível proibir o uso de arquivos específicos?

O acesso a Internet, assim como o uso de computadores portáteis, facilita a proliferação de comportamentos que são prejudiciais para a companhia; dentro deles estão a descarrega, armazenamento e uso de arquivos com propósitos não profissionais na estação de trabalho.

O A360 pode prevenir esses comportamentos, proibindo o acesso a arquivos que não estejam autorizados nas estações dos usuários.

E possível proibir o uso de aplicações específicas?

Redes locais de alta velocidade, assim como o acesso a Internet, motivam a instalação aleatória de aplicações piratas e não profissionais. O controle das aplicações instaladas nas estações de trabalho protege a companhia de todos os possíveis riscos.

O A360 permite restringir ao usuário de instalar aplicações específicas, incluso se o usuário é o administrador da estação de trabalho. Esta ferramenta também permite definir grupos de aplicações que devem ser eliminadas das estações de trabalho da companhia, tais como ferramentas P2P, e de Chat (MSN, ICQ, etc.).

4. Distribuição e Integração

Como se implementa Aranda 360?

A distribuição dos agentes do A360 é um processo simples. Os agentes podem ser distribuídos remotamente e instalados sem a intervenção do usuário, promovendo a gestão de software do A360. Cada agente pode ser carregado diretamente desde um servidor Web integrado na solução. O servidor e a console de administração têm seus próprios assistentes de instalação, cujo processo demora somente poucos minutos.

De que forma pode ser implementada uma política de segurança com Aranda 360?

Aranda 360 ENDPOINT SECURITY permite ao administrador definir várias políticas de segurança, de acordo com as necessidades dos diferentes grupos de usuários, assim como com o tipo de riscos que os usuários podem ter.

Uma política de segurança é um conjunto de regras que afetam o comportamento do sistema, as aplicações e a rede. Esta ferramenta permite anexar políticas a grupos de estações de trabalho, utilizando para isso, endereços IP ou objetos padrão do Diretório Ativo. A distribuição de políticas se faz com um simples clique na console de administração.

Aranda 360 é compatível com Windows XP SP2? Aranda 360 é compatível com o firewall Sp2?

O A360 é compatível com Windows XP SP2. Se você instala esta solução em Windows SP1 e quer atualizar-lo a SP2, não necessitará nenhuma modificação do agente. O A360 é tecnicamente compatível com o firewall de Windows XP Sp2.

Cabe salientar que a ferramenta tem seu próprio firewall, que oferece várias funções que não estão disponíveis nos firewalls de Windows, como por exemplo, a integração do (SDI), ou o filtro de conexões externas. Na realidade você pode desativar o firewall de Windows quando esta aplicação for utilizada.

Com que antivírus foi testado o Aranda 360?

Aranda 360 ENDPOINT SECURITY ha sido probado y certificado con la mayoría de software de antivirus existentes en el mercado. Por ejemplo, Norton Antivirus 2005, McAfee Virus Scan, Trend Micro Office Scan, Kaspersky Anti-Virus, and Sophos Anti-Virus. Si su antivirus no aparece en esta lista, por favor no dude en enviar un mail a info@arandasoft.com, para confirmar si su compatibilidad con A360 ya ha sido probada.

5. Configuração e Administração

Quanto tempo toma configurar o Aranda 360?

O A360 pode ser implementado quando for instalado na estação de trabalho, considerando regras de segurança que são predefinidas e incluídas no produto. Configurar esta aplicação permite aumentar o nível de segurança com um controle extra. Estes parâmetros refletiram suas políticas de segurança.

Normalmente, definir um conjunto inicial de políticas, assim como configurar parâmetros apropriados para a ferramenta, é um processo de poucos dias.

Que conhecimentos são indispensáveis para utilizar o produto?

O gerenciamento do A360 é de responsabilidade da rede da companhia, do sistema ou do administrador de segurança. Para atingir este objetivo não é necessário ter competências específicas; com a ajuda dos manuais de usuário, será possível administrar esta solução em poucos minutos.

Existem alguns modelos de configuração disponíveis?

O Aranda 360 ENDPOINT SECURITY tem vários modelos de configuração, com diferentes grupos de regras. Para cada política, você pode escolher se incluir ou não esses parâmetros.

Algumas destas políticas de usuário têm regras que impedem entre outros, a execução de aplicações proibidas, como o MSN ou o P2P.

Outras regras podem reforçar a segurança das estações de trabalho, restringindo determinadas ações de aplicações ou serviços críticos de Windows, como o explorador ou o e-mail.

Por que alguns produtos não necessitam de configurações prévias para proteger Pcs?

A diferença do Aranda 360 ENDPOINT SECURITY com alguns produtos de segurança para pontos finais que não requerem de configuração.

Isto sucede porque aqueles produtos consideram aspetos de segurança muito limitados, por exemplo, ataques referidos a transbordamentos de memória. Este tipo de ferramenta não necessita nenhum tipo de parâmetro, mas a proteção oferecida nestes casos, também é muito limitada.

6. Arquitetura

Quais são os pré-requisitos do Aranda 360?

O agente do A360 protege Pcs equipados com Windows 2000 SP4 ou Windows XP Sp1 ou Sp2. Não existe um requerimento específico de memória de seu CPU.

Quais são os componentes da solução?

O A360 tem vários componentes de software: agentes, servidores, base de dados, e console de administração. A proteção de cada estação de trabalho é desenvolvida por o agente da ferramenta.

Este agente se comunica com o servidor de instalação, que se encarrega da distribuição das políticas de segurança para cada agente, assim como de coletar toda a informação relacionada com a segurança da estação de trabalho. Esta informação é armazenada numa base de dados no servidor de instalação, que pode ser encontrada por meio da console. A base de dados ativa a console do A360, define e distribui as políticas de segurança, e apresenta a informação coletada pelos agentes.

Como se comunicam entre eles os componentes da solução?

A comunicação entre os componentes do A360 é autenticada e criptografada, usando os certificados SSL v3 y X509 v3. A autenticação é mútua entre todos os componentes, para reforçar o nível de segurança das soluções. A frequência da comunicação e o volume de dados transferidos, são controlados pelo administrador.

Qual é o tamanho do executável do agente?

Aproximadamente 7 MB de espaço no disco são requeridos para instalar o agente do A360.

E possível instalar o servidor num equipamento que é utilizado para outras tarefas, ou é necessário ter um servidor dedicado para esta aplicação?

O A360 não necessita de servidor dedicado. O requerimento de recursos depende do número de agentes que estão associados com este servidor, o tamanho das configurações, o volume dos registros coletados desde as estações de trabalho, e a frequência de comunicação entre os agentes e o servidor. Todos estes elementos podem-se controlar na console de administração.

E necessária uma base de dados? Pode ser usada uma base de dados já existente?

O Aranda 360 ENDPOINT SECURITY armazena a informação coletada desde as estações de trabalho numa base de dados relacional. Uma base de dados (motor de base de dados do Servidor SQL de Microsoft) se inclui com A360. Si você tem implementada uma base de dados 2000 do servidor SQL e deseja atualizar-la para armazenar os dados de A360, especifique-lo durante a instalação do produto, ou registre a base de dados na console de administração.

A instalação dos componentes de Aranda 360 pode ser organizada de acordo com as necessidades do administrador em um ou mais equipamentos?

Os componentes do A360 são módulos de software independentes, que podem ser instalados de acordo com sua preferência. Por exemplo, cada servidor, console e base de dados se podem instalar em máquinas diferentes, ou em um único computador definido com antecedência.

7. Desempenho

Que impacto tem o Aranda 360 no desempenho da estação de trabalho?

O A360 tem um consumo de recursos da estação de trabalho, incluso sob condições críticas como, por exemplo, quando existem muitas ameaças ao sistema ao mesmo tempo, esta solução utiliza somente de 2% a 3% da capacidade da CPU.

Que banda deveria ser destinado para a comunicação com os agentes de Aranda 360? E possível administrar e otimizar esta comunicação?

A comunicação entre os agentes do A360 e o servidor, permite a aplicação de políticas de segurança para os agentes, e a coleta e consolidação dos registros da estação. A diferença dos sistemas que estão baseados na atualização de assinaturas, a implementação das políticas de segurança para este caso, não é uma atividade obrigatória, porque esta ferramenta não necessita de atualizações quando uma nova ameaça aparece.

O tamanho em média de uma política de segurança é menos de 50 KB. A transmissão deste limitado volume de dados não é um problema, incluso nas redes limitadas. O tipo e quantidade de informação que é subida no servidor são determinados pelo administrador, quem deve ter em conta a capacidade específica da rede.

Finalmente, o administrador tem a possibilidade de otimizar a comunicação entre os componentes do A360, distribuindo-os sobre vários servidores, ou configurando a frequência de conexão entre eles.

Como escala Aranda 360? Quantas estações pode proteger?

Aranda 360 ENDPOINT SECURITY foi desenhado para proteger um número ilimitado de estações de trabalho virtualmente. Sua capacidade para escalar resultados é garantida por três aspectos: componentes de software especializados, uma arquitetura de alta disponibilidade, e a capacidade para otimizar a banda disponível.

Esta solução tem componentes modulares especializados, que podem ser executados nos diferentes computadores, permitindo uma maior distribuição da carga gerada pelas políticas de configuração, e os dados de verificação (console), protegendo as estações de trabalho (servidores) e finalmente, armazenando estes eventos (base de dados).

Um alto nível de disponibilidade é oferecido através da arquitetura de tipo multi-servidor com um balanceamento de carga e mecanismos de tolerância à falhas. Além de novos servidores que podem ser adicionados a qualquer momento para implementar o escalamento no sistema.

O escalamento também depende dos requerimentos de banda da rede, contrario aos produtos baseados na detecção de assinaturas de ameaças informáticas (que necessitam de cargas freqüentes de arquivos de assinaturas em cada estação de trabalho), o agente do A360 necessita ser atualizado somente quando o administrador deseja aplicar novas políticas.

Adicionalmente, com a console de administração o administrador pode definir claramente o volume de dados que deve ser coletado pelas estações de trabalho.

8. Atualizações

Aranda 360 requer de assinaturas para funcionar?

O A360 está baseado numa tecnologia de comportamento patenteada. Uma das vantagens mais importantes desta tecnologia é que não necessita de assinaturas para bloquear ataques conhecidos ou desconhecidos na estação de trabalho.

Para reforçar as capacidades de proteção do A360, o produto também tem um modulo de SDI (Sistema de Detecção de Intrusos), que é usado para analisar o tráfego entrante na rede. O SDI da aplicação é acoplado com um firewall baseado no kernel, que oferece uma capacidade de filtro instantânea onde exista um tráfego suspeito.

O (SDI) do Aranda 360 ENDPOINT SECURITY é a única parte do produto que usa assinaturas informáticas.

Existe alguma forma de verificar se o agente do A360 foi atualizado na estação de trabalho?

Qualquer processo de atualização é armazenado no registro da estação de trabalho. De igual maneira, se uma notificação de usuário é ativada, uma mensagem pop-up mostrará que uma nova versão é instalada.

9. Verificação

Que informação específica é registrada na console?

A informação referente à segurança da estação de trabalho é armazenada num arquivo de registro: atividade do sistema, comportamento das aplicações, e comunicações da rede. Todos os eventos relevantes são armazenados neste cadastro, incluso se não se implementou uma ação de bloqueio. O tipo e o formato da informação que é carregada na console, pode ser consultada na documentação técnica do produto.

A informação de segurança é enviada imediatamente á console de administração?

Os alertas são enviados na consola com uma freqüência configurada pelo administrador.

Aranda 360 ENDPOINT SECURITY tem funções integradas para segurança e criação de relatórios?

O Aranda 360 ENDPOINT SECURITY oferece uma completa verificação integrada e um módulo de relatórios.

A verificação permite uma análise detalhada dos dados de segurança provenientes das estações de trabalho.

Estas funções, além da seleção de muitos critérios, facilitam a rápida administração e o acesso à informação requerida. As ferramentas de análise integradas à solução e um gerador de relatórios gráficos oferecem ao administrador um completo panorama da segurança real das estações de trabalho.

E possível gerar alertas e ações nas consoles de verificação da rede?

O A360 comunica-se com os sistemas de verificação da rede mediante interfaces, utilizando um formato SMTP ou um syslog. O administrador pode ativar estas funções desde a console de administração.

Os dados de segurança podem ser utilizados por outras ferramentas de análises e relatórios, como por exemplo. Objetos de negócios ou Crystal Reports?

A informação que é carregada desde as estações de trabalho, é armazenada na base de dados. Você pode usar suas próprias ferramentas de análise e relatórios para consultar a base de dados do A360. Porém a console de administração da solução oferece sua própria análise e a capacidade de apresentar relatórios de forma gráfica e detalhada aos usuários.