



Boas Práticas

MAV (Antivírus Gerenciado)

N-able N-sight RMM

Aviso legal

As informações e o conteúdo deste documento são fornecidos apenas para fins informativos e são fornecidos "no estado em que se encontram", sem garantia de qualquer tipo, expressa ou implícita, incluindo, mas não se limitando às garantias implícitas de comercialização, adequação a um fim específico, e não violação. A ADDEE não se responsabiliza por quaisquer danos, incluindo danos consequentes, de qualquer tipo que possam resultar do uso deste documento e das ferramentas nele citadas. As informações do presente documento são obtidas de fontes publicamente disponíveis.

Sumário

Introdução	3
1. Pré-Requisitos	4
+ URLs de Comunicação	4
+ Sistemas Operacionais	4
+ Permissões do Usuário no N-sight RMM	4
+ Soluções Concorrentes	5
2. Política de Proteção	6
+ Aba VERIFICANDO – Verificando e Config. de Detecção	6
+ Abas VERIFICAÇÃO RÁPIDA e VERIFICAÇÃO PROFUNDA	8
+ Aba CORREÇÃO	8
+ Aba VERIFICAÇÃO COMPORTAMENTAL	9
+ Aba CRIPTOGRAFIA DE DISCO	10
3. Segurança da Comunicação	11
+ Instalação Sempre Pendente	11
+ Não Compatível – Falha na Instalação	14
+ Status DETECTADO	14
+ Tratando Falsos Positivos	15
+ Tratando Arquivos do Tipo PUA	15
4. Manutenção	16
5. Relatórios	17
6. Obrigado!	18

Introdução

Este documento tem como objetivo abordar a implementação do **MAV (Managed Antivírus, ou Antivírus Gerenciado)** de forma segura e evitando erros, bem como fornecer familiaridade com a ferramenta e os conceitos envolvidos.

Como qualquer outra solução, a implementação do **MAV** exige planejamento e compreensão do ambiente e da solução.

É necessário que você, enquanto prestador de serviço, entenda que está oferecendo um serviço de antivírus e não apenas uma licença do mesmo. O serviço envolve uma série de responsabilidades como acompanhamento e gestão das atualizações e verificações, manutenção das ameaças e quarentena, etc.

Vale ressaltar também a importância dos relatórios do **MAV** para a gestão e o acompanhamento diário.

Queremos sua opinião! Ajude-nos a aprimorar este documento. Qualquer dúvida, crítica ou sugestão, por favor, encaminhe um e-mail para boaspraticas@addee.com.br.

1. Pré-Requisitos

+ URLs de Comunicação

Além das URLs do N-able N-sight RMM e das URLs e Portas do Agente de Monitoramento, é necessário incluir essas URLs abaixo na lista de permissões do seu software de Firewall:

us-west-2.breckenridge.remote.management
breck-us-west-2-svc.logicnow.us
cannonball-us-west-2-push.logicnow.us
breck-update.logicnow.us
breck-files.logicnow.us
data.cdn-sw.net

Para simplificar a configuração do Firewall e minimizar o impacto de futuras alterações de URL, sugerimos também incluir na lista de permissões os seguintes domínios:

*.remote.management
*.logicnow.us
*.cdn-sw.net
*.bitdefender.net
*.bitdefender.com
*.v1.bdnsrt.org

+ Sistemas Operacionais

O MAV é compatível apenas com Sistemas Operacionais **Windows e MacOS**. Através **deste link** é possível identificar quais versões destes dois Sistemas Operacionais acima são compatíveis com a solução.

+ Permissões do Usuário no N-sight RMM

A instalação e configuração do **MAV** dependem dos privilégios do usuário e de sua função de conta no **N-sight RMM**. Para ter acesso as configurações o usuário precisa ser pelo menos do nível **superusuário** ou **administrador (não clássico)**.

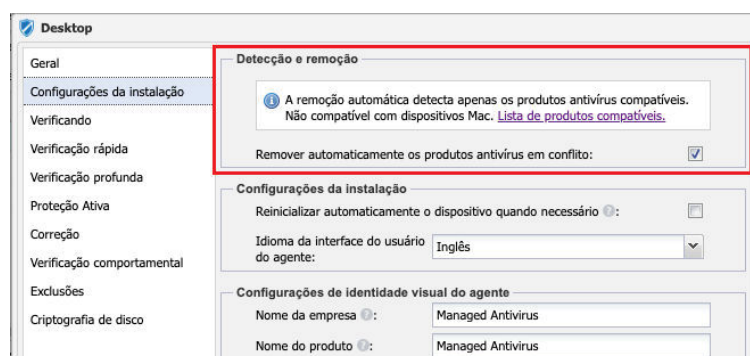
+ Soluções Concorrentes

Antes de instalar o **MAV** no dispositivo verifique se não há nenhuma outra solução de antivírus ativa no mesmo pois, se durante a instalação for detectado outro antivírus, o **MAV** não será instalado. **Isto também inclui instalações autônomas do Bitdefender.**

Portanto, caso haja algum outro antivírus instalado, desinstale-o antes de iniciar a ativação do **MAV**.

Para situações onde não seja possível fazer a desinstalação manual do antivírus no dispositivo, ou não tenha ciência de que há outra solução instalada, o **N-sight RMM** conta com uma opção de detecção de soluções concorrentes, onde o próprio agente se encarrega de fazer a desinstalação antes de prosseguir com a ativação do **MAV**.

Este recurso é o **CART (Competitor Antivirus Removal Tool, ou Ferramenta de Remoção de Antivírus do Concorrente)**, e ele fica localizado dentro da política de proteção do MAV, conforme demonstra a imagem abaixo:



Veja que a remoção automática, através do **CART**, detecta apenas as soluções de antivírus compatíveis com o **N-sight RMM** (mais informações sobre o recurso, incluindo a lista completa dos softwares compatíveis, você pode encontrar **neste link**).

2. Política de Proteção

Antes da ativação do recurso é preciso configurar uma política de proteção. Ela define, em vários aspectos, o comportamento que será adotado pelo **MAV**. Para acessar a política de proteção do MAV vá em: **Configurações / Antivírus Gerenciado / Política de Proteção**.

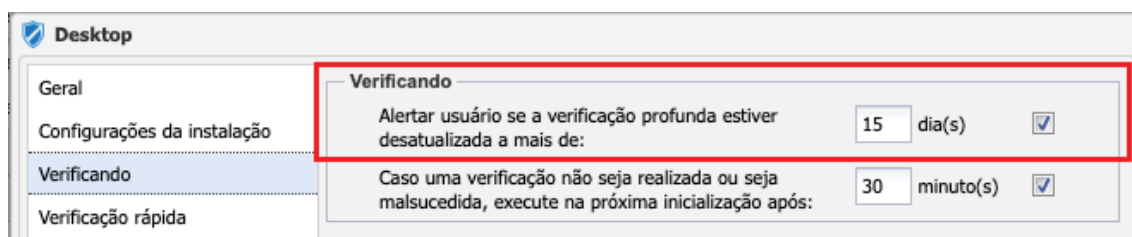
O **N-sight RMM** possui 3 políticas padrões (Server, Desktop e Laptop) préconfiguradas para o **MAV**, nas quais você pode se basear para configurar as suas próprias políticas.

A nossa recomendação é **não utilizar as políticas padrões nos ambientes em produção**. Ao invés disto, crie suas próprias políticas com base nas informações levantadas para cada cliente/site/dispositivo.

A política de proteção consiste em algumas configurações básicas e autoexplicativas, porém reforçaremos alguns pontos que precisam de uma atenção maior durante a configuração:

+ Aba VERIFICANDO – Verificando e Config. De Detecção

Nesta aba temos a configuração “Alertar usuário se a verificação profunda estiver desatualizada a mais de X dias”.



Muitas vezes a verificação profunda é interrompida durante seu processo, seja por falta de processamento ou memória disponível no dispositivo naquele momento, ou porque simplesmente o dispositivo foi desligado, causando assim uma falha.

Caso a política de proteção esteja configurada para realizar a verificação profunda apenas uma vez por semana uma nova tentativa será realizada somente 7 dias após esta falha.

Se o número de dias informado nesta configuração for menor do que o período de tempo entre uma verificação ou outra (exemplo: abaixo de 7 dias), uma verificação com falha será mostrada no **N-sight RMM** para este dispositivo.

Mesmo inserindo 15 dias (valor padrão), se a verificação profunda falhar duas vezes (deduzindo que a mesma está configurada para ser executada uma vez por semana) a falha também irá ocorrer.

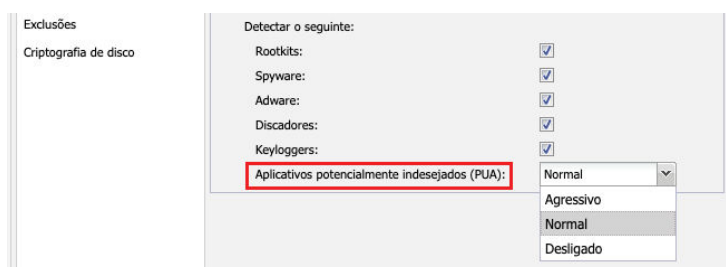
Portanto sempre monitore o status das verificações rápidas e profundas nos dispositivos dos seus clientes, para que estes alertas não sejam apresentados com frequência em seu painel. De preferência, combine um horário com o teu cliente (ou trace um plano de ação com o teu cliente) em que esta verificação possa ser executada sem problemas ou interrupções nos dispositivos.


Observação: O tempo de realização de uma verificação profunda pode variar, pois depende do número de processos e recursos ativos naquele momento, e também da quantidade de arquivos a serem analisados. Sendo assim, **recomendamos executar esta verificação quando o computador não estiver em uso, para que não haja nenhum impacto nos processos, e a verificação não seja interrompida.** Se o dispositivo for antigo ou tiver um processamento mais lento, recomendamos a execução desta tarefa **fora do horário de expediente.**

Nesta aba também temos algumas configurações de detecção, dentre elas o **PUA (Potentially Unwanted Programs ou Aplicativos Potencialmente Indesejados).**

Esta é uma categoria ampla de software, cujo objetivo não é tão claramente nocivo quanto outros tipos de malware, como vírus ou cavalos de Troia. Porém eles podem instalar softwares indesejados de forma adicional, alterar o comportamento do dispositivo digital ou realizar atividades não aprovadas ou esperadas pelo usuário.

Nesta aba você pode definir qual será o comportamento do **MAV** com relação aos **PUAs**. Definindo o modo como **“Desligado”**, a detecção de **PUAs** não será realizada. No modo **“Normal”** a detecção é feita, registrada e analisada pela proteção ativa, mas não bloqueada (apenas se a análise resultar em uma possível ameaça). Já no modo **“Agressivo”** a detecção é imediatamente bloqueada.





Observação: Recomendamos optar pelos modos “Normal” ou “Agressivo”, uma vez que a opção “Desligada” ignora este tipo de ameaça.

+ Aba VERIFICAÇÃO RÁPIDA e VERIFICAÇÃO PROFUNDA

Nestas duas abas deverá ser configurado os locais que serão analisados, e também o agendamento da execução da verificação.

A checkbox “**Usar prioridade baixa**” faz com que as verificações sejam realizadas com o mínimo de processamento possível, não causando nenhum impacto nos processos ativos do dispositivo e tornando o recurso imperceptível. Entretanto o tempo de conclusão das análises pode demorar um pouco mais do que o habitual, devido ao mínimo de processamento utilizado.

Em “**Verificando**” você deve configurar quais recursos serão analisados. Para a verificação profunda opte por marcar todas ou quase todas as opções, enquanto para a verificação rápida marque apenas as essenciais (Executando processos, Registros e Setores de reinicialização, por exemplo).

Como o próprio nome diz, o intuito desta verificação é checar os principais focos de ameaça e garantir a integridade do dispositivo, tendo a verificação profunda como uma análise mais completa do dispositivo.

O mesmo equivale para a sessão “**Tipo**”. Para a verificação rápida opte por marcar somente as opções essenciais (Locais comuns de ameaça, por exemplo) e para a verificação profunda marque todas (ou quase todas) as opções para análise.

+ Aba CORREÇÃO

Aqui nesta sessão você deve configurar o comportamento do **MAV**, quando se deparar com alguma ameaça.

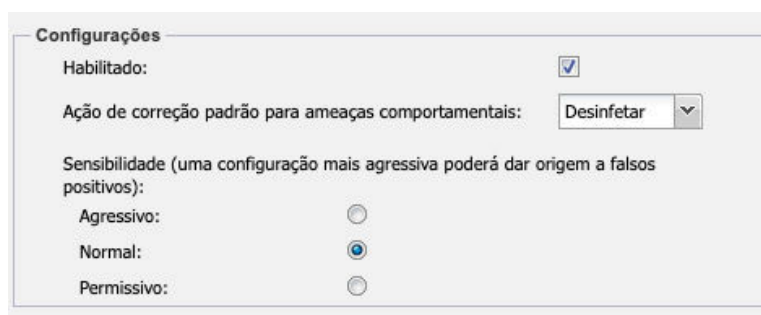
- “**Correção para arquivos infectados**” corresponde aos arquivos infectados relacionados a uma assinatura de malware no banco de dados da **Bitdefender**.
- “**Correção para arquivos suspeitos**” trata os arquivos suspeitos através da análise heurística.
- “**Correção para Rootkits**” trata os softwares utilizados por hackers para assumir o controle do dispositivo ou da rede.

Dentre as ações de tratamento disponíveis, encontramos as opções:

- **“Desinfetar”** (o **MAV** tentará remover o malware do arquivo e, em caso de falha, o arquivo será enviado para a quarentena). **Esta é a opção recomendada para primeiro uso**, e não é compatível com a opção **“Correção para arquivos suspeitos”**.
- **“Quarentena”** (Move os arquivos detectados do local para a quarentena, não permitindo os arquivos de serem executados ou abertos). Não é compatível com a opção **“Correção para Rootkits”**.
- **“Ignorar”** (Nenhuma ação é tomada na detecção, sendo apenas registrado nos logs da verificação). Opção menos recomendada, e aparece disponível somente na opção **“Correção para arquivos infectados”**.

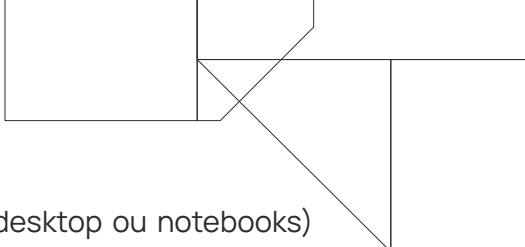
+ Aba VERIFICAÇÃO COMPORTAMENTAL

A **verificação comportamental** (disponível somente para **Windows**) é uma tecnologia de detecção proativa que usa métodos heurísticos para detectar potenciais novas ameaças em tempo real. As ações dos processos são observadas e pontuadas, onde se a pontuação geral de um processo atingir um determinado limite o processo é considerado prejudicial.



Se a ação de correção estiver definida para “Desinfetar”, o antivírus irá colocar em quarentena o aplicativo existente e também tentará repor quaisquer alterações feitas ao sistema. Se a ação de correção estiver definida para “Bloquear”, não será permitida a execução do aplicativo.

Esta verificação monitora em tempo real todas as mínimas ações realizadas no dispositivo e isto exige um constante e alto processamento. Portanto, recomendamos que o uso deste recurso seja direcionado para servidores, devido ao hardware mais robusto e também devido a criticidade de segurança.



É possível utilizá-lo em estações de trabalhos também (seja desktop ou notebooks) porém poderá apresentar lentidão no mesmo, devido ao consumo de processamento.

+ Aba CRIPTOGRAFIA DE DISCO

A **criptografia de disco**, no nível de volume, protege os dados de seus clientes contra roubo ou perda acidental, tornando as informações em discos rígidos ilegíveis para usuários não autorizados. Ou seja, basicamente, usando criptografia de disco, os dados não podem ser acessados por terceiros e as informações não podem ser roubadas.

As chaves de criptografia estão conectadas ao hardware em que o disco está instalado para garantir que a simples remoção de um disco não forneça acesso aos dados. Então, mesmo que a unidade de disco seja removida do computador, as informações permanecerão criptografadas e não poderão ser recuperadas sem as **chaves de recuperação**.

A nossa criptografia de disco usa o **Bitlocker do Windows** para proteger os dados dos dispositivos, renderizando as informações para que as mesmas não sejam lidas por usuários não autorizados.

Portanto para utilizar este recurso é necessário avaliar quais são os pré-requisitos, os passos de ativação e configuração descritos no manual do **N-sight RMM**, para que não haja nenhum problema durante o processo, e que os dados não sejam criptografados de forma indevida.

3. Problemas Comuns

As causas de falhas durante a instalação ou utilização do MAV podem variar e cada uma requer um procedimento específico para correção. Abaixo listaremos as mais comuns:

+ Instalação Sempre Pendente

Em alguns casos, após ativar o recurso, o mesmo pode permanecer com o status “**pendente**” por muito tempo.

Esta situação pode ocorrer quando há algum bloqueio na comunicação do agente com o painel, ou quando há resquícios de alguma instalação (ou tentativa) anterior no dispositivo, no caso de uma reinstalação.

Também pode acontecer quando não há um tempo hábil para concluir a instalação do recurso. Ou seja, o **MAV**, durante a instalação, efetua uma varredura completa no dispositivo antes de concluir a ativação, e esta varredura é realizada com o mínimo possível de recursos. Desta forma, esta ativação pode demorar até 1 hora ou mais, dependendo do processamento do dispositivo.

Observação: Conforme explicado acima, e diferente dos outros recursos que normalmente são ativados minutos depois da ativação, **é recomendado que seja aguardado até 1 hora após a ativação** para ter certeza de que há algum problema na instalação.

Uma vez que este tempo foi aguardado, faça as validações e procedimentos abaixo para reinstalar o **MAV** de forma limpa:

1. Se for a primeira vez que está ativando o **MAV** neste dispositivo verifique se as **URLs e portas** citadas no passo 1 deste manual estão liberadas nas suas soluções de filtro (**tanto da rede como do próprio dispositivo – Firewall do Windows, outro antivírus com solução de filtro de rede ativado, etc**).

Caso tenha realizado alguma alteração, desative o MAV no painel, aguarde alguns minutos até que o painel reconheça que o recurso foi desativado e ative-o novamente.

2. Verifique se o Sistema Operacional está com todas as atualizações de segurança em dia.

Se não estiver, instale todas as atualizações pendentes pelo **Windows Update** (caso utilize o nosso recurso **Gerenciamento de Patches**, faça a instalação de patches por ele), depois desative o **MAV** no painel, aguarde alguns minutos até que o painel reconheça que o recurso foi desativado e ative-o novamente.

3. Verifique se o dispositivo está com o .NET Framework instalado e atualizado. Você pode encontrar o download das últimas versões disponibilizadas **neste link**.
4. Agora, se for uma reinstalação, ou tiver certeza de que todas as URLs e portas do link acima estão liberadas, realize o procedimento abaixo para reinstalar o **MAV** de forma limpa. Isto corrigirá qualquer arquivo que foi corrompido durante a instalação anterior, seja por algum registro já existente ou não:

1. No Painel do N-sight RMM:

1. Clique com o botão direito sobre o dispositivo, escolha a opção Editar Servidor (ou Estação de Trabalho);
2. Em "Antivírus Gerenciado", mude a opção Configuração para "Desligado";
3. Clique em Ok para salvar as mudanças e aguarde o processo de desinstalação pelo painel;
4. Aguarde até que na aba Resumo deste device apareça "Antivírus Gerenciado - Não Instalado".

2. No computador local:

1. Acesse o dispositivo remotamente, após a desinstalação do Antivírus, e remova manualmente as pastas, arquivos e registros abaixo, caso ainda existam:
 - C:\Program Files (x86)\Advanced Monitoring Agent\BDInstall.log
 - C:\Program Files - Todas as entradas referentes a Managed Antivirus
 - C:\Program Files\Common Files - Todas as entradas referentes a Managed Antivirus

- C:\ProgramData - Todas as entradas referentes a ManagedAntivirus e Managed Antivirus (Atenção - Pasta Oculta)
- %TEMP% - Pasta BDInstall
- %WINDIR%\Temp - Pasta BDInstall
- Drive Local - Procure por "trufos.sys" (sem as aspas) e remova (se existir)

2. Acesse o arquivo **SETTINGS.INI**, localizado em: **C:\Program Files (x86)\Advanced Monitoring Agent** e apague as chaves **[MANAGEDAV]** e **[MANAGED_AV_BRECKENRIDGE]**, e todo o conteúdo dentro dela, semelhante a isto:

```

RUNTIME=1020432871
[MANAGEDAV]
LASTSCANRESULT=0
LASTSCAN=1626444183
CURRENTSTATE=0
[AUTOUPDATE]

VERSION=5
[MANAGED_AV_BRECKENRIDGE]
ACTIVATED=0
CURRENTSTATE=0
[ECHO]

```

3. No registro do Windows:

1. Abra o Registro do Windows (regedit.exe) e exporte um backup (**Arquivo/Exportar**) (**recomendado**).
2. Apague os registros abaixo, se eles ainda existirem:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EPProtectedService
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EPRedline
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ManagedAntivirus
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\atc
 - HKEY_LOCAL_MACHINE\SOFTWARE\Endpoint Security.remove
 - HKEY_LOCAL_MACHINE\SOFTWARE\{AAD1516D-28AB-4EB5-B7C8-DF54FE4442E9}.remove

4. Ferramenta de Remoção da Bitdefender:

1. Baixe e execute **esta ferramenta de remoção da Bitdefender**, com instalação silenciosa, e aguarde de 5 a 10 minutos para a conclusão.
2. Reinicie o dispositivo (se possível) para validar todas as alterações acima.

5. No Painel do N-sight RMM novamente:

1. Clique com o botão direito sobre o dispositivo, escolha a opção Editar Servidor (ou Estação de Trabalho);
2. Em "Antivírus Gerenciado", mude a opção Configuração para "Ligado";
3. Clique em **Ok** para salvar as mudanças e aguarde o processo de instalação pelo painel;
4. Aguarde até que na aba **Resumo** deste dispositivo apareça "Antivírus Gerenciado - Ativo".

+ Não Compatível – Falha na Instalação

Esta falha na instalação é consequência de um mecanismo de antivírus que está instalado, e o mesmo não possui compatibilidade com a desinstalação automática do MAV.

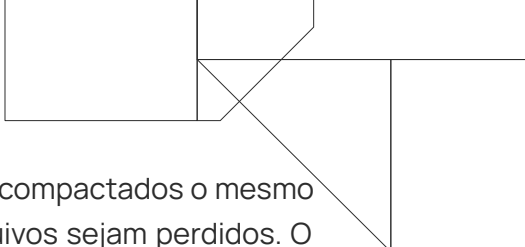
Para resolver isto, remova manualmente o antivírus do dispositivo no local. Depois abra o painel do **N-sight RMM**, vá na guia **Resumo** deste dispositivo e clique no link "**Forçar Instalação**" para que o MAV seja reinstalado.

+ Status DETECTADO

GenVariant.Zusy.365678	Vírus	30-Mar-2022 - 12:31	Detectado
JS:Trojan.Agent.EJDR	Vírus	30-Mar-2022 - 12:31	Detectado
JS:Trojan.Crylos.2282	Vírus	30-Mar-2022 - 12:31	Detectado
JS:Trojan.Crylos.6421	Vírus	30-Mar-2022 - 12:31	Detectado
Trojan.Agent.FOOL	Vírus	30-Mar-2022 - 12:31	Detectado
Trojan.GeneticFCA.Script.1620	Vírus	30-Mar-2022 - 12:31	Detectado
Trojan.GeneticID.30857477	Vírus	30-Mar-2022 - 12:31	Detectado
Trojan.GeneticID.38116674	Vírus	30-Mar-2022 - 12:31	Detectado
Trojan.GeneticID.39200933	Vírus	30-Mar-2022 - 12:31	Detectado
Trojan.GeneticID.39202528	Vírus	30-Mar-2022 - 12:31	Detectado
Threat:Phish.BAT3.Gen	Malware	30-Mar-2022 - 12:31	Detectado

O status "**Detectado**" ocorre quando o antivírus encontra uma possível ameaça dentro de algum arquivo ou conjunto de arquivos no qual ele não possa excluí-lo.

Por exemplo: Digamos que esta possível ameaça seja encontrada dentro de um **arquivo compactado (.zip, .rar)** ou encontrado no anexo de um e-mail (**.pst, .ost**).



Se o **MAV** excluir este arquivo infectado do pacote de arquivos compactados o mesmo poderá ser corrompido, fazendo com que todos os outros arquivos sejam perdidos. O mesmo acontece para o anexo de e-mail, que pode corromper todo o arquivo .pst de e-mail.

Portanto quando o **MAV** identifica este tipo de situação ele coloca o status como “**DETECTADO**” e te informa o caminho do local da ameaça.

O MSP pode simplesmente acessar o caminho e apagar o arquivo manualmente, ou retirá-lo deste caminho e colocar em outro lugar onde o **MAV** possa tratá-lo sem interferir em qualquer outro arquivo.

Mas mesmo colocando como “**DETECTADO**”, o **MAV** não permitirá que este arquivo seja executado, causando problemas no dispositivo. Ele mantém o arquivo sob observação, e não permite que a ameaça se espalhe ou seja executada. Esse comportamento existe para evitar perdas inesperadas.

+ Tratando Falsos Positivos

No caso de uma suspeita de um falso positivo, recomendamos primeiramente a realização do upload do arquivo no site da **Virus Total** (<http://www.virustotal.com>).

O **Virus Total** submete o arquivo à análise das principais soluções de antivírus do mercado e informa em quais foram detectadas ameaças.

Caso você confirme ou já tenha certeza que se trata de um falso positivo, você pode acessar **este link**, que é um canal direto da **Bitdefender**, onde será possível enviar informações sobre este arquivo (juntamente com o arquivo) e solicitar uma análise da **Bitdefender**.

Uma vez que eles constatem que não há nenhuma ameaça no arquivo, o mesmo será reclassificado e removido da lista de exclusão interna.

Observação: Se preferir, você pode abrir um chamado conosco, informando o nome do dispositivo e um print screen ou URL da infecção detectada, e nós iremos tratar esse falso positivo junto a **Bitdefender**.

A primeira opção é mais interessante, porque toda informação que a **Bitdefender** passar será diretamente para o teu e-mail, mas caso queira, nós podemos fazer esta intervenção, e toda informação será passada a você através do ticket aberto.

+ Tratando Arquivos do Tipo PUA

Outra opção são as detecções de ameaças do tipo **PUA**, ou seja, aplicativos potencialmente indesejados. Por não representarem necessariamente uma ameaça, as ações comuns (ignorar, deletar, quarentena) não são aplicáveis a eles, uma vez que não possuem assinaturas de ameaça, como por exemplo, malware.

No **N-sight RMM** você pode identificar o tipo de ameaça através da coluna “**Tipo de ameaça**” da guia “**Antivírus**”, no painel Sul.

Você pode alterar o comportamento do **MAV**, no caso de **PUAs**. Basta ir na política de proteção utilizada e, na guia “**Verificando**”, alterar as opções de **Aplicativos potencialmente indesejados (PUA)**.

No modo “**Desligado**”, a detecção de **PUAs** não será realizada. No modo “**Normal**” a detecção é feita, registrada e analisada pela proteção ativa. Já o modo “**Agressivo**” a detecção é imediatamente bloqueada.

4. Manutenção

Eventualmente, pode ser necessário intervir manualmente para que o MAV realize as seguintes ações:

- **Forçar a atualização das definições de ameaças:**
 - Botão direito do mouse sobre o dispositivo;
 - Antivírus Gerenciado;
 - Atualizar definições de ameaça.
- **Forçar varreduras rápidas e profundas:**
 - Botão direito do mouse sobre o dispositivo;
 - Antivírus Gerenciado;
 - Verificação rápida ou profunda.
- **Pausar a proteção do antivírus por um tempo indeterminado:**
 - Botão direito do mouse sobre o dispositivo;
 - Antivírus Gerenciado;
 - Adiar o antivírus

5. Relatórios

Além das informações contidas na aba Antivírus, no painel Sul do **N-sight RMM**, para um determinado dispositivo, é possível obter relatórios das informações captadas pelo **MAV**.

O **N-able N-sight RMM** disponibiliza 5 relatórios para o **Antivírus Gerenciado**:

- **Relatório de Ameaças:** Neste relatório é possível ter uma informação detalhada sobre as ameaças encontradas nos dispositivos, permitindo filtrar as informações por Cliente, Site e detalhes do evento, dentro de um determinado período selecionado. Permite ser exportado para CSV.
- **Relatório de Proteção Antivírus:** Neste outro relatório é possível obter informações sobre o antivírus gerenciado nos dispositivos. Apresenta a versão de definição de ameaças, qual é a política de proteção aplicada, quantos itens estão em quarentena, horário da última verificação e se a criptografia de disco está ativada ou não. Permite ser exportado para CSV.
- **Relatório de Quarentena:** Como o próprio nome sugere, este relatório traz uma informação detalhada sobre todas as ameaças que foram encaminhadas para a Quarentena, podendo trazer também o rastro de cada ameaça nos dispositivos. Permite ser exportado para CSV.
- **Relatório de Criptografia de Disco:** Por este relatório é possível obter as informações sobre os dispositivos que estão com a criptografia de disco ativada, trazendo detalhes do dispositivo e do volume. Permite ser exportado para PDF.
- **Relatório de Chave de Recuperação:** E por este último relatório é possível obter informações sobre a chave de recuperação da criptografia de disco, sendo possível obter informações até de dispositivos removidos (com o máximo 90 dias). Permite ser exportado para PDF.



Empresa brasileira, iniciamos nossas operações em 2013 com o objetivo de revolucionar o mercado de Prestação de Serviços de TI e contribuir com o enriquecimento moral, intelectual e financeiro de nossos clientes e colaboradores.

Nascemos da necessidade de um Prestador de Serviços de TI e hoje somos Distribuidores das melhores ferramentas para Prestadores de Serviços de TI de todo o Brasil.

Trabalhamos para o crescimento sustentável do mercado de tecnologia, através do compartilhamento de conhecimentos e a distribuição de soluções inovadoras para Gestão de TI. Com estrutura local, fornecemos atendimento e suporte em português, além de todo o apoio comercial necessário para empresas de Serviços de TI.

Compreendemos as necessidades locais e por isso somos o principal parceiro de negócios dos nossos clientes.

Com um time de profissionais altamente qualificados e apaixonados por tecnologia e relacionamento, colocamos acima de tudo, as pessoas. É assim que fazemos negócios.

Última alteração: Março/2023

Responsável: Caio Gutierri

E-mail: boaspraticas@addee.com.br



YouTube



Instagram



LinkedIn



Site



Blog