

Estratégia Trusted Connection™ Série de White Papers

Redução do risco de sistemas fora de controle com o ePolicy Orchestrator 3.5

Segundo da Série



McAfee®
System Protection

Soluções líderes de mercado em prevenção de invasões

NOTA DE DIREITOS AUTORAIS

Copyright © 2004 Network Associates Technology, Inc. Todos os direitos reservados. Nenhuma parte desta publicação poderá ser reproduzida, transmitida, transcrita, armazenada em sistemas de acesso ou traduzida em qualquer idioma, de qualquer forma ou por quaisquer meios sem a permissão por escrito da Network Associates Technology, Inc., ou de seus fornecedores ou empresas afiliadas. Para obter essa permissão, escreva para o departamento jurídico da Network Associates: 5000 Headquarters Drive, Plano, Texas 75024, ou ligue para +1-972-963-8000.

Índice

O que é a estratégia Trusted Connection da McAfee?	3
Introdução	4
O que é o McAfee ePolicy Orchestrator	5
Deteção de sistemas fora de controle no ePolicy Orchestrator 3.5	5
Panorama da arquitetura	6
O sensor de sistemas fora de controle	8
O servidor	8
Distribuição de sensores de sistemas fora de controle	9
Medidas de reação a sistemas fora de controle	10
Sistemas e dispositivos impossíveis de gerenciar	12
Perguntas mais frequentes	13
Acróimos usados neste documento	14

Aviso Legal

© Copyright 2004 Network Associates Technology, Inc. Todos os direitos reservados.

Este documento contém informações confidenciais e/ou reservadas ou segredos comerciais da Network Associates, Inc. nenhuma parte desta publicação pode ser reproduzida, transmitida, transcrita, armazenada em sistema de acesso, distribuída, revista, modificada ou traduzida em qualquer idioma, de qualquer forma ou por quaisquer meios sem a permissão por escrito da Network Associates Technology, Inc., de seus fornecedores ou de suas empresas afiliadas. Para obter essa permissão, escreva para o departamento jurídico da Network Associates: 5000 Headquarters Drive, Plano, Texas 75024, ou ligue para +1-972-963-8000.

A Network Associates, Inc. não faz qualquer declaração nem oferece qualquer garantia em relação ao teor desta obra, isentando-se especificamente de qualquer garantia expressa ou implícita de possibilidade de comercialização ou adequação a qualquer finalidade específica. A Network Associates reserva para si o direito de revisar esta obra e de realizar alterações no seu conteúdo, a qualquer momento, sem qualquer obrigação de notificar qualquer pessoa física ou jurídica a respeito das revisões ou alterações.



Redução do risco de sistemas fora de controle com o ePolicy Orchestrator 3.5

Panorama Técnico

Este *white paper* é o segundo da série da Estratégia Trusted Connection da McAfee. A série foi criada para apresentar idéias e detalhes sobre partes específicas da Estratégia Trusted Connection™ da McAfee.

Este trabalho trata da *Redução do risco de sistemas fora de controle com o ePolicy Orchestrator 3.5*. O número de referência deste documento é White Paper 2.

As informações apresentadas neste documento são um panorama de como usar o ePolicy Orchestrator 3.5 para monitorar — em tempo real — sistemas fora de controle ou desprotegidos que se conectam à rede interna. O objetivo aqui não é demonstrar estratégias de bloqueio automático, que serão apresentadas em *white papers* ou aperfeiçoamentos do produto subseqüentes.

O que é a Estratégia Trusted Connection da McAfee?

A estratégia Trusted Connection da McAfee é uma maneira de garantir a conformidade dos sistemas com a segurança antes que eles se conectem à rede da empresa. Esta estratégia baseia-se em várias iniciativas tecnológicas da McAfee Security e em parcerias fundamentais com os principais fabricantes de VPNs, acesso remoto, sistemas sem fio e redes do mercado.

O objetivo desta estratégia é permitir que os usuários da McAfee verifiquem a conformidade dos sistemas com a segurança antes que eles se conectem à rede, além de colocá-los automaticamente em conformidade, se for necessário, a partir de pontos de acesso externos e internos. Com essas soluções, os administradores de TI podem assegurar que somente os sistemas configurados de maneira segura possam se conectar à sua rede corporativa, obtendo maior controle e melhorando a proteção preventiva contra vulnerabilidades e contra a transferência de vírus, worms e cavalos de Tróia.

Introdução

Uma das dificuldades enfrentadas por qualquer empresa no gerenciamento da segurança dos seus sistemas e para assegurar a proteção total da empresa é que, para fiscalizar a conformidade com as políticas, é necessário saber que o sistema existe. Essa situação é complicada pelo fato de que, na maioria das redes, a única exigência para a conexão é o acesso físico. Não há necessidade de nenhuma autenticação a mais. Portanto, qualquer visitante que entre no prédio de uma empresa e use, sem intenção, uma conexão de rede disponível representa uma considerável ameaça a essa empresa.

Essa situação pode ocorrer com:

- Contratados, funcionários terceirizados ou parceiros de negócios — cujos computadores não são gerenciados pela sua infra-estrutura de segurança — conectando-se à rede.
- Recursos ou sistemas desconhecidos ou não-autorizados na empresa que se conectam à rede, embora possam passar despercebidos.
- Visitantes em salas de reunião que se conectam à rede para sincronizar seus e-mails.

Um único computador que não conte com proteção gerenciada adequada pode constituir uma ameaça a toda a rede, e isso significa que conhecer todos os sistemas conectados à rede é essencial ao sucesso da proteção da empresa. Sistemas que se conectam à rede e que não são conhecidos ou que não estão de acordo com a política de segurança definida são considerados *sistemas fora de controle*.

Existem várias estratégias de criação e manutenção de uma lista de todos os sistemas conectados a uma rede, mas cada uma delas apresenta consideráveis desvantagens:

Estratégia	Desvantagem
Manter manualmente uma lista de todos os sistemas de uma rede	Não é possível na maioria das redes de hoje, pois o ambiente de rede é muito dinâmico para que uma única pessoa (ou até mesmo mais de uma pessoa) mantenha atualizado esse tipo de lista.
Cadastramento dos sistemas com scripts de login	Os scripts de login são executados <i>após</i> a autenticação de um usuário em alguma entidade (por exemplo, um domínio do Windows). Portanto, o script de login não é pré-requisito para que um sistema se conecte à rede.
Varreduras periódicas por meio de uma ferramenta de varredura ativa (por exemplo, Nmap) ou uma ferramenta semelhante de varredura de vulnerabilidades	Se as varreduras forem periódicas, apenas os sistemas fora de controle conectados no exato momento da varredura serão descobertos. O aumento da frequência das varreduras para compensar não é viável, pois elas podem ser: <ul style="list-style-type: none"> ▪ Muito demoradas. ▪ Invasivas, criando muito tráfego de rede e, às vezes, gerando um tráfego que afeta negativamente os serviços que estão passando pela varredura. A execução das varreduras também pode ser impedida por programas de firewall de desktop, se eles tiverem sido configurados para ignorar todas as conexões feitas de fora, tornando um sistema invisível para programas de varredura.
Importação periódica de um diretório (por exemplo, Active Directory)	Embora esse método reduza muito o tempo gasto pela administração com a manutenção do diretório, ele tem as mesmas limitações das duas estratégias anteriores. Como na varredura ativa, ele é periódico e, como nos scripts de login, ele não permite que os ePolicy Orchestrator veja os sistemas da rede que não estiverem registrados no Active Directory.

Para contornar essas dificuldades e as limitações das soluções existentes, a McAfee está apresentando uma abordagem inovadora de detecção e gestão de sistemas fora de controle, com o lançamento do McAfee ePolicy Orchestrator 3.5.

O que é o McAfee ePolicy Orchestrator?

O McAfee ePolicy Orchestrator, ou ePO, é a solução líder de mercado para gerenciamento de sistemas – proporcionando à empresa uma defesa preventiva contra ameaças e ataques. Oferecendo uma ampla e incomparável gestão de segurança de sistemas ao mais baixo custo de propriedade, ele garante a conformidade com a política de segurança de sistemas e a eficiência da proteção dos sistemas, evitando as dispendiosas interrupções dos negócios causadas por infecções e ataques de invasão. Com o eixo central das soluções de proteção de sistemas da McAfee, os administradores podem tomar a iniciativa de reduzir o risco de sistemas fora de controle e não-conformes, manter atualizada a proteção, configurar e fiscalizar as políticas de proteção e monitorar as condições de segurança 24 horas por dia, 7 dias por semana, a partir de um único console centralizado e com verdadeira flexibilidade de grande porte.

Detecção de sistemas fora de controle no ePolicy Orchestrator 3.5

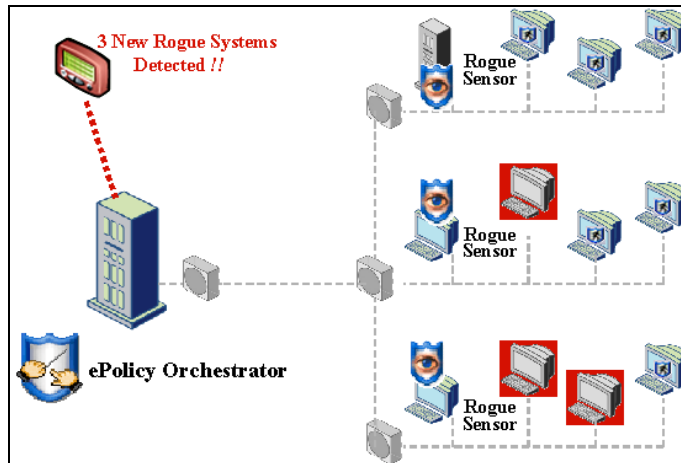
A detecção de sistemas fora de controle é um novo recurso da próxima versão do ePolicy Orchestrator 3.5. Esse recurso foi criado para aumentar a conformidade com as políticas nas empresas, identificando todos os sistemas fora de controle ou desprotegidos, além de permitir que o ePolicy Orchestrator invoque uma reação por políticas nesses sistemas.

No coração da solução está um sensor lógico (*software*) que emprega o monitoramento passivo para detectar todos os sistemas que participam da rede. Especificamente, o sensor escuta transmissões de L2 (para saber mais, veja [Sobre o modelo de referência OSI em 7 níveis](#) na página 7). Os computadores que participam de uma rede tendem a fazer transmissões múltiplas frequentes, especialmente quando acabam de entrar em uma rede. Portanto, os novos sistemas são normalmente detectados pelo sensor em questão de segundos após a primeira conexão à rede. Os sensores distribuídos por toda a empresa relatam todos os sistemas detectados ao servidor ePolicy Orchestrator e o servidor determina quais desses dispositivos estão fora de controle.

Panorama da arquitetura

O diagrama abaixo apresenta um panorama da arquitetura de detecção de sistemas fora de controle.

Figura 1: Panorama da arquitetura



Ao menos um sensor de sistemas fora de controle deve ser instalado em cada segmento L2 em toda a empresa, uma vez que os sensores detectam sistemas por transmissões (que são propagadas apenas por meio de um segmento L2). À medida que os sistemas são detectados, o sensor utiliza o protocolo HTTPS para enviar mensagens descrevendo os sistemas ao servidor ePolicy Orchestrator. O sensor não realiza qualquer tentativa de classificar os sistemas como “fora de controle” ou “gerenciados”; ele simplesmente relata tudo o que vê.

Quando o servidor ePolicy Orchestrator recebe uma mensagem de **sistema detectado**, ele inspeciona o banco de dados para determinar se o sistema deve ser classificado como “fora de controle” ou “gerenciado”. Um sistema é considerado fora de controle quando:

- Não estiver presente no banco de dados de sistemas gerenciados do ePolicy Orchestrator, e
- O agente ePolicy Orchestrator do sistema não estiver se comunicando ativamente com o servidor.



O ePolicy Orchestrator fiscaliza a política nos sistemas por meio de um pequeno agente de software que funciona nos sistemas gerenciados. Esses agentes são responsáveis pela verificação periódica do servidor ePolicy Orchestrator para obter as configurações de políticas mais recentes. Se um agente deixar de verificar e confirmar a sua configuração de política, isso será considerado uma violação de política porque o servidor ePolicy Orchestrator não poderá confirmar se as configurações do sistema estão atualizadas.

O endereço MAC (Controle de Acesso à Mídia) detectado do sistema é usado como principal chave na pesquisa do banco de dados de sistemas gerenciados do ePolicy Orchestrator; o hostname também pode ser usado para reduzir falsos positivos nos casos em que um sistema utilizar várias interfaces de rede, por exemplo, um laptop com conexão sem fio e Ethernet (consulte detalhes nas [Perguntas mais freqüentes](#) na página 13).

Um sensor informa sobre um determinado sistema na primeira vez em que ele for detectado (por exemplo, quando o primeiro pacote transmitido que contenha o endereço MAC desse sistema for recebido pelo sensor) e, em seguida, passa a informar somente uma vez por período de tempo (configurável, que é de 1 hora se nada for definido em contrário). Sempre que o servidor receber uma mensagem de **sistema detectado** em relação a um sistema detectado anteriormente, ele recalcula e atualiza o status de “fora de controle” e outras informações associadas ao sistema. Esse modelo de processamento tem algumas conseqüências altamente desejáveis:

- As informações dos sistemas fora de controle no banco de dados do ePolicy Orchestrator representam o estado de momento da rede, não um instantâneo de algum momento anterior, o que acontece com as ferramentas de varredura ativas.
- O administrador pode saber se um sistema fora de controle ainda está ativo, quando ele esteve ativo pela última vez e por quanto tempo ele esteve na rede. A seção de sistemas fora de controle do console do ePolicy Orchestrator classifica sistemas **inativos** (sistemas que não se comunicaram durante um determinado período de tempo – que pode ser configurado) separadamente dos **sistemas ativos fora de controle**, de forma que o administrador possa se dedicar às ameaças atuais à rede.
- A arquitetura do servidor fica muito simples porque o status de cada sistema fora de controle e outras propriedades permanecem atualizados sem qualquer processamento explícito em segundo plano. O servidor processa as ocorrências à medida que elas chegam.

Sobre o modelo de referência OSI em 7 níveis

O modelo de referência OSI (Interconexão de Sistemas Abertos) é um modelo teórico de como as aplicações em rede se comunicam entre eles. Esse modelo descreve uma pilha de protocolos em 7 níveis, na qual cada nível representa um protocolo de rede que aproveita os recursos do nível imediatamente inferior. Aplicações, tais como http funcionam no **Nível 7**, ao passo que os meios físicos são representados no **Nível 1**. Os níveis importantes para a compreensão deste documento são os seguintes:

Nível 2 — Nível de Link de Dados: A Ethernet é um exemplo de protocolo de L2. Os dispositivos são endereçados por meio do seu endereço MAC (Controle de Acesso à Mídia) de 6 bytes. A Ethernet permite o envio de pacotes a um único dispositivo ou a transmissão múltipla simultânea (*broadcast*) desses pacotes a todos os dispositivos da rede. Os dispositivos que receberão os pacotes transmitidos um do outro são considerados como pertencentes ao mesmo domínio de transmissão múltipla simultânea; um domínio de transmissão múltipla simultânea é, às vezes, chamado de “segmento”. Pode-se usar *hubs*, *switches* e pontes para conectar dispositivos em um domínio de transmissão múltipla simultânea. Os roteadores não encaminham pacotes transmitidos simultaneamente; portanto, uma rede de L2 pode conter muitos *switches* e *hubs*, mas não terá nenhum roteador.

Nível 3 — Nível de Conexão em Rede: O IP (Protocolo de Internet) está neste nível. Os dispositivos em uma rede IP (v4) são endereçados por meio de um endereço IP de 4 bytes. O ARP (Protocolo de Conversão de Endereços) é usado para converter endereços IP de L3 em endereços MAC de L2; isso é necessário porque, em um segmento, o L3 depende do L2 para transmitir pacotes ao host remoto. O ARP depende da função de transmissão múltipla simultânea do L2 para perguntar a todos os sistemas da rede: *Para quem tiver o endereço IP 1.2.3.4, qual é o seu endereço MAC?* Várias redes IP são conectadas por meio de roteadores.

Para saber mais, existem vários *sites* úteis na Internet (por exemplo, http://www.webopedia.com/quick_ref/OSI_Levels.asp).

O sensor de sistemas fora de controle

Como já foi mencionado, o sensor detecta sistemas escutando as transmissões simultâneas do L2. Dois dos protocolos de rede comuns que utilizam transmissões simultâneas são o ARP, usado para converter endereços IP de L3 em endereços MAC de L2, e o DHCP (Protocolo de Configuração Dinâmica de Hosts), usado para atribuir dinamicamente endereços IP a hosts. É muito raro que um sistema se conecte e use uma rede sem utilizar um desses protocolos. Provas empíricas também demonstram que os computadores usados ativamente tendem a fazer transmissões simultâneas com uma certa frequência.

O sensor não é totalmente passivo na sua coleta de informações. Embora o IP e o MAC sejam coletados passivamente, o sensor faz uma consulta ativa para obter o hostname e as propriedades. Quando o sensor recebe um pacote de transmissão múltipla simultânea, ele extrai o endereço IP de origem e o endereço MAC. Antes que a existência do sistema seja informada ao servidor, o sensor coleta mais algumas informações no host, as quais são incluídas na mensagem **sistema detectado**, por exemplo:

- O nome do DNS.
- O nome do NetBIOS.
- Várias outras propriedades do NetBIOS.

O sensor de sistemas fora de controle é um serviço lógico leve que funciona em sistemas não-dedicados e é instalado e gerenciado por meio dos parâmetros de configuração do ePolicy Orchestrator, definidos com o console do ePolicy Orchestrator e fiscalizados em cada sistema pelos agentes ePolicy Orchestrator. A instalação do sensor pode ocorrer de uma das seguintes maneiras: por meio do ePolicy Orchestrator, com um instalador autônomo ou com uma imagem de disco copiada. Independentemente da maneira de instalação, o sensor precisa da presença do ePolicy Orchestrator para funcionar corretamente.

O servidor

As informações em todos os sistemas detectados e o seu status de “fora de controle” são armazenados no banco de dados do ePolicy Orchestrator. O servidor também controla em quais sub-redes os sistemas foram encontrados e quais sensores estão informando ativamente a sua presença em cada sub-rede. Essas informações são exibidas em uma janela HTML incorporada ao console do ePolicy Orchestrator. A página **Máquinas Fora de Controle** apresenta um resumo geral dos sistemas fora de controle e gerenciados detectados na rede, além de permitir o aprofundamento até um modo de exibição de lista filtrada e detalhes sobre cada sistema. O modo de exibição de lista pode ser organizado por sub-rede ou filtrado e classificado por praticamente qualquer tipo de informação conhecida sobre os sistemas.

Figura 2: Máquinas Fora de Controle : Lista de Máquinas

The screenshot shows the 'Rogue Machines' interface in the McAfee ePolicy Orchestrator. The page title is 'Rogue Machines' and it includes navigation tabs for 'Machines', 'Subnets', 'Events', 'Responses', and 'Configuration'. Below the navigation, there are options for 'Summary' and 'List'. The main section is titled 'Machine List' and includes a filter set to '192.168.1.0 - (Custom Filter)'. There are also buttons for 'Refresh (Auto)', 'Configure Table', and 'Custom Filter'. A 'Back' button is located in the top right corner of the machine list area.

<input type="checkbox"/>	Status	Rogue Type	Friendly Name	IP	Last Detect Time
mdb-padre 192.168.1.0/24					
<input type="checkbox"/>	Rogue	No Agent	Apple	192.168.1.100	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Pear	192.168.1.101	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Walnut	192.168.1.102	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Salmon	192.168.1.103	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Thyme	192.168.1.104	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Cookie	192.168.1.105	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Pork	192.168.1.106	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Ginger	192.168.1.107	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Egg	192.168.1.108	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Grape	192.168.1.109	5/24/04 3:27:44 PM
<input type="checkbox"/>	Rogue	No Agent	Salsa	192.168.1.110	5/24/04 3:27:44 PM

At the bottom of the table, there are links for 'Check All' and 'Uncheck All', and a note that '11 items in 1 page.' Below the table, there is a section for 'Checked machines:' with a dropdown menu set to 'Add to ePO tree' and an 'Apply' button.

Distribuição de sensores de sistemas fora de controle

Dada a necessidade de um sensor por sub-rede, como o administrador pode distribuir sensores com facilidade em todas as sub-redes gerenciadas e, depois, ter certeza de que, a qualquer momento do futuro, todos os segmentos continuarão contando com ao menos um sensor instalado neles? O console do ePolicy Orchestrator possui várias maneiras de solucionar diretamente essa questão.

- Sub-redes com ao menos um sensor instalado e enviando informações ativamente são consideradas protegidas.
- Sub-redes sem nenhuma atividade de sensor durante um determinado período de tempo (que pode ser configurado) são consideradas desprotegidas.

A seção de sistemas fora de controle do console do ePolicy Orchestrator exibe uma lista de todas as sub-redes conhecidas pelo ePolicy Orchestrator, além da sua situação de proteção. Os administradores podem configurar o ePolicy Orchestrator para que seja enviado um aviso quando qualquer sub-rede anteriormente protegida ficar desprotegida. Isso pode acontecer se um sistema que hospeda um sensor for desligado ou mudar de sub-rede. Essa situação também pode ser solucionada com a instalação de mais de um sensor por sub-rede.

Como uma sub-rede precisa ficar em um único domínio de transmissão múltipla simultânea (por exemplo, uma sub-rede não pode cobrir dos ou mais domínios de transmissão múltipla simultânea), se você garantir que todas as sub-redes estão protegidas, também poderá garantir que todos os domínios de transmissão múltipla simultânea estarão protegidos. Em toda a seção de sistemas fora de controle do console do ePolicy Orchestrator, a proteção pelos sensores é descrita em termos de sub-redes, não de segmentos ou domínios de transmissão múltipla simultânea.

Figura 3: Máquinas Fora de Controle : Lista de Sub-Redes

The screenshot shows the 'Rogue Machines' interface with the 'Subnet List' window open. The window has a 'Back' button and a 'Filter: (Custom Filter)' dropdown. Below the filter are 'Refresh (Auto)', 'Configure Table', and 'Custom Filter' options. The main content is a table with the following data:

<input type="checkbox"/>	Status	Address/Mask	Network Name	Sensors	Last Sensor Comm.
<input type="checkbox"/>	Uncovered	10.13.50.0/24	QA	0	
<input type="checkbox"/>	Covered	10.13.51.0/24	Dev	1	5/24/04 3:41:19 PM
<input type="checkbox"/>	Uncovered	10.13.52.0/24	HR	1	5/19/04 3:48:14 PM
<input type="checkbox"/>	Uncovered	10.13.53.0/24	Support	0	
<input type="checkbox"/>	Uncovered	10.13.54.0/24	Sales	0	
<input type="checkbox"/>	Covered	10.13.55.0/24	Marketing	2	5/24/04 3:47:35 PM

Below the table are 'Check All' and 'Uncheck All' buttons. At the bottom right, it says '176 items in 12 pages. Go to page: 1'. Below the table is a 'checked subnets:' section with a 'Deploy Sensors' button.

Na janela **Subnet List (Lista de Sub-Redes)**, o administrador pode selecionar sub-redes que não estão protegidas e instalar sensores nelas por meio dos recursos de instalação de software do ePolicy Orchestrator. Nas sub-redes selecionadas, os sistemas usados para hospedar o software do sensor podem ser selecionados manualmente em uma lista ou escolhidos automaticamente pelo servidor ePolicy Orchestrator, utilizando critérios definidos pelo administrador. Entre os possíveis critérios de seleção automática de sistemas estão os seguintes: versão do sistema operacional, velocidade do processador, memória do sistema ou a hora da última comunicação do agente ePolicy Orchestrator.

Medidas de reação a sistemas fora de controle

Existem varias medidas diferentes que um administrador pode tomar para reagir à detecção de sistemas fora de controle. Cada uma dessas medidas pode ser tomada manualmente, por meio da seleção do sistema na lista de sistemas fora de controle da interface do usuário e, em seguida, selecionando a medida, ou por meio da implementação automática de uma reação predefinida.

As medidas automáticas possuem um conjunto de condições associadas. Com a detecção de novos sistemas fora de controle, as medidas são invocadas apenas se as condições forem satisfeitas. A condição de uma medida pode depender de qualquer uma das informações conhecidas sobre um sistema fora de controle, podendo ser uma simples comparação de um único campo ou um comando composto complexo. Um exemplo de condição pode ser a frase em português: *Se o IP de um novo sistema fora de controle estiver no intervalo entre 192.168.1.0/24 e o sistema operacional for o Windows, envie um agente ePolicy Orchestrator para esse sistema.* Uma medida automática e as suas condições associadas são denominadas coletivamente "reação automática" na seção de sistemas fora de controle do console do ePolicy Orchestrator.

Figura 4: Máquinas Fora de Controle : Incluir ou Editar Resposta Automática

Rogue Machines

Machines Subnets Events Responses Configuration

Automatic Responses Help

Add or Edit Automatic Response [Back]

Name:

Event: **Rogue Machine Detected**

Enabled:

Conditions:

Match All (AND) Match Any (OR)

Property	Comparison	Value	Delete
IP	is in range	192.168.1.0 - 192.168.1.255	✖
OS Platform	contains	Windows	✖

Actions:

Method	Parameters	Delete
Mark as Exception	(none)	✖
Add to ePO tree		
Mark for Action		
Mark as Exception		
Push ePO Agent		
Query ePO agent		
Remove Host		
Send E-mail		
Send ePO Server Event		
Unmark For Action		
Unmark as Exception		

Estas são algumas das ações que podem ser realizadas em sistemas fora de controle detectados:

- **Distribuir o Agente ePO:** Esta é a forma mais direta de resolução de sistemas descontrolados. Assim que o agente é instalado, ele aplica as políticas do ePolicy Orchestrator, e o sistema-alvo é considerado gerenciado. Quando isso ocorrer, o servidor o retira da lista de sistemas fora de controle.
- **Enviar E-mail:** Com a nova função de alerta do ePolicy Orchestrator, o administrador pode receber avisos por e-mail ou SNMP quando um novo sistema fora de controle for encontrado.
- **Executar uma ferramenta externa:** Outras opções aparecem no menu suspenso se você tiver alguma ferramenta externa (de outro fabricante) instalada. Uma ferramenta externa pode ser qualquer executável instalado no servidor ePolicy Orchestrator. Esta ação permite a personalização da solução ou notificação (um recurso que não existe originalmente no ePolicy Orchestrator). Isso também permite a integração de ferramentas de sondagem de outros fabricantes para que o administrador possa coletar mais informações sobre um determinado sistema fora de controle antes de tomar outras providências.
- **Marcar como Exceção:** Marcar um sistema como uma exceção altera o seu estado no banco de dados de sistemas fora de controle para indicar que ele não pode ser gerenciado pelo ePolicy Orchestrator e, portanto, não deve ser considerado fora de controle. Consulte [Sistemas e dispositivos impossíveis de gerenciar](#) na página 12 para saber mais sobre falsos positivos, além de detalhes sobre exceções
- **Marcar para Ação:** Marcar um sistema como “aguardando ação posterior” é uma forma que os administradores têm para marcar sistemas fora de controle que ainda não podem ser solucionados, mas que querem rever posteriormente para que possam tomar outras providências. A lista de sistemas pode ser classificada ou filtrada de acordo com a existência ou não de uma marca de ação nesses sistemas. Essa marca é exibida ao lado do nome do sistema no console do ePolicy Orchestrator.

Sistemas e dispositivos impossíveis de gerenciar

A classificação de sistemas impossíveis de gerenciar como “fora de controle” ocorrerá em todas as redes. Entretanto, algumas dessas classificações podem ser falsos positivos. Isso ocorre porque muitos dos dispositivos participantes de uma rede não precisam poder ser gerenciados pelo ePolicy Orchestrator. Alguns exemplos de falsos positivos: roteadores, impressoras, vários tipos de dispositivos físicos (appliances) de rede, e sistemas que funcionam com sistemas operacionais que o ePolicy Orchestrator não reconhece. Para impedir que esses sistemas sejam classificados como “fora de controle”, o banco de dados de sistemas fora de controle trabalha com a noção de “sistemas excepcionais”, que podem ser marcados no console do ePolicy Orchestrator.

Quando o administrador marca como exceções os sistemas “fora de controle” que não podem ser gerenciados, esses sistemas deixam de aparecer na lista de sistemas fora de controle do ePolicy Orchestrator. As informações coletadas pelo sensor (nome do DNS, nome do NetBIOS e outras informações do NetBIOS, tais como sistema operacional, comentários e domínio) e o nome OUI (Identificador Exclusivo dentro da Empresa) da IEEE. O OUI ocupa os três primeiros bytes de um endereço MAC, sendo registrado para uma empresa ou organização (normalmente, um fabricante de placas de rede). O OUI pode ajudar o administrador a identificar exceções. Ferramentas de sondagem de terceiros e outros aplicativos externos também podem ser usados para coletar mais informações. Então, os dados gerados são capturados e exibidos junto com as informações de outros sistemas fora de controle.

Além de selecionar manualmente os sistemas como exceções, o administrador também pode criar regras para marcar sistemas como exceções quando eles satisfizerem determinados critérios, utilizando o mecanismo de reação automática descrito anteriormente. Por exemplo, se uma empresa utiliza roteadores da Cisco e não usa nenhuma placa de rede desse fabricante, uma das possíveis reações automáticas é *“Se o nome do OUI de um novo sistema fora de controle contiver ‘Cisco’, marque-o como exceção.”*

Imediatamente após a primeira instalação de sensores de sistemas fora de controle, são previstos alguns falsos positivos que não precisam ser gerenciados pelo ePolicy Orchestrator. Durante esse período de ajuste, o administrador deve marcar manualmente esses sistemas como exceções ou gravar reações automáticas para ajudar a automatizar o processo. Após a maioria das exceções ser encontrada, a maior parte das detecções de novos sistemas fora de controle será legítima. Nesse momento, o administrador pode permitir o uso de regras ou notificações mais agressivas de solução automática.

Perguntas mais freqüentes

Os sensores funcionam corretamente em uma rede comutada?

Sim, porque os switches propagam tráfego de transmissão múltipla simultânea de L2. Os switches apenas limitam os dispositivos em um domínio de transmissão múltipla simultânea que podem ver pacotes de difusão ponto a ponto (*unicast*).

Os sensores funcionam corretamente em uma LAN virtual (VLAN)?

Sim, do ponto de vista da detecção de sistemas fora de controle, não há diferença entre uma VLAN e uma LAN. Os switches que operam com VLANs devem encaminhar pacotes de transmissão múltipla simultânea a cada um dos outros dispositivos da VLAN, e um sensor deve ser instalado por VLAN.

Os sensores funcionam corretamente com switches em tronco (por exemplo, 802.1q)?

Sim, os switches com tronco, que permite a extensão de uma VLAN a vários switches por meio da transmissão do tráfego da VLAN por meio de um único link ponto a ponto, precisam garantir que o tráfego de transmissão múltipla simultânea seja propagado a todos os dispositivos da VLAN. Do ponto de vista da detecção de sistemas fora de controle, uma VLAN que se estende a switches com tronco não difere de uma VLAN em um switch ou uma LAN normal.

Os sensores funcionam corretamente com placas de rede (NICs) que não operam no modo promiscuo?

Sim, o uso do driver de uma placa de rede no modo promiscuo é necessário apenas para o recebimento de pacotes de difusão ponto a ponto cujo destino não seja o sistema local. Como o sensor escuta apenas pacotes de transmissão múltipla simultânea, ele não precisa abrir o driver no modo promiscuo.

O sensor detecta sistemas que se conectam por meio de uma VPN?

Não, os servidores de VPN atuam como roteadores (L3). Portanto, eles não propagam transmissões múltiplas simultâneas em L2. Entretanto, como parte da estratégia Trusted Connection, a McAfee estabeleceu várias parcerias com grandes fornecedores de VPNs, entre eles Check Point, Nortel, Neoteris, Cisco e Aventail para permitir a detecção e o bloqueio de sistemas que não atinjam um nível predefinido de conformidade de segurança. No início, essas parcerias se dedicam à conformidade antivírus, mas, com o tempo, estamos procurando aumentar a profundidade dessas parcerias.

O sensor detecta sistemas que se conectam por meio de um Ponto de Acesso Sem Fio (WAP)?

Sim, se houver um sensor na sub-rede sem fio, ele detectará todos os sistemas que se conectam por meio de um WAP. Se um WAP estiver atuando como roteador ou dispositivo de NAT e o sensor estiver do lado de fora, ele detectará a presença do próprio WAP, mas não poderá ver nada dentro da rede sem fio.

O sensor precisa funcionar em um sistema dedicado?

Não, embora seja desejável que os sensores funcionem em sistemas que não sejam desligados regularmente por longos períodos de tempo, o sensor não precisa necessariamente funcionar em servidores ou sistemas dedicados. O consumo de memória e processador de um sensor é muito pequeno; normalmente, a utilização não chega a 1% em uma máquina de 500 MHz, e o consumo normal de memória é de 5-10 megabytes. O sensor não precisa de hardware especial.

A detecção de sistemas fora de controle pode lidar com sistemas que sempre se conectam com várias placas de rede, tais como um laptop com uma placa sem fio e um conector Ethernet e uma estação de ancoragem?

Sim, embora o endereço MAC seja a chave principal usada para procurar sistemas detectados no banco de dados do ePolicy Orchestrator, a detecção de sistemas fora de controle também pode ser configurada para pesquisar apenas pelo hostname, *ou* tanto pelo hostname quanto pelo domínio. Nesse caso, independentemente de onde o laptop for detectado na rede sem fio ou na LAN, se ele for gerenciado pelo ePolicy Orchestrator, será encontrado no banco de dados e identificado corretamente como “gerenciado”.

Como a detecção de sistemas fora de controle lida com sistemas gerenciados por outro servidor ePolicy Orchestrator?

Esses sistemas serão considerados fora de controle, mas o sistema de detecção de sistemas fora de controle pode ser configurado para identificar esses sistemas como possuidores de *agentes externos*. O servidor de detecção de sistemas fora de controle consultará a presença de um agente do ePolicy Orchestrator nesses sistemas e, se um agente for encontrado, o sistema será identificado como possuidor de um agente externo. O nome do servidor externo do ePolicy Orchestrator será registrado e exibido na seção de detecção de sistemas fora de controle do console do ePolicy Orchestrator.

Acrônimos usados neste documento

ARP	Protocolo de Conversão de Endereços
HTTPS	Protocolo (Seguro) de Transferência de Hipertexto
LAN	Rede Local
Lx	Nível x (onde x é um número) do modelo de referência OSI
MAC	Controle de Acesso à Mídia
NAT	Conversão de Endereços de Rede
NIC	Placa de Rede
Nmap	Ferramenta de Mapeamento de Rede
OSI	Interconexão de Sistemas Abertos
OUI	Identificador Exclusivo dentro da Empresa
VLAN	Rede Local Virtual
VPN	Rede Privada Virtual
WAP	Ponto de Acesso Sem Fio