RESUMO DA SOLUÇÃO

SEGURANÇA DE ENDPOINT COM CLEARPASS E INTROSPECT DA ARUBA

DESAFIOS DE SEGURANÇA ATUAIS

Os ataques direcionados de hoje são projetados para permanecer "sob o radar" movendo-se em passos pequenos, mas deliberados, por longos períodos de tempo - muitas vezes com credenciais legítimas de um usuário, sistema ou dispositivo comprometido.

A proteção contra ameaças cibernéticas agora requer uma estratégia de segurança multicamada que inclui a capacidade de detectar e combater ameaças que evadiram as regras tradicionais e as soluções baseadas em assinaturas, ao usar credenciais legítimas de funcionários comprometidos, contratantes, parceiros ou dispositivos IoT. De acordo com o Verizon 2016 Data Breach Investigation Report (Relatório de investigação de violação de dados Verizon 2016):

- Mais de 60% das violações confirmadas de dados envolvem senhas fracas, padrão ou roubadas
- 70% de todas as infrações de uso indevido de informação e de privilegios demoraram meses ou anos para ser descobertos.

As equipes de segurança normalmente lidam com esses tipos de ataques usando métodos de investigação manuais e demorados, com processos de remediação reativa e retardada que muitas vezes não são eficazes. O objetivo é aproveitar o controle de acesso granular e visibilidade - combinada com detecção automática de ataques - para uma abordagem de segurança mais proativa e oportuna:

- Visibilidade em todos os dispositivos conectados, multifornecedores, com e sem fio.
- Controle para garantir que apenas dispositivos autenticados ou autorizados acessem a empresa
- Resposta de ataque usando o próprio sistema de corretagem da ClearPass e parceiros de troca para fornecer segurança a vetores de ataque conhecidos e desconhecidos

DETECÇÃO DE ATAQUE AUTOMÁTICO E REMEDIAÇÃO ACELERADA

Dos sensores aos sistemas, dos sistemas aos usuários, os ataques internos exigem uma nova estratégia. Felizmente, soluções de segurança inovadoras que utilizam análises baseadas em aprendizado automático o de máquinas e grandes plataformas de dados agora podem fornecer às empresas uma nova dimensão de proteção que os produtos de segurança tradicionais não possuem.

BENEFÍCIOS DE ALTO NÍVEL

Seja um parceiro desonesto ou botnets IoT, o Aruba ClearPass e o IntroSpect fornecem um antídoto potente contra os ataques internos, não importa onde eles originem-se.

- Perfil e visibilidade de precisão com base no usuário em tempo real e no contexto do dispositivo
- Suporte para qualquer tipo de dispositivo, incluindo IoT
- Detecção de ataque baseada em aprendizado de máquina não disponível em defesas de segurança tradicionais
- Suporte de decisão escalável e abrangente para uma investigação e correção mais rápida
- Aplicação automatizada e precisa independentemente do tempo, localização ou proprietário do dispositivo
- Integração perfeita sem custos entre soluções

O Aruba IntroSpect, uma solução líder da indústria em Análise de Comportamento dos Usuários e Entidades (UEBA), usa o aprendizado de máquinas supervisionado e não supervisionado para automaticamente observar o comportamento básico do usuário e do dispositivo enquanto procura ativamente uma atividade anômala que pode indicar uma ameaça. Quando a UEBA da IntroSpect é integrada com o Aruba ClearPass, a solução combinada oferece três principais inovações de segurança: detecção de ataque avançado, investigação acelerada e aplicação proativa, baseada em políticas.

Agora, os usuários comprometidos ou mal-intencionados, ou sistemas que participam de ataques ou dispositivos IoT recrutados para um exército de botnet latente podem ser descobertos e remediados antes que o dano seja feito na infra-estrutura, os bens ou a reputação de uma organização.

ARUBA INTROSPECT E CLEARPASS PARA PROTECÇÃO DE 360 GRADOS

O IntroSpect detecta sistemas ou dispositivos de usuários comprometidos usando modelos de aprendizado de máquina supervisionados e não supervisionados para ver mudanças indicadoras no acesso e uso típico de TI. Quando esses sinais

sutis são agregados e colocados no contexto ao longo do tempo, confirma-se e alerta-se a presença de um próximo ataque. Através de uma comunicação bi-direcional bem integrada, o IntroSpect aciona o ClearPass para realizar uma alteração de autorização para a entidade em questão.

DETECTA, RESPONDE, INVESTIGA E REMEDEIA

CLEARPASS + UEBA = PROTECÇÃO 360 °

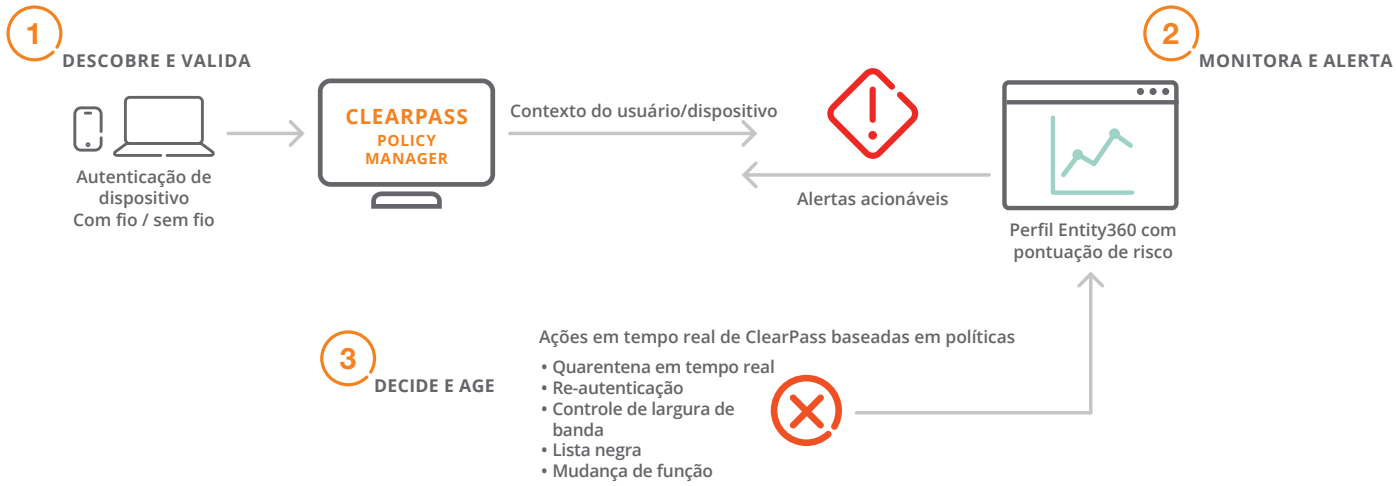

Figura 1: Quando a UEBA do IntroSpect é integrada com o Aruba ClearPass, a solução combinada oferece três inovações principais de segurança: detecção de ataque avançado, investigação acelerada e aplicação automatizada baseada em políticas.

Uma vez que a ameaça está sob controle, um analista pode então recorrer ao sistema de investigação de incidentes baseado em big data da IntroSpect, onde todo o histórico de TI da entidade sob o escrutínio (até o nível do pacote) está disponível em segundos, de modo que a tomada de decisões e a remediação são diminuídas de horas e dias a minutos.

PRIORIZA RISCOS DE SEGURANÇA

Portáteis funcionando mal? Dispositivos IoT descontrolados? As ameaças de hoje requerem um fluxo de trabalho de gestão de ameaças inteligente que integre detecção, resposta, investigação em tempo real e remediação abrangente.Para realizar este nível avançado de gestão de ataque de insider, o ClearPass fornece ao IntroSpect informações de perfil sobre cada dispositivo que faz logon na rede, incluindo a função do usuário ou dispositivo, tempo de conexão, local e o que a entidade está autorizada a acessar.

Com visibilidade detalhada, o IntroSpect pode então fornecer informação básica e analisar o tráfego de um dispositivo com base nas características esperadas.

Por exemplo, se o IntroSpect detectar que um dispositivo associado a um "Convidado" exibe comportamentos anormais, o IntroSpect pode acionar uma resposta de segurança baseada em políticas que o ClearPass pode aplicar, o que pode incluir a quarentena de uma entidade ou a inclusão do dispositivo na lista negra.

Como parte do fluxo de trabalho da investigação do IntroSpect, um analista pode facilmente ver mudanças na quantidade de dados transferidos, endereços visitados, ciclo de trabalho e tempo ou local para o qual uma anomalia é reconhecida. A capacidade de aproveitar o perfil, as regras de acesso granular e os níveis diferenciados de execução asseguram a correção adequada de uma entidade comprometida.

aruba
a Hewlett Packard Enterprise company
www.arubanetworks.com/br

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM