RESUMO EXECUTIVO

ARUBA 360 SECURE FABRIC

360º de proteção cibernética ativa baseada em análise e acesso seguro

Há pouco tempo, as equipes de segurança empresarial podiam identificar o perímetro que estavam protegendo e trabalhar com operações de TI para obter o controle total dos recursos que seus funcionários podiam acessar e usar, de redes a sistemas, aplicativos e dados. Hoje, não há escassez de interrupções tecnológicas - móveis, BYOD, virtualização, nuvem, big data e a IoT agora se apoderaram da empresa e tornou a abordagem de segurança baseada no perímetro insuficiente. O problema é agravado por uma era de desagregação da TI e ataques altamente organizados e direcionados. Garantir a segurança da organização não é apenas uma missão crítica, agora tornou-se exponencialmente mais difícil. Claramente, é necessária uma abordagem moderna para lidar com o cenário de ameaças em rápida mudança de hoje.

De acordo com a Gartner, a Análise de Comportamento dos Usuários e Entidades (User and Entity Behavior Analytics - UEBA) é uma categoria inovadora de tecnologia de segurança para identificar e mitigar ameaças avançadas. "Pelo menos nos últimos dois anos, a Gartner testemunhou o aparecimento de muitos novos fornecedores com análises avançadas em vários segmentos do mercado de segurança. Uma área que tem incentivado muita inovação é a UEBA, que permite análises de segurança de amplo alcance, bem como informações de segurança e gerenciamento de eventos (Security Information and Event Management - SIEM) que possibilitam o monitoramento de segurança de amplo alcance. A UEBA fornece análises em torno do comportamento do usuário, mas também em torno de outras entidades, como endpoints, redes e aplicativos. A correlação das análises em várias entidades torna os resultados da análise mais precisos e a detecção de ameaças mais eficaz, assim como acontece com o SIEM."[1]

O ARUBA 360 SECURE FABRIC

A maioria das soluções de segurança no mercado hoje são uma miríade das tecnologias de segurança projetadas para ambientes estáticos, fechados, baseados em perímetros de ontem. Essas tecnologias de segurança diferentes podem abordar apenas um dos muitos tipos de ameaças e vulnerabilidades atuais. São necessárias operações de TI e de segurança para criar uma solução de segurança de patchwork que combina firewalls com o IPS para o controle de acesso ao anti-malware para análise.

Impulsionada pelas demandas de mobilidade empresarial, BYOD, nuvem e IoT, a Aruba viu a necessidade de uma abordagem de design diferente para conectar e proteger as redes. A Aruba agora está mudando o paradigma com o Aruba 360 Secure Fabric, uma estrutura de segurança corporativa que dá segurança e oferece às equipes de TI uma maneira integrada de ganhar visibilidade e controle. Permite que você detecte ataques de gestação com inteligência de aprendizado automático ou de máquina e responda proativamente a esses ataques cibernéticos avançados em qualquer infra-estrutura - com a escala da empresa para proteger milhões de usuários e dispositivos e garantir grandes quantidades de dados distribuídos.

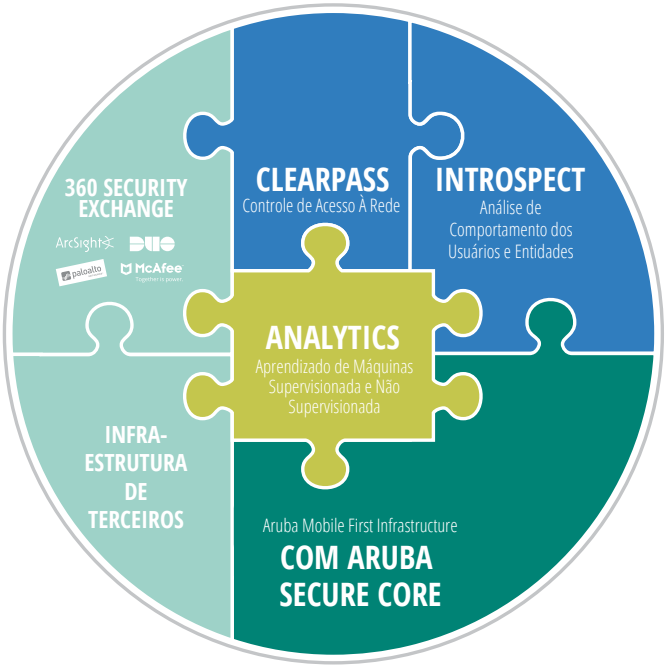


Figura 1: O Aruba 360 Secure Fabric fornece uma estrutura de segurança integrada para equipes de TI e segurança a fim de obter visibilidade e controle de sua rede, com foco na análise.

Existem 3 elementos para este Fabric:

- O software de segurança Aruba: controle proativo de acesso à rede, gestão de políticas e a UEBA líder na indústria para qualquer rede
- Aruba Secure Core: infraestrutura de rede pronta para análise com segurança incorporada
- Um ecossistema de segurança líder

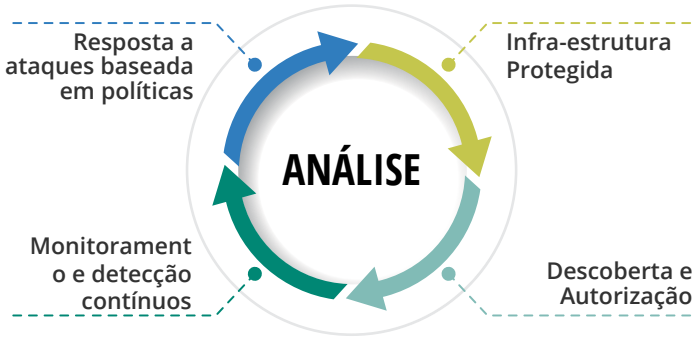
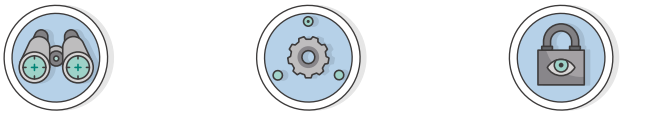


Figura 2: A nova necessidade imperiosa para a segurança

A Aruba baseou-se no seu início dos principais recursos de segurança incorporados na base de todos os access points Wi-Fi (APs), switches, roteadores e controladores, ao integrar a detecção de ataques fundamentada no aprendizado de máquina IntroSpect com sistemas de controle de acesso como o Aruba ClearPass numa plataforma aberta, multi-fornecedora. Com o Aruba 360 Secure Fabric, as equipes de segurança agora podem desenvolver um caminho contínuo do acesso e da descoberta de usuários e dispositivos, além da detecção e resposta a ataques orientados à análise, com base em políticas definidas pela organização.

UMA MANEIRA INTEGRAL DE GANHAR VISIBILIDADE E CONTROLE DE SUAS REDES, USUÁRIOS E DISPOSITIVOS

A desagregação de TI significa que as organizações não só precisam de uma base de rede segura, mas também a visibilidade e o controle dos usuários e dos dispositivos conectados à rede. O ClearPass permite que a empresa cubra todo o conjunto de casos de uso com controle de acesso com e sem fio de convidado, integração de BYOD e remediação baseada em políticas e resposta a ataques.



VISIBILIDADE
Saiba o que está na sua rede

CONTROL
Autentique e autorize todas as "coisas"

RESPOSTA
Coordenação de ferramentas de segurança através do ClearPass Exchange

Figura 3: o ClearPass fornece não só visibilidade, mas também controle estendido para dispositivos e usuários conectados a sua rede.

Avançando um pouco mais, em fevereiro de 2017, a Aruba adicionou as funções de detecção de ataque baseadas no aprendizado automático com a aquisição de Niara. Esta adição aproveita a visibilidade do ClearPass no acesso à rede, bem como a capacidade de tomar uma série de ações manuais ou automatizadas em resposta a um ataque.

O Análise de Comportamento dos Usuários e Entidades do IntroSpect da Aruba (UEBA) detecta ataques ao identificar pequenas mudanças de comportamento que, muitas vezes, são sinal de façanhas que evadiram o monitoramento e a análise de segurança tradicionais. Os ataques de hoje podem ser compostos por muitas ações menores que ocorrem por longos períodos de tempo. Esses tipos de ataques também são notoriamente difíceis de detectar porque podem envolver usuários e hosts comprometidos onde criminosos virtuais evadiram as defesas perimetrais usando credenciais legítimas para acessar recursos corporativos. Os phishing scams, a engenharia social e os malware são apenas algumas das técnicas mais conhecidas pelas quais esses criminosos adquirem credenciais corporativas dos empregados. O IntroSpect usa inteligência de aprendizado de máquina e automatiza a detecção desses ataques, dando segurança e visibilidade inicial das operações de rede. Os modelos de aprendizado de máquinas supervisionados e não supervisionados processam grandes quantidades de dados, a fim de estabelecer uma linha de referência da atividade de TI típica de um usuário, dispositivo ou sistema. Os desvios dessas linhas de referência são muitas vezes a primeira indicação de que um ataque está em curso.

Ambos o ClearPass e o Introspect servem como solução de software de segurança da Aruba e podem ser aplicados individualmente ou em conjunto a qualquer rede em ambientes de campus, empresa distribuída, nuvem e borda de IoT. Ao sobrepor o Secure Core, o ClearPass e o Introspect da Aruba é oferecida uma proteção incomparável baseada em análise contra a paisagem de ameaças em constante mudança de hoje.

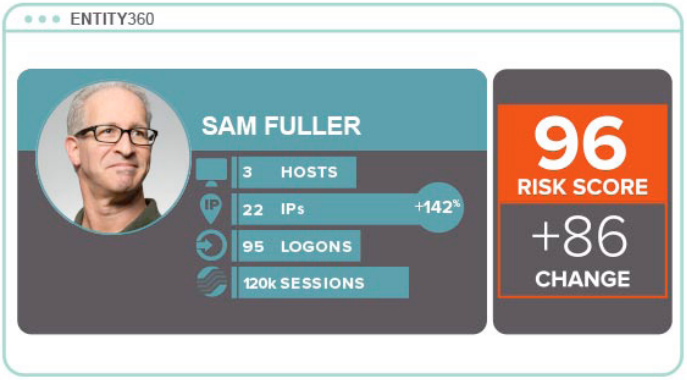


Figura 4: Detecta ameaças antes que elas possam causar danos com o IntroSpect User e Entity Behavior Analytics.

ARUBA SECURE CORE: INFRA-ESTRUTURA SEGURA, CONFIÁVEL DA REDE

Por mais de 15 anos, a Aruba tem estado na vanguarda da entrega de redes com e sem fio de alto desempenho, altamente confiáveis e seguras - começando com os access points e controladores sem fio, expandindo-se ao acesso e à comutação de núcleo. Como fornecedor de segurança, a Aruba tem introduzido consistentemente inovações nas áreas de criptografia, endurecimento físico, acesso remoto e firewalls incorporados para garantir que o tráfego do usuário, do sistema e do dispositivo possa ser confiável. Os Diretores de Segurança da Informação (CISOs) em todo o mundo passaram a confiar na "vantagem" de segurança que a infraestrutura segura da Aruba fornece.

ARUBA 360 SECURITY EXCHANGE: PROTEÇÃO ABERTA MULTIFORNECEDORA CONTRA LOOP FECHADO

Uma vantagem fundamental do Aruba 360 Secure Fabric é uma integração aberta de multi-fornecedores das soluções de segurança da Aruba com mais de 100 parceiros no 360 Security Exchange Program. Os clientes podem aproveitar seus investimentos em segurança já existentes integrando perfeitamente os produtos originários do Exchange com soluções Aruba. Ao contrário de outros fornecedores de infra-estrutura que limitam seus clientes a atualizações caras e uma única fonte de produtos, o Aruba 360 Secure Fabric fornece os melhores elementos de uma solução unificada com a flexibilidade de uma arquitetura aberta.

RESUMO

Ao trabalhar em conjunto com um ecossistema aberto multi-fornecedor de parceiros, o Aruba Secure Core na Aruba Mobile First Infrastructure, combinado com a visibilidade e controle do ClearPass e a detecção de ataques avançados do IntroSpect, o Aruba 360 Secure Fabric oferece 360º de detecção de ataques com análise e resposta da borda ao núcleo para a nuvem - isso é o que significa ser "Aruba Secure".

[1] Gartner Foundational Research Report, Refreshed 9 August 2017, The Fast Evolving State of Security Analytics

a Hewlett Packard Enterprise company

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

www.arubanetworks.com/br