aruba
a Hewlett Packard Enterprise company

VISÃO GERAL DA SOLUÇÃO

ARUBA CLEARPASS POLICY MANAGER

Visibilidade e segurança de acesso para conexão com e sem fio

Lembra-se de quando a TI era o guardião e dominava com uma combinação de políticas rígidas e um ecossistema totalmente contido? Essa realidade já não existe mais. Hoje, a TI e os dispositivos de propriedade dos usuários estão conectados dentro e fora da segurança de perímetro.

Laptops, smartphones, tablets e dispositivos de Internet das Coisas (IoT) estão tomando conta do local de trabalho, e identificar o que está na rede é o primeiro passo para proteger seus dados. A aplicação de política automatizada assegura que apenas os usuários e os dispositivos desejados possam se conectar, e a proteção em tempo real é necessária para garantir o atendimento dos requisitos de auditoria e conformidade internos e externos.

E se as expectativas estiverem corretas, o uso de dispositivos de IoT em redes com e sem fio está mudando o foco da TI. A maioria das organizações protegeu seus dispositivos e redes sem fio, mas negligenciou as portas com fio em salas de conferência, atrás de telefones por IP e em áreas de impressoras. E como os dispositivos de IoT podem não ter atributos de segurança e exigir acesso de recursos de administração externos, o acesso com fio é o novo risco.

Como a TI luta para manter o controle, eles precisam do conjunto certo de ferramentas para rapidamente programar a infraestrutura subjacente e controlar o acesso à rede para qualquer dispositivo móvel e de IoT – conhecido e desconhecido. A solução de segurança de acesso de hoje deve fornecer definição de perfil, aplicação de política, acesso de convidado, integração de BYOD e muito mais para oferecer proteção avançada contra ameaças, com descarga de TI e uma experiência avançada ao usuário.

MOBILIDADE E IoT ESTÃO MUDANDO O MODO COMO PENSAMOS EM NAC

Os limites do domínio da TI agora vão além das quatro paredes de uma empresa. E o objetivo das organizações é oferecer conectividade a qualquer hora, em qualquer lugar sem comprometer a segurança. Como a TI mantém a visibilidade e o controle sem afetar os negócios e a experiência do usuário? Tudo começa com um plano em três etapas.

1. **Identifique** quais dispositivos estão sendo usados, quantos, de onde estão se conectando e quais sistemas operacionais são suportados: isso fornece a base. E o insight contínuo das alterações e de quais dispositivos entram e saem lhe oferece a visibilidade necessária com o tempo.
2. **Aplique** políticas precisas que oferecem o acesso correto ao usuário e ao dispositivo, independentemente do usuário, do tipo de dispositivo ou do local; isso

proporciona uma experiência de usuário esperada. As organizações devem se adaptar aos dispositivos em evolução de hoje e seu uso – seja o dispositivo um smartphone ou uma câmera de vigilância.

3. **Proteja** os recursos por meio de controles dinâmicos de política e correção de ameaças reais que se estendem a sistemas de terceiros. Essa é a última peça do quebra-cabeça. Estar preparado para comportamento de rede incomum às 3 da manhã requer uma abordagem unificada que bloqueie o tráfego e altere o status da conexão de um dispositivo.

As organizações devem se planejar para desafios existentes e imprevistos. Não é realista depender da TI e da equipe de help desk para realizar intervenção manualmente sempre que um usuário decidir trabalhar remotamente ou comprar um novo smartphone. O NAC não é mais apenas para realizar avaliações em dispositivos conhecidos antes do acesso.

THE POWER OF CLEARPASS EXCHANGE

UM LUGAR PARA VER E GERENCIAR TUDO

A política ClearPass e a solução AAA oferecem criação de perfil de dispositivo integrada, uma interface administrativa baseada na web e geração de relatórios abrangente com alertas em tempo real. Todos os dados contextuais são utilizados para garantir que os usuários e os dispositivos recebam privilégios de acesso apropriados, independentemente do método de acesso ou da propriedade do dispositivo.

O mecanismo de criação de perfil integrado coleta dados em tempo real, o que inclui categorias de dispositivo, fornecedores, versões de SO etc. Não existe mais motivo para adivinhar quantos dispositivos estão conectados em redes com e sem fio. A visibilidade granular fornece os dados necessários para aprovar auditorias e determinar de onde os riscos de desempenho e segurança poderiam vir.

O ClearPass Universal Profiler independente oferece a mesma visibilidade de definição de perfil a essas organizações, que podem não estar prontas para aplicação total de política. Ou, para áreas remotas em que o ClearPass não pode ser implantado inicialmente.

Uma aplicação de política baseada em modelo permite que a TI crie políticas orientadas com e sem fio que aproveitam as funções de usuário, os tipos de dispositivo, os dados de MDM/EMM, o status do certificado, o local, o dia da semana etc. As políticas podem aplicar regras facilmente para funcionários, alunos, médicos, convidados, executivos e cada um dos tipos de dispositivos que eles decidem trazer.

ClearPass OnConnect é um recurso integrado que permite às organizações bloquear aquelas milhares de portas com fio que usam aplicação não AAA. Nenhuma configuração de dispositivo é necessária, e só é preciso uma entrada de linha de comando no switch. Os métodos AAA/802.1X padrão também são suportados para conexões com e sem fio.

Isso permite uma aplicação de política consistente e uma abordagem de ponta a ponta que as soluções de AAA, NAC e de política em silos não conseguem oferecer. A capacidade de utilizar vários armazenamentos de identidade em um serviço de política, incluindo Microsoft Active Directory, diretórios compatíveis com LDAP, bancos de dados SQL compatíveis com ODBC, servidores de token e bancos de dados internos, destaca o ClearPass das soluções legadas.

PROVISIONAMENTO DE DISPOSITIVO SEM ENVOLVIMENTO DA TI

O gerenciamento da integração de dispositivos pessoais para implantações de BYOD pode sobrecarregar os recursos de TI e de help desk e gerar preocupações de segurança.

O ClearPass Onboard permite que os usuários configurem dispositivos para uso em redes seguras por conta própria. Os certificados específicos de dispositivo até mesmo eliminam a necessidade de digitar credenciais de login repetidamente durante o dia todo. Essa conveniência, por si só, é uma vitória. A segurança adicional obtida com o uso de certificados é um bônus.

A equipe de TI define quem pode integrar dispositivos, os tipos de dispositivos que eles podem integrar e quantos dispositivos por pessoa. Uma autoridade de certificado integrada permite à TI oferecer suporte a dispositivos pessoais mais rapidamente como uma PKI interna, e os recursos de TI subsequentes não são necessários.

Acesso de convidado simples e rápido

BYOD não se trata apenas de dispositivos de funcionários. Diz respeito a qualquer visitante cujo dispositivo necessite de acesso de rede, com ou sem fio. A TI requer um modelo simples que encaminhe o dispositivo para um portal de sua identidade, automatize o provisionamento de credenciais de acesso e também forneça recursos de segurança que mantêm o tráfego empresarial separado.

O ClearPass Guest torna mais fácil e eficiente para funcionários, recepcionistas, coordenadores de eventos e outras equipes que não são de TI criar contas temporárias de acesso a redes para qualquer número de convidados por dia. O armazenamento em cache de MAC também assegura que os convidados possam se conectar facilmente durante o dia todo sem digitar credenciais repetidamente no portal de convidado.

O autorregistro elimina a tarefa dos funcionários e permite que os convidados criem suas próprias credenciais. As credenciais de login são fornecidas por meio de emblemas impressos, texto SMS ou email. As credenciais podem ser armazenadas no ClearPass por períodos limitados e definidas para expirar automaticamente após um número específico de horas ou dias.

Quando a integridade do dispositivo determina o acesso

Durante o processo de autorização, pode ser necessário realizar avaliações de integridade em dispositivos específicos para garantir que eles sigam as políticas corporativas de antivírus, antispyware e firewall. A automação motiva os usuários a realizar uma verificação antivírus antes de se conectar à rede empresarial.

O ClearPass OnGuard conta com recursos integrados que realizam verificações de integridade baseadas em postura para eliminar vulnerabilidades em uma ampla gama de sistemas operacionais e versões de computador. Se clientes persistentes ou dissolúveis estiverem sendo usados, o ClearPas pode identificar centralmente os pontos de extremidade compatíveis em infraestruturas com fio, sem fio e de VPN.

Exemplos de verificações de integridade avançadas que oferecem segurança extra:

- Manuseio de aplicativos de ponta a ponta, serviços e chaves de registro.
- Determinação da permissão ou não de dispositivos de armazenamento USB ou instâncias de máquina virtual.
- Gerenciamento do uso de interfaces de rede interligadas e criptografia de disco.

Melhor aproveitamento de soluções de terceiros

O ClearPass Exchange permite automatizar a correção de ameaças de segurança ou aprimorar um serviço usando soluções de terceiros conhecidas, como firewalls, MDM/EMM, MFA, registro de visitantes e ferramentas de SIEM. O aproveitamento da inteligência de contexto que o ClearPass tem permite que as organizações garantam que a segurança e a visibilidade sejam fornecidas em um nível de dispositivo, acesso de rede e inspeção de tráfego e de proteção contra ameaças.

O uso de uma API de linguagem comum (REST), um repositório integrado e de mensagens de syslog chamado ClearPass Extensions, os fluxos de trabalho automatizados e as decisões ajudam a simplificar as tarefas e proteger a empresa: não há mais linguagens de script complexas e configuração manual tediosa. E para integração mais rápida, o Extensions permite que os parceiros façam o upload de uma extensão, para entrega em tempo real de novos serviços a clientes conjuntos.

Com o ClearPass Exchange, as redes podem executar ações automaticamente:

- Os dados de MDM/EMM, como status de desbloqueio de um dispositivo, podem determinar se ele pode se conectar a uma rede.
- Os firewalls podem aplicar políticas com precisão com base em usuário, grupo e atributos específicos de dispositivo e aproveitar o ClearPass para corrigir um dispositivo que apresenta comportamento ruim.
- As ferramentas de SIEM podem ser configuradas para armazenar dados de autenticação de todos os dispositivos conectados.
- Os usuários podem ser solicitados a usar autenticação multifator para provar que são eles mesmos que estão se conectando às redes e aos recursos.

Os eventos de rede podem também solicitar que firewalls, SIEM e outras ferramentas instruam o ClearPass a agir em um dispositivo por meio do disparo de ações de uma forma bidirecional. Por exemplo, se um usuário falhar na autenticação de rede várias vezes, o ClearPass poderá disparar uma mensagem de notificação diretamente para o dispositivo ou impedi-lo de acessar a rede.

Acesse os aplicativos de trabalho com segurança de qualquer lugar

O login nos aplicativos de trabalho durante todo o dia precisa ser rápido e sem complicações. Por esse motivo, o ClearPass suporta SSO e o recurso ClearPass Auto Sign-On. Em vez de um login único, que requer que todos façam login uma vez nos aplicativos, o Auto Sign-On usa um login de rede válido para automaticamente oferecer aos usuários acesso aos aplicativos móveis empresariais. Os usuários precisam apenas de seu login de rede ou de um certificado válido nos dispositivos.

O ClearPass pode também ser usado como seu provedor de identidade (IdP) ou provedor de serviços (SP) em que o login único é usado.

Serviços Bonjour, DLNA e UPnP

Projetores, TVs, impressoras e outros dispositivos de mídia que usam DLNA/UPnP ou Apple AirPlay e AirPrint podem ser compartilhados entre usuários em sua infraestrutura Aruba Wi-Fi. O ClearPass simplifica a descoberta desses dispositivos e o compartilhamento entre eles.

Por exemplo, o professor que quer fazer uma apresentação de um tablet verá apenas um monitor na sala de aula. Ele não verá dispositivos no outro lado do campus. Ele pode também usar o portal para escolher quem mais pode usar o monitor. Isso impede que os alunos assumam o comando do monitor.

Outro exemplo está no setor de saúde: os médicos podem projetar imagens digitais de PACS facilmente de seus iPads em uma tela maior em qualquer lugar do hospital. A colaboração do paciente ficou mais simples.

BASE ADAPTÁVEL PARA SEGURANÇA E SERVIÇOS

O oferecimento de uma experiência sem igual aos usuários móveis de hoje e a adoção rápida de tecnologias de IoT criaram inúmeros desafios novos de TI. É necessário ter planejamento, as ferramentas certas e uma base sólida para garantir o acesso a qualquer hora, em qualquer lugar em conexões com e sem fio.

O ClearPass vence esses desafios fornecendo identidade de dispositivo, controle de política, automação de fluxo de trabalho e proteção contra ameaças automatizada a partir de uma solução coesa única. Com a captura e a correlação de dados contextuais em tempo real, o ClearPass lhe permite definir políticas que funcionam em qualquer ambiente: escritório, campus ou estádio.

Os aprimoramentos mais recentes do ClearPass também lidam com desafios de segurança de rede emergentes que envolvem a adoção de IoT, autenticação mais forte de dispositivo móvel e aplicativo e visibilidade mais detalhada dos incidentes de segurança. A proteção contra ameaças automatizada e os recursos de serviço inteligentes asseguram que cada dispositivo receba com precisão privilégios de acesso à rede com interação de TI manual mínima.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089 USA
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com