VMWARE WORKSPACE ONE TRUST NETWORK

Segurança para o espaço de trabalho digital em evolução

VISÃO GERAL

O VMware Workspace ONE™ Trust Network™ oferece às organizações uma abordagem abrangente e moderna à segurança corporativa para proteger funcionários, aplicativos, endpoints e redes. Com os recursos para proteger, detectar e corrigir as ameaças atuais, o Workspace ONE Trust Network melhora os recursos de segurança inerentes à plataforma Workspace ONE orientada por inteligência com um ecossistema avançado de soluções de parceiros, integradas para fornecer monitoramento contínuo e resposta rápida para redução dos riscos no espaço de trabalho digital.

PRINCIPAIS BENEFÍCIOS

O Workspace ONE Trust Network simplifica a segurança e o gerenciamento com estrutura de confiança e verificação. Com o Workspace ONE Trust Network, a TI pode:

- Eliminar os silos de soluções de segurança com uma estrutura baseada em ações que fornece uma visualização agregada e reduz a complexidade no espaço de trabalho digital.
- Combinar de modo exclusivo o gerenciamento e a segurança de acesso, dispositivos e aplicativos com informações e automação para reduzir os riscos em um ecossistema de computação para o usuário final.
- Aproveitar um ecossistema de parceiros aberto e confiável e continuar usando os investimentos existentes, o que ajuda a reduzir os custos.

A segurança é a maior barreira para uma estratégia moderna de espaço de trabalho digital

Um espaço de trabalho digital pode aumentar a produtividade dos funcionários 5 vezes[1], oferecendo a eles acesso simples e seguro aos aplicativos e aos dados a partir do dispositivo que preferirem. À medida que as organizações continuam avançando na transformação digital, o ecossistema de funcionários, aplicativos, endpoint e redes do espaço de trabalho digital continua aumentando e evoluindo além do perímetro tradicional com tendências comuns como a adoção de BYOD e a consumerização da TI. E, à medida que o perímetro tradicional é eliminado, começam a surgir ameaças cibernéticas avançadas, como os ataques de dia zero, Man-in-the-Middle (MiTM), phishing, bots e ransomware.

A segurança é a principal prioridade para o investimento em mobilidade e espaço de trabalho digital[2], embora as ferramentas de segurança existentes forneçam à TI uma visibilidade limitada, concentrando-se apenas nos silos de segurança que fornecem funcionalidade legada. Isso resulta em uma abordagem reparadora que afeta negativamente as organizações com custos altos devido à complexidade e às tarefas manuais associadas para proteger o espaço de trabalho digital. Consequentemente, a segurança tornou-se a maior barreira para uma estratégia moderna de espaço de trabalho digital.

Segurança abrangente e preditiva na organização sem perímetro

Um novo conjunto de requisitos para atender às necessidades de segurança sem comprometer a experiência do usuário deve ser cumprido:

1. Para obter uma visão agregada, as organizações precisam usar uma estrutura para estabelecer a confiança entre os componentes que protegem o ecossistema.
2. E para reduzir continuamente o risco, as organizações devem ser capazes de obter informações do ambiente para tomar decisões automatizadas e preditivas, direcionadas à proteção do espaço de trabalho digital.

O Workspace ONE Trust Network oferece às organizações uma abordagem abrangente e moderna à segurança corporativa para proteger funcionários, aplicativos, endpoints e redes. O Workspace ONE Trust Network oferece um conjunto de recursos para proteger, detectar e corrigir as ameaças no espaço de trabalho digital em evolução, com base em uma estrutura de confiança e em verificação. Quando a confiança é estabelecida em um espaço de trabalho digital, o resultado é um sistema interconectado com o mínimo de privilégios que capacita os funcionários mantendo a segurança onde quer que estejam. Para gerenciar os riscos relacionados às ameaças cibernéticas atuais, o Workspace ONE Trust Network combina informações da plataforma Workspace ONE orientada por inteligência a soluções de parceiros de segurança confiáveis para fornecer segurança preditiva e automatizada no espaço de trabalho digital.

1 Fonte: https://www.vmware.com/radius/impact-digital-workforce/

2 de dezembro de 2017 CCS Insights Mobile Technology Buyer Survey

Proteção, detecção e correção

Não se trata de "se" uma organização encontrará um ataque cibernético, mas sim de "quando" ela encontrará. Com essas expectativas, as equipes de segurança e operações de TI podem gerenciar o risco à segurança cibernética, simplificando o mapeamento de funções de segurança com uma estrutura de segurança cibernética da NIST, para os recursos fornecidos pelo Workspace ONE Trust Network:

- Os recursos de segurança protegem primeiro o espaço de trabalho digital; isso inclui a prevenção contra malware usando a aprendizagem de máquina, a prevenção contra extração de dados dos aplicativos corporativos com base em nuvem e a microssegmentação das redes para proteger contra ameaças avançadas persistentes (APTs, Advanced Persistent Threats).
- Quando as ameaças entram no espaço de trabalho digital, elas podem ser detectadas usando o monitoramento contínuo e adaptável, o que permite às equipes de segurança e operações de TI detectarem as ameaças em aplicativos e endpoints móveis e de desktop.
- Depois que as ameaças forem detectadas, o Workspace ONE Trust Network pode automatizar a correção, aproveitando um mecanismo avançado de decisão. Quando um ataque for detectado com base em anomalias comportamentais, uma política automatizada pode ser iniciada para bloquear o acesso aos dados corporativos.

Unificação da segurança e do gerenciamento de acesso, dispositivos e aplicativos com técnicas de análise

O Workspace ONE Trust Network combina os recursos inerentes de segurança da plataforma Workspace ONE orientada por inteligência, que incluem a segurança e o gerenciamento de acesso, dispositivos e aplicativos com técnicas de análise para interligar de uma forma única os silos de soluções de segurança e gerenciamento. O serviço de inteligência do Workspace ONE potencializa as técnicas de análise na plataforma Workspace ONE e oferece agregação, correlação e recomendações de dados do espaço de trabalho para fornecer informações e automação integradas. Ao integrar os recursos do Workspace ONE Trust Network ao serviço de inteligência do Workspace ONE, as organizações podem oferecer monitoramento contínuo aos riscos de segurança e respostas rápidas de atenuação no mundo sem perímetro de hoje.

Um mecanismo de decisão ajuda a correlacionar informações, como dispositivos corporativos fora da rede e comportamento dos usuários, para detectar ameaças e automatizar a correção por meio de políticas de acesso. Informações integradas aos dados de ameaças e ao status detalhado de conformidade do dispositivo proporcionam um modo fácil de identificar e reduzir os problemas de segurança em tempo real, aprimorando a higiene de segurança para o espaço de trabalho digital. Com o mecanismo de decisão, a TI pode criar regras para automatizar e otimizar tarefas comuns, como correção de endpoints Windows 10 vulneráveis com um patch crítico e definição de controles de acesso condicional aos aplicativos e serviços no nível individual ou de grupo.

Utilização do ecossistema avançado de soluções de parceiros confiáveis

Para permitir a segurança abrangente no espaço de trabalho digital, o estabelecimento da confiança deve ser feito entre os componentes que protegem um espaço de trabalho digital em crescimento e evolução. O Workspace ONE Trust Network fornece uma estrutura de confiança, ao aproveitar as vantagens das APIs baseadas na plataforma Workspace ONE. Essas APIs permitem que um ecossistema avançado de soluções de segurança se comunique com o Workspace ONE e, por fim, forneça aos administradores a visualização agregada que eles desejam e precisam para simplificar a segurança e o gerenciamento. Ao conectar silos de soluções de segurança, os clientes podem aproveitar os investimentos existentes para aprimorar significativamente o monitoramento contínuo e a análise de riscos para obter melhores tempos de resposta. Isso resulta em uma estratégia de segurança preditiva, baseada em tendências e padrões, que pode ser dimensionada com a implantação.

SAIBA MAIS

Para saber mais sobre o Workspace ONE Trust Network, visite: www.vmware.com/br/products/workspace-one/security

Avalie um laboratório prático gratuito: https://www.vmware.com/go/workspace-hol

PARA OBTER MAIS INFORMAÇÕES OU ADQUIRIR OS PRODUTOS VMWARE

LIGUE PARA

877-4-VMWARE (fora da América do Norte, ligue para +1-650-427-5000),

ACESSE O SITE

http://www.vmware.com/br/products ou pesquise um revendedor autorizado on-line.

Principais recursos

As organizações podem aproveitar as vantagens desses recursos de segurança críticos que o Workspace ONE Trust Network fornece para proteção, detecção e correção do cenário em evolução de ameaças cibernéticas.

RECURSO	DESCRIÇÃO
Uma plataforma básica de espaço de trabalho digital que conecta soluções de segurança	Simplifique a segurança e o gerenciamento com uma estrutura de confiança que aproveita APIs para permitir a comunicação entre um ecossistema de segurança aberto e o Workspace ONE.
Gerenciamento de acesso que simplifica seus negócios	Capacite a TI para oferecer aprovisionamento de aplicativos, um catálogo de autoatendimento, autenticação de vários fatores e um logon único (SSO) para todos os aplicativos.
Experiência de usuário e segurança otimizadas com políticas contextuais	Controle a autenticação com políticas de acesso condicional com base em estado de conformidade de dispositivo, força de autenticação de usuário, sensibilidade de dados, local do usuário, entre outros fatores.
Políticas de DLP ajudam na prevenção contra perda de dados	Ative a criptografia no nível de dispositivo, as políticas de criptografia de dados e segurança de hardware. Configure políticas que incluem listas negras, pareamento de dispositivos, segurança de Wi-Fi e aplicação de TLS. Monitore as ameaças de malware, aplicativos mal-intencionados, ataques na memória ou dispositivos desprotegidos e corrija automaticamente com bloqueio remoto, limpeza de dispositivos, bloqueio de acesso ou controles personalizáveis de quarentena de dispositivos.
Proteção dos aplicativos sem sacrificar a experiência do usuário	Utilize os controles de segurança nos aplicativos de produtividade seguros da VMware: VMware Boxer™, Browser™ e Content Locker™. Detecte ameaças e automatize a remediação para todos os outros aplicativos e serviços de computação em nuvem.
Criptografia de dados em repouso e dados em trânsito	Autentique e criptografe o tráfego dos aplicativos em dispositivos ao data center com o VMware Tunnel. Proteja os dados de aplicativos em repouso e em trânsito com criptografia AES de 256 bits.
A microssegmentação automatiza a segurança entre as redes	Minimize a superfície de ataque no data center usando recursos de microssegmentação com o VMware NSX®, automatizando a segurança em toda a rede.
Automação e informações integradas orientam a segurança preditiva	Identifique e reduza os problemas de segurança em tempo real com informações integradas de dados de ameaça e status detalhado de conformidade de dispositivo fornecidos pelo Workspace ONE Intelligence.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel.: 877-486-9273 Fax: 650-427-5001 www.vmware.com
Rua Surubim, 504 4º andar CEP: 04571-050 Cidade Monções - São Paulo - SP Tel.: (11) 5509-7200 www.vmware.com/br
