WHITE PAPER – **MARÇO DE 2018**

UMA ABORDAGEM ABRANGENTE À SEGURANÇA NO ESPAÇO DE TRABALHO DIGITAL

vmware®

Índice

As empresas que capacitam seus funcionários com os aplicativos que eles desejam e precisam e os disponibilizam a qualquer hora, em qualquer lugar e de qualquer dispositivo podem se beneficiar de decisões mensuráveis e de ganhos em produtividade e eficiência no nível individual e organizacional.[1]

Introdução

Os benefícios de negócios recém-quantificados, mostrando que os funcionários com espaços de trabalho digitais são mais produtos e que suas empresas superam aquelas com espaços de trabalho digitais, aumentaram o interesse corporativo no modo de obtenção de ganhos semelhantes, sem deixar de fornecer os aplicativos em qualquer dispositivo com segurança. As empresas desejam aproveitar as vantagens citadas no estudo *Impact of the Digital Workforce* da Forbes Insights, mas nenhuma delas precisa comprometer a segurança para alcançá-las, mesmo que o perímetro de trabalho tradicional desapareça.

Eliminar o perímetro de trabalho expõe as organizações

As equipes de TI em todos os lugares continuam lutando contra o aumento das ameaças de segurança em número e gravidade. Para muitas delas, as invasões por malware já resultaram em interrupções operacionais que custaram caro. Por exemplo, o ataque cibernético WannaCry aproveitou uma vulnerabilidade no Microsoft Windows para atingir milhões, mantendo reféns os computadores em 150 países em troca de taxas de ransomware. Nos EUA, o número de incidentes de violações de dados rastreados em 2017 atingiu um novo recorde.[2]

Atualmente, a expansão de perímetros organizacionais e de trabalho fornece ótimas oportunidades inclusive para os criminosos cibernéticos. As modernas ameaças de dia zero e os ataques Man-in-the-Middle (MITM) são bons exemplos; o primeiro identificado na fase da exploração, que ocorre antes ou no primeiro dia (ou dia zero) em que o desenvolvedor toma ciência do bug; e o segundo na forma de espionagem em que o invasor intercepta uma troca de mensagens de chave pública e retransmite a mensagem substituindo a chave solicitada pela sua própria chave, controlando, monitorando e modificando a comunicação entre os dois usuários sem o conhecimento deles.[3] Técnicas avançadas de phishing que usam engenharia social e conhecimento de programação, bots e ameaças de ransomware expõem mais frequentemente as organizações, mesmo aquelas que trabalham duro para estarem sempre um passo à frente.

Combate a ameaças e proteção dos dados corporativos

É necessária uma abordagem melhor à segurança do espaço de trabalho digital em evolução, por meio de proteção, detecção e correção de ameaças com uma plataforma orientada por inteligência. Com ela, as organizações podem proteger os dados confidenciais de modo mais eficiente, à medida que as estratégias do espaço de trabalho digital se expandem e evoluem e as ameaças cibernéticas dinâmicas aumentam e se adaptam para aproveitarem as novas vulnerabilidades além dos perímetros tradicionais.

Este documento descreve uma abordagem nova, abrangente e preditiva à segurança no mundo moderno sem perímetro. Ele destaca a importância da segurança no espaço de trabalho digital em evolução e a necessidade de as empresas adotarem uma estrutura de confiança entre os componentes e o ecossistema. Ele também apresenta os oito principais recursos de proteção, detecção e correção necessários para garantir que as organizações de TI possam aproveitar informações dos dados coletados e usá-las para tomar decisões certas para prevenir as ameaças e impedir a propagação dos ataques.

1 Forbes Insights. “The High-Performance Digital Culture: Empowerment, Trust, and the New Equilibrium Between the Employee and IT”, outubro de 2017.

2 Identity Theft Resource Center. “2017 Annual Data Breach Year-End Review.”

3 Technopedia. “Zero-Day Threat,” 2018.

"A segurança é a principal prioridade dos investimentos em mobilidade e espaço de trabalho digital em 2018."

– CCS INSIGHTS

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

Atualmente, trabalha-se em qualquer lugar. Os funcionários estão acessando informações e aplicativos no escritório de casa, de cafés e até mesmo a 10 mil pés e de muitos endpoints pessoais e corporativos, por uma variedade de redes. As equipes de TI, reconhecendo as necessidades dos funcionários quanto ao momento, ao lugar e ao dispositivo para se trabalhar, estão ocupadas tentando acomodar às preferências dos funcionários, mantendo a proteção dos valiosos dados corporativos.

Mas as soluções de segurança existentes são inadequadas. As equipes de TI ainda estão tentando atender às necessidades dinâmicas dos usuários finais com tecnologias de segurança legadas, complexas e normalmente combinadas; algumas delas estão sendo implantadas para proteger itens que não precisariam de proteção. Como resultado da compra muitas soluções diferentes feita pelas equipes de TI ao longo do tempo, muitas tecnologias não se comunicam bem umas com as outras, oferecendo uma ampla variedade de possíveis formas de ataque. Embora a satisfação dos funcionários seja vital para o sucesso da organização, os líderes de TI relatam que a segurança é a principal prioridade dos investimentos em mobilidade e espaço de trabalho digital em 2018.[4]

Em uma pesquisa recente realizada pela CCS Insights, quase metade (47%) dos compradores de TI disseram que a principal prioridade de investimento foi a segurança das redes para o espaço de trabalho digital nos últimos 12 meses, seguida pela segurança dos dispositivos (42%) e pela segurança dos aplicativos (27%). Esses investimentos podem melhor a proteção dos dados e dos aplicativos, à medida que as cargas de trabalho se movem. Contudo, ter silos de soluções de segurança só aumenta a complexidade e ainda deixa espaço para erros. Por exemplo, pode ser prejudicial para as empresas impedir a possível penetração de uma invasão em um sistema com a aplicação de um firewall de rede e depois perceber que a invasão está afetando o tráfego leste-oeste em vários sistemas porque ela passou despercebida por meses. Com uma abordagem que conecta silos de soluções de segurança com base em uma estrutura de confiança, a TI não precisa priorizar a proteção, a detecção e a correção de ameaças, porque ela já faz isso continuamente.

As empresas podem combater mais efetivamente as ameaças cibernéticas em constante evolução, utilizando uma abordagem moderna à segurança do espaço de trabalho digital para sistemas e dados, em que a segurança acompanhe o espaço de trabalho digital dos funcionários. Esse modelo deve estabelecer a confiança entre os componentes que protegem o ecossistema de computação para o usuário final (funcionários, aplicativos, endpoints e redes) e permitir apenas o acesso autorizado com base em confirmação.
Abrangente e integrada, uma estrutura de confiança pode ajudar a garantir que os dados estejam protegidos e sejam usados para detecção e correção contínuas, por meio de informações e inteligência automatizada, minimizando assim os riscos.

4 CCS Insights Survey, "IT Buyer Survey", setembro de 2017.

NOVOS REQUISITOS DE SEGURANÇA

- Para proteger a organização, apresente os oito principais recursos de proteção, detecção e correção.
- Para uma visão agregada, use uma estrutura para estabelecer a confiança entre os componentes que protegem o ecossistema.
- Para reduzir continuamente o risco, obtenha informações do ambiente para tomar decisões automatizadas e preditivas, direcionadas à proteção do espaço de trabalho digital.

Três etapas para a segurança abrangente no espaço de trabalho digital em evolução

As organizações de TI precisam de uma abordagem abrangente à segurança corporativa para proteger os ambientes dos usuários finais. Esse modelo abrange a segurança de endpoints, aplicativos, funcionários e redes, interligando os silos de tecnologia de segurança. Para obter os melhores resultados, a TI deve considerar estas etapas para proteger, de modo estratégico, seu espaço de trabalho digital em evolução.

Etapa 1: Proteção, detecção e correção de ameaças

As ameaças cibernéticas evoluíram. O que pode ter começado como uma atividade de invasão despretensiosa, por exemplo, os estudantes queriam impressionar os amigos com proezas em TI, entrando e saindo imediatamente de sistemas não autorizados, hoje é visto como uma atividade realizada por hackers mal-intencionados. A proteção contra o crime cibernético requer uma resposta abrangente que impõe o bom e busca o mau, para fins de:

Proteção

As empresas, principalmente aquelas reguladas, como no setor de serviços financeiros e assistência médica, esforçam-se para atender aos requisitos de conformidade relacionados ao armazenamento de back-end de dados valiosos e altamente confidenciais. Contudo, um gerente pode acessar dados confidenciais em um dispositivo móvel durante uma reunião com o cliente e deixar acidentalmente um tablet no táxi, e os dados confidenciais que estão nele podem ser roubados. Essa perda e o comprometimento das informações do cliente quase certamente resultariam em um impacto negativo tanto para as finanças quanto para a marca.

Fornecer aos funcionários acesso contínuo e simplificado a dados e aplicativos não deve ser uma tarefa com riscos para as empresas. É por isso que os recursos da segurança corporativa começam protegendo o espaço de trabalho digital dos funcionários. A TI deve ser capaz de impedir a entrada dos malwares nos ambientes, ensinando os funcionários a não clicarem em links suspeitos e implantando políticas para prevenção contra perda de dados. Além disso, identificar as vulnerabilidades e proteger os ambientes contra a entrada e a saída de ameaças só é possível quando as organizações obtêm visibilidade completa de todos os seus ativos, de funcionários e aplicativos a dispositivos e redes. As organizações só têm tranquilidade e avançam para a fase de detecção quando conseguem implementar totalmente uma variedade de proteções, incluindo aplicação regular de patches e elaboração de políticas para controle de acesso, classificação de dados confidenciais e restrições ao uso de dispositivos. No final das contas, as iniciativas de proteção sem métodos de detecção igualmente eficientes impedem que a TI saiba se até mesmo ela está solucionando os problemas mais críticos.

Detecção

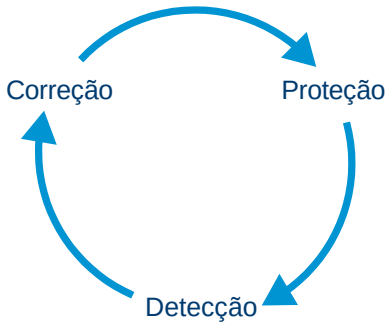
Com a eliminação de perímetros, os invasores internos e os criminosos cibernéticos cada vez mais criativos transferiram a conversa sobre segurança de “se” para “quando” o ataque ocorrerá. Sendo assim, as empresas precisam olhar além da proteção dos ativos para detectar quando ocorrerá uma invasão, desde o comprometimento de credenciais até a exploração de vulnerabilidades que ainda não foram corrigidas. As equipes de TI devem ser capazes de identificar e neutralizar uma ameaça ativa antes que ela tenha a chance de causar um dano significativo à organização. A detecção também deve ser implementada de um modo que não leve à fadiga de alertas.

Quando as ameaças entram no espaço de trabalho digital, as empresas preparadas podem detectá-las usando o monitoramento contínuo e adaptável, o que permite às equipes de segurança e operações de TI encontrarem as ameaças em aplicativos e endpoints móveis e de desktop. Com monitoramento automatizado e contínuo e alertas sobre quem está acessando quais informações, de onde, como e em qual rede, a TI mantém-se no controle. Então, usando o último estado bom conhecido, registros em log e inteligência nas técnicas de análise, a TI tem as ferramentas necessárias para reconhecer o que está diferente e usar essa informação para tomar melhores decisões sobre os próximos passos.

Correção

Os negócios digitais são dinâmicos, tornando obsoletas as soluções tradicionais de segurança que requerem correção manual para a maioria das tarefas. Hoje, as empresas exigem respostas rápidas quando estão lidando com invasões mal-intencionadas e paralisações inesperadas. Aguardar uma resposta pode levar até mesmo a uma violação ainda maior. Um estudo interno da VMware indicou que um em cada dez clientes corporativos demora pelo menos um ano para concluir os patches do Windows que afetam a maioria ou todos os seus endpoints. Isso dá aos criminosos cibernéticos tempo para criarem métodos de exploração.

As equipes de TI devem ser capazes de aproveitar as informações de seu ambiente para predefinir políticas com confiança, baseadas em causa raiz, para automatizar rapidamente a resposta e a recuperação a fim de obter melhores resultados. Por meio da automação, a TI pode optar por colocar em quarentena, suspender ou bloquear o acesso a um aplicativo ou serviço de computação em nuvem. Depois que as ameaças são detectadas, a maioria das empresas preparadas tem uma solução efetiva para automatizar a correção por meio de um mecanismo que pode detectar anomalias comportamentais e iniciar uma política automatizada para bloquear o acesso a dados confidenciais.



As empresas que optarem por uma estrutura estratégica que possa estabelecer a confiança entre os componentes no ecossistema e por soluções que protejam esses componentes terá melhores condições de proteger totalmente os ativos corporativos críticos e agilizar a detecção e a correção.

Etapa 2: Recursos para proteger, detectar e corrigir

Estes oito recursos críticos movem as empresas rumo à segurança moderna e abrangente do espaço de trabalho digital:

Abordagem de plataforma única e aberta	Uma plataforma única e aberta permite que a TI simplifique a aplicação de conformidade, por exemplo, de dispositivos e aplicativos, e reduza o risco. As empresas devem adotar uma plataforma única e aberta que combine funcionalidade de gerenciamento de dispositivos e aplicativos com inteligência e técnicas de análise para interligar de forma única os silos complexos e caros de soluções de segurança existentes. Uma plataforma com serviços de inteligência garante agregação, correlação e recomendações de dados do espaço de trabalho para fornecer informações e automação integradas. As empresas que usam essa abordagem devem ter uma visão agregada de funcionários, aplicativos, endpoints e redes. Essa abordagem de plataforma deve ser criada em uma estrutura de comunicação de APIs que ajude a estabelecer a confiança entre os componentes no ecossistema das empresas. Isso é essencial porque estabelecer a confiança em todo o espaço de trabalho digital resulta em um sistema interconectado com o mínimo de privilégios que capacita os funcionários mantendo a segurança onde quer que estejam.
Políticas de prevenção contra perda de dados	As políticas de prevenção contra perda de dados (DLP, Data Loss Prevention) ajudam as organizações a proteger os dados independentemente de onde eles residam, dentro ou fora do data center. As equipes de TI devem ser capazes de bloquear e limpar um dispositivo remotamente se ele for perdido ou roubado, localizar um dispositivo perdido e obter informações em tempo real do dispositivo, como versão do sistema operacional, última atualização, localização e outras. Utilizar uma infraestrutura de desktop virtual (VDI, Virtual Desktop Infrastructure) para centralizar desktops e aplicativos pode ajudar a reduzir a perda de dados ocasionada por perda ou roubo de dispositivos. Em todos os endpoints, as empresas também devem ser capazes de aplicar e gerenciar políticas de segurança por aplicativos com controles de DLP fornecidos por SOs nativos e de prevenir a perda de dados de conteúdo com controles de anexos de e-mail, restrições às ações recortar/copiar/colar, marca d'água dinâmica e muito mais. É um requisito controlar e restringir a capacidade do usuário de remover conteúdo corporativo usando um Software Development Kit (SDK). Um mecanismo de política e conformidade pode ajudar a automatizar a conformidade para DLP avançada. As políticas de segurança avançada incluem a definição de proteções contra dispositivos desprotegidos ou com a raiz modificada, aplicativos na lista branca e na lista negra, restrições de aplicativos “open in”, área geográfica (geofencing), configuração de rede e bloqueio de exportações e capturas de tela, bem como backup ou gravação de informações da empresa em cartões SD externos ou soluções remotas de backup em nuvem.
Políticas contextuais	Usar políticas contextuais para definir e aplicar o acesso condicional dos usuários finais pode ajudar a garantir que apenas os usuários autorizados tenham acesso a recursos e informações confidenciais. As empresas devem ser capazes de estabelecer acesso condicional, por função, departamento, nível de liberação, para que apenas usuários autorizados possam ter acesso a determinados recursos e informações. Ao combinar a aplicação de política com o gerenciamento de acesso e dispositivos, a TI pode restringir as permissões dos usuários a dados, aplicativos ou dispositivos. As mesmas tecnologias podem ser usadas também para aplicar o acesso condicional a aplicativos móveis e garantir que apenas os aplicativos em conformidade possam acessar os sistemas internos.

Proteção de aplicativos	Ao aplicar as políticas de DLP no nível dos aplicativos, as empresas dão outro passo enorme rumo a políticas de acesso mais detalhadas que protegem melhor os dados. Os espaços de trabalho digitais devem incluir políticas de DLP (descritas anteriormente no recurso dois) que ofereçam a mesma funcionalidade no nível dos aplicativos. Para ambos os dispositivos pessoais (BYO) e corporativos, o gerenciamento de aplicativos móveis facilita o aprovisionamento e controla o acesso, em vigor, agrupando os aplicativos em políticas definidas por identidade. De modo semelhante, a proteção contra perda de dados na nuvem, bem como a administração de acesso e atividades em serviços de computação em nuvem sancionados e não sancionado, é melhor contra as ameaças aos dados. Com o suporte a VPN em todo o dispositivo, VPN por aplicativo e comunicação de gateway proxy com base em SDK em todos os principais SOs, incluindo iOS, Android, macOS e Windows 10, a TI tem flexibilidade para escolher a solução certa para proteger a conectividade dos aplicativos. Além disso, os aplicativos de produtividade (por exemplo, e-mail, gerenciamento de documento etc.) devem oferecer a funcionalidade Rights Management Services (RMS), incluindo: • E-mail protegido por Information Rights Management (IRM) • S/MIME com PKI • Classificação de e-mails • Políticas de informações confidenciais e informações de identificação pessoal (PII, Personally Identifiable Information) • Criptografia de anexos • Política de acesso para impressão, visualização e roaming • Expiração de documentos • Marca d'água
Gerenciamento de acesso	As empresas fortalecem a proteção de dados verificando a identidade do usuário pelo uso de vários fatores ou de uma vez só para muitos aplicativos. Para eliminar a tarefa cada vez mais complexa de definição de políticas individuais para um crescente número de aplicativos, dispositivos e serviços de computação em nuvem, as empresas devem ser capazes de usar a identidade do usuário final para estabelecer parâmetros de segurança. O acesso com um toque, ou logon único (SSO), permite que os usuários acessem aplicativos móveis, de desktop e em nuvem, evitando o tempo gasto e as dificuldades de múltiplos logins. Pelo SSO, a identidade de um usuário pode ser verificada por muitos aplicativos de uma vez, com o fornecimento de uma chave única para abrir uma só porta do espaço de trabalho digital e acessar uma variedade de aplicativos móveis, da web, de SaaS e legados, no endpoint escolhido a partir de um catálogo de aplicativos. Pela autenticação de vários fatores (MFA, Multi-Factor Authentication), a identidade dos usuários e dos componentes do sistema pode ser verificada usando vários fatores (não apenas simples senhas) e pode ser proporcional ao risco do acesso ou da função solicitada.
Criptografia	A criptografia garante às organizações que os dados confidenciais estejam protegidos, ao impedir que destinatários não pretendidos vejam os dados à medida que são enviados e recebidos. Para os processos críticos de negócios, as práticas recomendadas incluem criptografia de todos os dados, armazenados ou transmitidos. No caso de uma violação de dados, o roubo de arquivos críticos deve resultar apenas na obtenção de dados que não podem ser lidos. A utilização de um Advanced Encryption Standard, como a criptografia AES de 256 bits, para dados em trânsito e em repouso é essencial. Como um transmissor entre as plataformas de dispositivos e os sistemas corporativos, a TI pode usar túneis ou VPNs por aplicativos para autenticar e criptografar o tráfego de aplicativos individuais em dispositivos em conformidade para sistemas de back-end com o qual estão tentando se conectar usando certificados exclusivos.

Microssegmentação	As organizações podem combater as ameaças de modo mais agressivo, reduzir o risco e melhorar sua postura de segurança com a microssegmentação em suas redes. A microssegmentação fornece uma combinação de recursos, incluindo: • Redução da superfície de ataque dentro do perímetro do data center por meio de firewall sem estado distribuído e gateways no nível dos aplicativos (ALGs, Application Level Gateway) com granularidade por carga de trabalho. • Permissão para usar os grupos de segurança para aplicação de políticas baseadas em objetos para VMs, incluindo desktops virtuais e hosts de aplicativos virtuais, criando controles granulares no nível dos aplicativos. • Segmentação e isolamento baseado na sobreposição da rede lógica que pode abranger racks e data centers independentemente do hardware de rede subjacente, permitindo uma política de segurança de vários data centers gerenciada de modo centralizado. Ambientes de TI inteiros, divididos em pequenas partes, o que os torna mais gerenciáveis para proteger ou conter danos caso uma das partes seja comprometida. Separação do tráfego leste-oeste do aplicativo para cargas de trabalho específicas no data center reduz substancialmente o vetor de ataques de malware/vírus que têm como objetivo causar sérios danos à empresa.
Técnicas de análise	As empresas melhoram sua postura de segurança com informações úteis da implantação e do uso dos aplicativos. A implantação e o uso de aplicativos agregados, a segurança dos dispositivos e os detalhes da experiência do usuário final ajudam a TI a entender melhor o desempenho e a segurança dos ambientes de espaço de trabalho digital. Um serviço de inteligência integrado com ações automatizadas agiliza o planejamento e aprimora a segurança e a experiência do usuário final. Ele também fornece monitoramento contínuo dos riscos à segurança e respostas rápida de atenuação no mundo sem perímetro de hoje. Junto com um mecanismo de decisão, um serviço de inteligência ajuda a correlacionar informações para detectar ameaças e automatizar a correção com base em políticas de acesso.

Etapa 3: Parceiros confiáveis incorporam a segurança em todo lugar

As ameaças à segurança estão aumentando não só em frequência e custo, mas também em foco e sofisticação, tornando uma plataforma com soluções de parceiros em segurança confiáveis uma abordagem ideal à proteção, detecção e correção de ameaças. As ferramentas de segurança legadas e independentes, projetadas para proteger informações valiosas, fornecem visibilidade limitada para a TI, o que normalmente leva à criação de silos de soluções no ambiente. Isso resulta em uma abordagem descoordenada que afeta negativamente as organizações, aumentando os custos devido à complexidade e às tarefas manuais associadas à tentativa de proteger o espaço de trabalho digital.

A confiança estabelecida entre os componentes que protegem um espaço de trabalho digital em crescimento e evolução ajuda a garantir uma segurança abrangente. A abordagem ideal utiliza uma estrutura de confiança que aproveita as vantagens das APIs baseadas em uma plataforma comprovada de espaço de trabalho digital. Isso porque as APIs permitem que um ecossistema avançado de soluções de segurança se comunique com a plataforma e, por fim, forneça aos administradores a visualização agregada que eles desejam e precisam para simplificar a segurança e o gerenciamento.

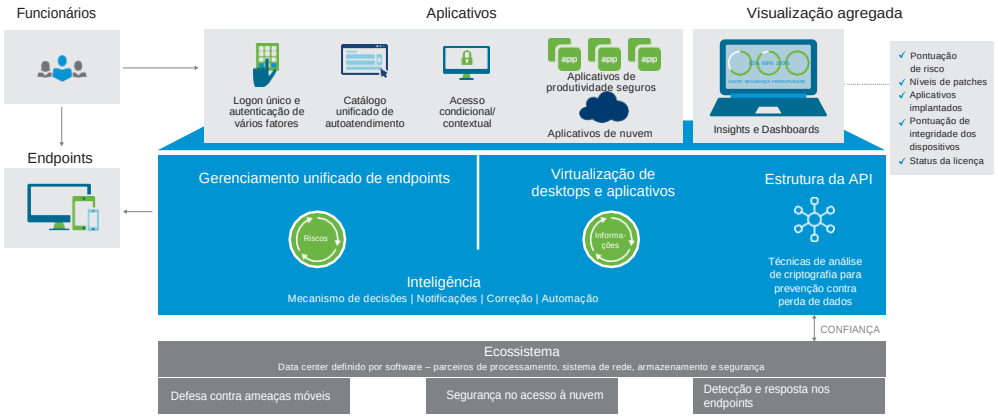
Uma estratégia robusta de espaço de trabalho digital incluirá um ecossistema aberto de soluções confiáveis de segurança, especializadas em frustrar os ataques e reduzir os riscos em áreas como:

- Visibilidade de falhas na segurança do SO
- Avaliação da integridade dos dispositivos
- Recuperação dos dispositivos
- Administração de acesso e controle
- Definição de política
- Varredura de vírus
- Aplicação de patches
- Recuperação de desastres
- Monitoramento de conformidade

Como a VMware ajuda a transformar a segurança tradicional do espaço de trabalho digital

Embora esteja acontecendo uma enorme inovação nas ferramentas de segurança cibernética, o grande número e a variedade delas no mercado reforçam a mensagem de que os líderes de TI devem aguardar uma abordagem de práticas recomendadas para a segurança do espaço de trabalho digital. Hoje, as empresas podem avançar com confiança. Com a ajuda da VMware, elas podem simplificar a segurança com uma estrutura para combater os ataques nas mais diversas situações de ameaça.

O VMware® 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 do Workspace ONE, uma plataforma de espaço de trabalho digital orientada por inteligência, a soluções de parceiros de segurança confiáveis para fornecer segurança preditiva e automatizada no espaço de trabalho digital.



Proteção, detecção e correção

A abordagem da VMware ajuda as equipes de segurança e operações de TI a gerenciar o risco à segurança cibernética, por meio da simplificação do mapeamento de funções de segurança, usando, por exemplo, uma Estrutura de segurança cibernética da NIST, para os recursos das soluções disponíveis com a abordagem do Workspace ONE Trust Network:

- Os recursos de segurança protegem primeiro o espaço de trabalho digital; isso inclui usar a aprendizagem de máquina para reconhecer o malware, aproveitar a microssegmentação das redes para proteger contra ameaças avançadas persistentes (APTs, Advanced Persistent Threats) e impedir a extração de dados dos aplicativos corporativos com base em nuvem.
- Quando as ameaças entram no espaço de trabalho digital, os recursos de segurança da VMware detectam-nas usando o monitoramento contínuo e adaptável nos endpoints e nos aplicativos móveis e de desktops.
- Essa abordagem automatiza a correção, ao usar um mecanismo de decisão poderoso. Por exemplo, se um ataque de cavalo de Tróia ou MITM for detectado com base em anomalias comportamentais, uma política automatizada é iniciada para bloquear o acesso aos dados corporativos.

Unifique o gerenciamento de acesso, dispositivos e aplicativos com as técnicas de análise

O Workspace ONE Trust Network combina a principal funcionalidade de espaço de trabalho digital do Workspace ONE — gerenciamento de acesso, dispositivos e aplicativos — a técnicas de análise fornecidas pela inteligência do Workspace ONE, para interligar de forma única os silos existentes de soluções de segurança. O serviço de inteligência do Workspace ONE oferece agregação, correlação e recomendações de dados do espaço de trabalho para fornecer informações e automação integradas. Ao complementar os recursos do Workspace ONE Trust Network com o serviço de inteligência do Workspace ONE, a VMware garante que as empresas possam 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.

Aproveite um ecossistema de soluções de parceiros confiáveis

A segurança abrangente no espaço de trabalho digital requer o estabelecimento da confiança entre os componentes que protegem um espaço de trabalho digital em crescimento e evolução. A VMware faz isso com o Workspace ONE Trust Network, que fornece uma estrutura de confiança, ao aproveitar as vantagens das APIs baseadas na plataforma Workspace ONE. Essas APIs ajudam a garantir que um ecossistema avançado de soluções de segurança possa se comunicar com o Workspace ONE e, por fim, fornecer aos administradores a visualização agregada que eles desejam e precisam para simplificar a segurança e o gerenciamento.

Ao conectar os silos de soluções de segurança, os clientes da VMware podem aproveitar os investimentos existentes para aprimorar significativamente o monitoramento contínuo e as análises de risco para agilizar o tempo de resposta, obtendo uma estratégia de segurança preditiva com base nas tendências e nos padrões que podem ser dimensionados com a implantação.

Os clientes da VMware aproveitam os investimentos existentes para aprimorar significativamente o monitoramento contínuo e as análises de risco para agilizar o tempo de resposta, obtendo uma estratégia de segurança preditiva com base nas tendências e nos padrões que podem ser dimensionados com a implantação.

É imprescindível que as empresas adotem uma nova abordagem de segurança do espaço de trabalho digital, porque agora não há mais perímetro. Uma estrutura que estabelece a confiança entre os componentes no ecossistema acomoda novos funcionários, aplicativos, dispositivos e redes. Ela serve como a base para os avanços da empresa digital que busca se modernizar, enquanto reduz os riscos, protege sua marca, reduz os custos, aumenta a agilidade e fornece experiência semelhante à do consumidor em todos os dispositivos no trabalho.

Proteção, detecção e correção: Oito recursos indispensáveis

vmware WORKSPACE ONE™ TRUST NETWORK	
RECURSO	IMPORTÂNCIA
Abordagem de plataforma única e aberta	Simplifica a aplicação de conformidade e reduz os riscos, ao eliminar os silos de tecnologia em plataformas, aplicativos e perfis de usuários.
Políticas de prevenção contra perda de dados	Protege os dados independentemente de onde eles residam com limpeza de dispositivos, bloqueio remoto e políticas de segurança por aplicativos.
Políticas contextuais	Garante que apenas os usuários autorizados tenham acesso a recursos e informações confidenciais com aplicação de políticas de acesso condicional.
Proteção de aplicativos	Protege informações controlando quem pode acessar quais recursos com políticas de DLP no nível dos aplicativos.
Gerenciamento de acesso	Fortalece a proteção de dados verificando a identidade do usuário usando vários fatores ou de uma vez só para muitos aplicativos com o logon único.
Criptografia	Protege os dados confidenciais, impedindo que os destinatários não pretendidos vejam os dados à medida que são enviados e recebidos.
Microssegmentação	Reduz a superfície de ataque de sua organização, separando as cargas de trabalho e o tráfego.
Técnicas de análise	Aprimora a postura de segurança e a conformidade com informações úteis, técnicas de análise de aplicativos e automação.

Saiba mais

Capacite os funcionários com um espaço de trabalho digital que beneficia trabalhadores e empresas. Não deixe que as preocupações da TI em relação à segurança atrapalhem a produtividade e a eficiência. A abordagem do Workspace ONE Trust Network ajuda a fornecer os recursos que sua empresa precisa para garantir que uma solução de segurança abrangente esteja em vigor para proteger os dados confidenciais, à medida que sua estratégia de espaço de trabalho digital se expande e evolui com escalonamento dinâmico de ameaças cibernéticas e adaptação para manter as novas vulnerabilidades além do perímetro tradicional. Proteja seu espaço de trabalho digital combinando o gerenciamento de acesso, dispositivos e aplicativos às técnicas de análise, aproveitando uma estrutura de confiança no ecossistema inteiro e usando as informações dos dados coletados para tomar as decisões de segurança certas.

Saiba mais sobre o Workspace ONE Trust Network em www.vmware.com/br/products/workspace-one/security.

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

Nº do item: VMW-WP-CMPRHENSIVE_APPROACH_SECURITY_WRKPLC-USLET_103