EBOOK

MAP
Manage, Automate and Prioritize

cleveris

Sumário

Por que ler este eBook?

Ataques decorrentes de vulnerabilidades de software, malware, roubo de credenciais e uma série de outros vetores de ameaça têm crescido exponencialmente, tanto em frequência quanto em sofisticação. Além disso, agravando o problema, temos o aumento do Everywhere Workplace, com a rápida mudança para trabalho remoto, bem como restrições significativas, tanto no orçamento quanto no número de pessoal de segurança qualificado disponível. Manter-se a par de toda vulnerabilidade, embora antes difícil, agora é virtualmente impossível.

Nas empresas e, em última instância, em TI, as circunstâncias exigem uma estratégia de segurança abrangente que melhore a postura de segurança, assegure o gerenciamento contínuo de riscos cibernéticos e reduza a disrupção. Isso significa ir além das soluções projetadas para um mundo dominado por PCs e datacenters, e seguir em direção a soluções construídas para o Everywhere Workplace, onde as tecnologias móveis e em nuvem são primordiais.

Este guia serve como um ponto de partida, uma estrutura de passos para ajudá-lo a avançar nessa jornada de cibersegurança. Seguindo as presentes recomendações, você poderá avançar na proteção de usuários, dispositivos, redes, aplicações e dados contra as ameaças crescentes no local de trabalho e em todos os lugares.

Introdução

O cenário atual da cibersegurança

A ameaça não está se aproximando. Ela está aqui. Como chegamos a este ponto?

A rápida ascensão do Everywhere Workplace levou a um extraordinário aumento dos pontos de exposição vulneráveis. Enquanto a mudança abrupta para um cenário de negócios digitais remoto foi inicialmente assumida como temporária, o Everywhere Workplace agora está aqui para ficar.

De acordo com Gartner,1 82% das organizações pretendem permitir o trabalho remoto em parte do tempo e 47% pretendem permitir que no futuro os funcionários trabalhem remotamente em tempo integral.

Claramente, o PC e as soluções de segurança centradas em bancos de dados, em que se confiava antes da pandemia, não são mais adequados diante da força de trabalho distribuída e do uso generalizado de dispositivos móveis pessoais e aplicações em nuvem.

Um bom exemplo são os códigos QR. Eles têm aparecido em todos os lugares, de restaurantes a consultórios médicos, e muitas vezes são escaneados com os mesmos dispositivos móveis que os funcionários usam para o trabalho. Mas a ubiquidade e a facilidade de uso dos códigos QR também os tornou um veículo ideal para ataques de phishing. Com apenas soluções de phishing por e-mail, o usuário e a empresa são vulneráveis a ataques.

Pior ainda, as ameaças de todos os tipos cresceram em sofisticação - muitas vezes visando especificamente vulnerabilidades geradas por trabalho remoto - e estão ocorrendo a um ritmo alarmante. As tentativas de phishing, por exemplo, aumentaram 85% ano após ano (com 74% das organizações sendo vítimas), e 59% das organizações relataram ter sido vitimizadas por um ransomware em 2021. Fatores como a escassez global de especialistas em segurança, combinados com orçamentos apertados em todos os lugares, e agora o simples ato de organizar e priorizar as vulnerabilidades consomem a maior parte da segurança e do tempo de TI - até 53%.2

É a tempestade perfeita: um local de trabalho em mudança, muitas coisas para garantir e recursos insuficientes para agir. Ficar quieto não é uma opção. As empresas que não agirem provavelmente sofrerão mais desproteção de dados, incluindo ransomware, phishing, hackers e vulnerabilidades causadas por funcionários internos (intencionais ou não intencionais), e potencialmente enfrentarão mandatos de conformidade em constante mudança. O impacto da marca é astronômico, com tempo de inatividade não planejado.

É a tempestade perfeita: um local de trabalho em mudança, muitas coisas para garantir e recursos insuficientes para agir.

Problemas de conformidade, perda de reputação e clientes, e um custo estimado de US$ 4,24 milhões por vulnerabilidade de dados. Os ataques de Ransomware causam uma interrupção média de 22 dias.

E as violações regulamentares custaram às empresas mais de 1,3 bilhões de dólares...

É hora de M.A.P. sua jornada de cibersegurança

M.A.P, acrônimo de *Manage, Automate and Prioritize* (Gerenciar, Automatizar e Priorizar), é uma jornada em três fases para construir uma estratégia de cibersegurança abrangente, escalável e alinhada com o local de trabalho em todos os lugares.

Gerenciar, a primeira fase, é estabelecer as bases de sua cibersegurança. Nela, seu objetivo é passar de um estado desconhecido para um estado conhecido. Isso significa ganhar visibilidade sobre quem são seus usuários e os dispositivos e aplicações que eles utilizam, para entender melhor onde se encontram suas vulnerabilidades. Também significa eliminar práticas que poderiam colocar sua organização em risco, como ter dispositivos não gerenciados acessando os recursos da empresa (especialmente os que estão na nuvem) ou não acompanhando os últimos patches.

Automatizar, a segunda etapa, consiste em aliviar as cargas. Uma vez chegado a um estado conhecido, o próximo passo é liberar recursos, automatizando processos manuais e repetitivos, tais como manutenção do inventário, instalação de dispositivos a bordo e a implantação de espaços de trabalho e aplicações. Você também pode acrescentar soluções de auto remediação e auto-entrega para reduzir ainda mais a necessidade de intervenção da TI.

A última etapa, **Priorizar**, é chegar a um estado onde a TI tenha a informação e a capacidade de identificar e abordar as principais áreas de risco. Apesar da automatização, ainda existirão áreas que requerem intervenção de TI.

Em vez de adotar uma abordagem não estratégica e de adivinhação do risco, a priorização permite que a TI tenha os dados certos e as pontuações de risco para adotar uma abordagem inteligente e estratégica de resposta e remediação do risco.

M.A.P tem uma aparência diferente para cada organização, mas em cada instância deve cobrir os principais pilares dos usuários, dispositivos, rede, aplicações e dados, e incluir fatores consistentes, como:

- Descoberta;
- Gerência;
- Aplicação e verificação da configuração segura;
- Atualização dos sistemas de patches baseados em risco;
- Redução do risco induzido por funcionários, através de métodos que incluem credenciais verificadas;
- Controle adaptativo e gerenciamento do ciclo de vida.

Embora esta abordagem não possa impedir cada ataque, ela minimiza a superfície de ataque e permite uma gestão de risco inteligente e proativa, permitindo que você esteja o mais preparado possível. E quando surgem ameaças, o gerenciamento contínuo de riscos cibernéticos, projetado para acelerar a ação, reduz a exposição à segurança e limita a interrupção dos negócios.

Os benefícios potenciais também incluem melhor visibilidade, menos dispositivos não gerenciados e não conformes acessando os sistemas empresariais, menos tempo gasto com correções, menor risco de falhas de auditoria e economia financeira. Com as ferramentas certas, tudo isso é possível com menos intervenção manual.

O dilema que mantém as empresas presas e seis passos para sair dele

Embora o acima exposto pareça ótimo, entendemos que também pode ser assustador. No início, parece um dilema sem uma resposta clara. Precisamos melhorar a segurança, reduzir as ameaças, melhorar a produtividade e conservar recursos, mas como estamos muito dispersos, enfrentamos uma paisagem de ameaças e uma superfície de ataque cada vez maior, não temos largura de banda para implantar novos programas neste momento.

É por isso que mapeamos seis passos para ajudar a orientar as organizações em sua jornada. Cada um deles cobre um componente crítico para a cibersegurança efetiva hoje em dia, e, tomados em conjunto, formam a base de uma estratégia de gestão de cibersegurança abrangente e escalável.

PASSO 1

Obter visibilidade completa dos ativos

Não se pode controlar o que não se conhece. A falta de um inventário preciso e consolidado de nuvens e ativos (hardware e software) deixa sua organização vulnerável a riscos de segurança, deficiências de conformidade, rastreamento excessivamente complexo e dados confusos.

Com recursos de TI sob pressão em todo o mundo, agora é o momento de investir em uma plataforma automatizada que faça o maior e melhor uso das capacidades de seu equipamento. Uma iniciativa de descoberta exaustiva encontra todos os ativos de sua rede, tanto de propriedade corporativa como de BYOD, e os mapeia juntamente com o contexto para que você saiba quem está usando qual dispositivo, como e quando eles estão utilizando, o quanto interagem com sua organização, e a que eles têm acesso.

Os benefícios da descoberta incluem:

- Reunir visibilidade completa e em tempo real de todos os dispositivos e softwares conectados e seu contexto;
- Permitir a gestão eficiente, proteção e manutenção de ativos em qualquer lugar;
- Racionalizar e organizar todos os dados de todas as fontes;

- Rastrear e recuperar licenças de software;
- Otimizar o gasto geral dos ativos de TI (hardware, software, nuvem).

O que procurar em sua solução de descoberta:

- A capacidade de descobrir, gerenciar e proteger dispositivos que estão dentro e fora da rede.
- Isto inclui dispositivos que se conectam aos serviços na nuvem;
- Descoberta automática e M.A.P das conexões entre os principais ativos de hardware e software com os serviços e aplicações que dependem desses ativos;
- Um banco de dados consolidado de ativos, que pode extrair informações de uma variedade de sistemas, tais como gerenciamento unificado de endpoints (UEM), gateways de rede, serviços em nuvem
- e ITSM;
- Reconciliação entre o que é adquirido por TI e o que está ativamente conectado aos serviços comerciais;
- Conectores a fontes de dados (fornecedor, bancos de dados contratuais, garantia de hardware, etc.);
- Integração com ITSM e processos de segurança para remediação proativa de problemas de TI e vulnerabilidades de segurança.

PASSO 2

Modernizar o gerenciamento de dispositivos com gerenciamento unificado de endpoints

À medida que mais organizações continuam mudando para ambientes de trabalho híbridos, a segurança e a gestão de endpoints nunca foram tão críticas, tanto para o pessoal de TI quanto para os funcionários. O gerenciamento moderno de dispositivos é necessário para aumentar a produtividade dos usuários e de TI, permitindo, aos administradores de TI, automatizar o provisionamento de dispositivos e as implantações de software, e solucionar rapidamente os problemas dos usuários.

Para reduzir o tempo de suporte e garantir que todos os dispositivos sejam gerenciados de acordo com os mesmos padrões, escolha uma solução UEM com capacidade de gerenciamento para uma ampla gama de sistemas operacionais, incluindo iOS, Android, Windows, macOS, Linux, ChromeOS, dispositivos para trabalhadores da primeira linha para fins especiais, wearables e dispositivos IoT, com suporte tanto para gerenciamento moderno quanto para gerenciamento baseado no cliente.

Uma solução unificada de gerenciamento de endpoints deve estar disponível tanto no local quanto como uma oferta SaaS, para atender às suas exigências de implantação empresarial.

A UEM ajuda a proteger a privacidade dos funcionários, separando os dados empresariais e pessoais nos endpoints. A UEM também é totalmente compatível com as iniciativas da BYOD, maximizando a privacidade do usuário e protegendo os dados corporativos ao mesmo tempo.

Os benefícios de gerenciar dispositivos usando uma abordagem unificada de gerenciamento de endpoints incluem:

- Gestão consistente e segurança em todos os seus dispositivos;
- Fácil integração, provisionamento de aplicações e configuração de dispositivos em escala, melhorando tanto a produtividade de TI quanto a experiência do usuário;
- Monitoramento da postura do dispositivo e garantia da conformidade em todo momento;
- Eliminação de problemas de forma rápida e remota;
- Automatização das atualizações de software e implantações de SO;
- Fornecimento de painéis de controle abrangentes
- e inteligência em tempo real para melhorar a tomada de decisões de TI;
- Detecção e remediação de vulnerabilidades de OS e aplicações de terceiros;
- Redução dos tempos de interrupção do usuário final e fornecimento de uma experiência de integração perfeita.

PASSO 3

Estabelecer a higiene do dispositivo

Uma boa higiene dos dispositivos envolve a adoção de uma abordagem proativa, para garantir que somente dispositivos que atendam aos requisitos de segurança definidos tenham acesso aos recursos da empresa. Isto inclui ter sistemas que possam corrigir automaticamente dispositivos ou pôr em quarentena dispositivos com vulnerabilidades de software, tanto no sistema operativo como em aplicações. O estabelecimento de uma boa higiene dos dispositivos requer o uso de soluções de boa reputação para reduzir a superfície de ataque digital.

Por outro lado, a falta de higiene do dispositivo pode deixar sua organização suscetível a ciberataques, como ransomware. Para organizações com má higiene de dispositivos, o ônus é a TI, em vez de soluções criadas propositalmente, para rastrear ativamente as vulnerabilidades e proteger a organização de ciberataques.

Higiene para dispositivos móveis

Enquanto 71% dos profissionais sentem que os dispositivos móveis são essenciais para seu trabalho, os líderes de segurança quase unanimemente concordam que os trabalhadores remotos estão expostos a mais riscos do que os trabalhadores em escritório. E ainda assim, três em cada

quatro profissionais de segurança sucumbiram à pressão de sacrificar a segurança dos dispositivos móveis por uma questão de conveniência.

Isso é um grande problema. Uma higiene sólida dos dispositivos móveis é essencial para combater as vulnerabilidades dos dispositivos (jailbreak, detecção de root, versões vulneráveis do SO, etc.), da rede (ataques man-in the-middle, hotspots maliciosos, Wi-Fi inseguro, etc.) e das aplicações (avaliação de alto risco de segurança, avaliação de alto risco de privacidade, comportamento suspeito da aplicação, aplicação de carga lateral, etc.).

Os benefícios de estabelecer a higiene dos dispositivos móveis incluem:

- Limita tanto o erro humano quanto o investimento em TI com inteligência automatizada e acionável baseada em risco;
- Detecção e remediação Zero-day para que você não tenha que adivinhar o que está por vir;
- Detecta e remedia problemas mesmo em dispositivos que estão desligados ou não conectados.

Características a ter em conta em sua solução de defesa contra ameaças móveis:

- Priorização do software que protege contra todos os tipos de ataques móveis, incluindo phishing e ataques a nível do dispositivo, da rede e das aplicações;

- Procure uma proteção multinível, a partir de uma solução que defenda contra ameaças em níveis de dispositivo, rede e aplicação - além de ameaças de phishing - com capacidades de detecção de ameaças no dispositivo e na nuvem. A proteção no dispositivo também não deve requerer uma conexão com a Internet para detectar e remediar as ameaças;

- Uma política de conformidade por níveis, que pode ser aplicada para alertar o usuário final e o administrador de que seu dispositivo está fora de conformidade é essencial. A não conformidade é atendida com ações graduais, desde o bloqueio do acesso aos recursos corporativos até a quarentena, a retirada do dispositivo e a remoção de todas as aplicações, conteúdos, configurações, etc., fornecidos pela UEM.

Higiene para dispositivos desktop/laptop

Até que os ataques de ransomware e outras vulnerabilidades de dados sejam coisa do passado - um dia que pode nunca vir com base em sua trajetória atual - as organizações devem tomar medidas de proteção contra eles. A correção de Vulnerabilidades e Exposições Comuns (CVEs) é uma das melhores coisas que uma instituição pode fazer para combater os ataques de resgate. A pesquisa da Ivanti mostra que, infelizmente, 71% dos profissionais de TI e segurança consideram a aplicação de patches excessivamente complexa e demorada. Isso pode ser devido ao enorme volume de vulnerabilidades que existem.

Existem bem mais de 100.000 vulnerabilidades listadas no U.S. National Vulnerability Database (NVD). Enquanto apenas uma pequena porcentagem dessas vulnerabilidades está vinculada ao ransomware, e uma ainda menor é de exploração de tendências/ativas, identificar quais representam o maior risco para uma organização pode ser complicado. Um relatório da Ivanti mostra8 que, de 2018- 2020, usando a pontuação CVSS v3, se uma organização consertasse apenas vulnerabilidades críticas, sua cobertura contra o ransomware seria de apenas cerca de 35%.
A correção automatizada, informada do risco, é essencial para a higiene dos dispositivos desktop/laptop.

Os benefícios de estabelecer a higiene dos dispositivos desktop/laptop incluem:

- Limitação tanto o erro humano quanto o investimento em TI com inteligência automatizada e acionável baseada em risco;
- Redução da probabilidade de ataques de ransomware, através da aplicação de patches para corrigir CVEs com base no risco do mundo real;
- Aproveitamento da priorização automatizada das ameaças, para que você possa corrigir estrategicamente e otimizar a alocação de recursos;
- Ir além da aplicação de patches para automatizar as respostas, de modo que uma ameaça seja combatida sem a contingência da intervenção humana.

Características a ter em conta em sua solução de higiene dos dispositivos desktop/laptop:

Para dispositivos desktop/laptop, é essencial atualizar o software regularmente para erradicar - ou pelo menos limitar - as vulnerabilidades. Como a aplicação de patches pode se tornar esmagadora, é útil encontrar uma solução que possa avaliar automaticamente os riscos e fornecer inteligência acionável, com prioridade para as vulnerabilidades mais urgentes;

A priorização baseada em risco traz visibilidade aos pontos fracos mais arriscados em um ambiente. Isto permite às organizações avisar as necessidades mais críticas dos patches. Contexto de ameaça ativa, o que significa mapear as vulnerabilidades para informação baseada em ameaças do mundo real, é tão crítica quanto ajuda as equipes de TI/segurança a priorizar a aplicação de patches para combater as ameaças que provavelmente causarão o maior dano.

PASSO 4

Proteja seus usuários

As únicas pessoas que parecem gostar de senhas são os atores da ameaça que as armam. Além de ser onerosa para os usuários, a autenticação baseada em senha carece de dispositivo, aplicação, rede e contexto de ameaça.

Não há como saber se a pessoa que digita a senha é um funcionário ou um atacante que obteve a senha de um funcionário. Mesmo as senhas mais complexas podem ser comprometidas com relativa facilidade, através de força bruta, phishing e outros tipos de ataques.

As credenciais, assim como as senhas, continuam sendo um dos tipos de dados mais visados, estando implicados em 61% de todas as vulnerabilidades9. As credenciais são comprometidas mais rapidamente do que qualquer outro tipo de dado, e isto é especialmente verdadeiro no caso de phishing, que normalmente visa credenciais para obter mais acesso à organização da vítima escolhida.

As soluções SSO criam um único ponto de falha, que pode ser explorado por hackers para obter acesso à maioria ou a todas as aplicações empresariais. De acordo com a pesquisa, quarenta e dois por cento reutilizam senhas entre contas, e 17% reciclam de duas a cinco senhas para tudo. Isso significa que, se alguém tem uma conta comprometida fora de um contexto de trabalho, mas está usando as mesmas senhas no trabalho, sua organização está em risco.

Com o aumento do trabalho remoto, pode ser assumido que organizações reforçaram os protocolos de senhas, mas, na pesquisa da Verizon11, mais de um terço dos entrevistados disse que sua empresa flexibilizou os requisitos de autenticação para lidar com as restrições da COVID-19.

É hora da autenticação sem senhas via zero sign-on.

PO zero sign-on é um método de autenticação que usa senhas zero (como o uso de uma senha única).

Os benefícios de proteger seus usuários via autenticação sem senhas incluem:

- Sem senhas = sem credenciais a serem roubadas ou pescadas;
- Sem senhas = usuários mais felizes que não precisam se lembrar de senhas ou ser bloqueados nas contas;
- Aumenta a maturidade de sua segurança Zero Trust;

- Conserva fundos que anteriormente eram gastos no gerenciamento de redefinições de senhas e no tratamento de vulnerabilidades.

Não há como saber se a pessoa que digita a senha é um funcionário ou um atacante que obteve a senha de um funcionário.

Características a ter em conta em sua solução de autenticação:

- A solução ideal fornecerá acesso sem senhas a dispositivos, aplicações empresariais e serviços em nuvem;
- O acesso efetivo sem senha se baseia na autenticação multi-fator, que inclui posse (o que você tem, com um dispositivo móvel), inerência (biometria como impressão digital, Face ID, etc.) e contexto (localização, hora do dia, etc.), em vez de fatores de conhecimento (como senhas ou questões de segurança) para estabelecer a autenticação;
- Para uma abordagem de segurança Zero Trust com acesso contextual, alavanque uma solução que possa se integrar com uma solução unificada de gerenciamento de endpoints, que possa verificar usuário, dispositivo, aplicação, rede e ameaças antes de conceder o acesso;
- Procura soluções de autenticação sem senha que se integrem perfeitamente com soluções de identidade existentes, como IdP/IAMs, MTD/XDR/EDR, SOAR, SIEMs, e muito mais.

PASSO 5

Forneça acesso seguro

Os perímetros de rede que funcionavam quando sua equipe estava no escritório não são mais suficientes no Everywhere Workplace. Com funcionários trabalhando em vários locais (e muitas vezes imprevisíveis), um perímetro de rede contemporâneo deve refletir esta dinâmica, removendo limitações e complexidades enquanto garante a segurança.

As redes de hoje devem ser construídas sobre os princípios do perímetro definido pelo software (SDP). Um SPD fornece uma arquitetura de segurança integrada que, de outra forma, é difícil de ser alcançada através de produtos de segurança existentes, como o anti-malware. Ele foi projetado para aproveitar componentes comprovados e baseados em padrões, tais como criptografia de dados, atestado remoto, segurança mútua na camada de transporte e Security Assertion Markup Language. A incorporação destas e de outras tecnologias baseadas em padrões ajuda a garantir que o SDP possa ser integrado com seus sistemas de segurança existentes.

Embora o SPD seja uma estrutura de rede, ele ainda requer um nível de segurança para maximizar os benefícios. É aí que o Zero Trust - e especificamente o acesso à rede zero trust (ZTNA) - entra em jogo. Gartner define ZTNA como um produto ou serviço que cria uma fronteira lógica de acesso baseada em identidade e contexto em torno de uma aplicação ou conjunto de aplicações. O SDP pode ser usado para implementar redes Zero Trust.

Os benefícios de estabelecer acesso seguro em qualquer lugar incluem:

- Verificação de que somente usuários confiáveis e autenticados têm acesso aos recursos;
- Permite que a rede borre o perímetro externo, permitindo implantações mais flexíveis e fluxos de trabalho mais simples para o usuário final;
- Evita as limitações e complexidades dos perímetros rígidos, incluindo sua propensão a abrir acesso adicional e desnecessário às subseções da rede;
- Preserva a segurança e a visibilidade ao mesmo tempo em que facilita o acesso.

Características a ter em conta em sua rede Zero Trust:

- Soberania dos dados: os dados de aplicação não atravessam a rede de fornecedores e nem são expostos à Internet. Este caminho direto maximiza o desempenho e a experiência do usuário;
- Visibilidade holística: atividade por usuário, por dispositivo e por aplicação, incluindo recursos implantados SaaS;
- Avaliação contínua e adaptativa da postura de segurança do cliente, com aplicação automatizada
- da política com base em vários elementos contextuais em mudança, tais como comportamento e localização.

PASSO 6

Gerencie sua conformidade e risco

Para permanecer em conformidade e mitigar as ameaças, é imperativo controlar a governança, o risco e a gestão de conformidade (GRC).

Com muita frequência, as organizações administram a conformidade manualmente em planilhas, acredite ou não. Elas também costumam gastar uma grande quantidade de dinheiro em produtos de segurança fragmentados, sem verdadeiramente compreender como integrá-los e aproveitá-los. Isso se traduz no provérbio "atirar espaguete na parede para ver se ele gruda".

É essencial gerar um quadro geral a respeito da exposição ao risco. A maioria das avaliações da postura de segurança são realizadas após um ataque e são específicas para o vetor de ataque. Esta abordagem reativa, combinada com demasiadas posições vazias em funções de TI, é um problema substancial.

Com muita frequência, as organizações gerenciam o cumprimento manualmente... em planilhas, acredite ou não

Os benefícios de compreender a conformidade e o risco incluem:

- Substitui as tarefas manuais por processos de conformidade automatizados;
- Prepara o cenário para auditorias mais suaves;
- Mitiga o risco de forma proativa;
- Alinha o orçamento com o risco real, eliminando adivinhações;
- Cria uma estrutura de conformidade mais estratégica e confiável;
- Atende às mudanças de requisitos em constante evolução, sem a necessidade de desenvolvedores;
- Libera recursos humanos para se concentrarem em um trabalho mais estratégico.

Características a ter em conta em sua solução de conformidade:

- Uma solução robusta aliviará a carga de conformidade regulamentar, com rápida e fácil documentação para as nomeações do M.A.P. com verificações de segurança e conformidade;
- A capacidade de gerenciar o risco, de forma proativa, significa colocar a atenção no lugar certo e no momento certo,
- Procure substituir as tarefas manuais por atividades de governança repetitivas automatizadas, fazendo com que sua conformidade funcione como uma máquina bem lubrificada;

- A gestão da maturidade do processo significa que você pode avaliar a maturidade de seus processos e controles críticos de segurança, e otimizá-los de acordo com as prioridades e riscos;
- Para garantir resultados eficientes e precisos, procure uma solução que forneça orientação automatizada na avaliação de riscos.

M.A.P sua jornada de ciberseguridad

Cada um desses passos são elementos essenciais para gerenciar, automatizar e priorizar sua jornada de cibersegurança. Impressionado? Não sabe por onde começar? É fundamental que você faça parcerias e aproveite as soluções para apoiar sua jornada.

As soluções corretas serão abrangentes e integradas para aliviar a carga de seu pessoal de TI. As soluções ideais também preservarão uma experiência produtiva e intuitiva do usuário, o que manterá a integridade, não importa onde, quando ou como seus funcionários trabalhem.

Trabalhe em qualquer lugar. Proteja em todos os lugares.

Sobre a Cleveris

A Cleveris conta com uma solução integrada que permite a descoberta de dispositivos, gerenciamento de endpoints, segurança e ferramentas tradicionais de TI. Com ela, é possível viabilizar a implementação do Everywhere Workplace por meio de um único fornecedor.

Nossa plataforma encontra, corrige e protege qualquer dispositivo, em qualquer lugar e de maneira automática. Assim, todos os funcionários podem trabalhar melhor, independente do ambiente que se encontram.

Além disso, o Everywhere Workplace se conecta com outros recursos presentes em nosso portfólio, garantindo conformidade em nosso modo de atuação - que consiste em propor planos de ação diferenciados para cada perfil e necessidade.

Ofereça o melhor da tecnologia para seu time.

Conte com a empresa líder na América Latina e América Central.

Para mais informações, acesse cleveris.com.br ou escaneie o QR Code ao lado.


cleveris