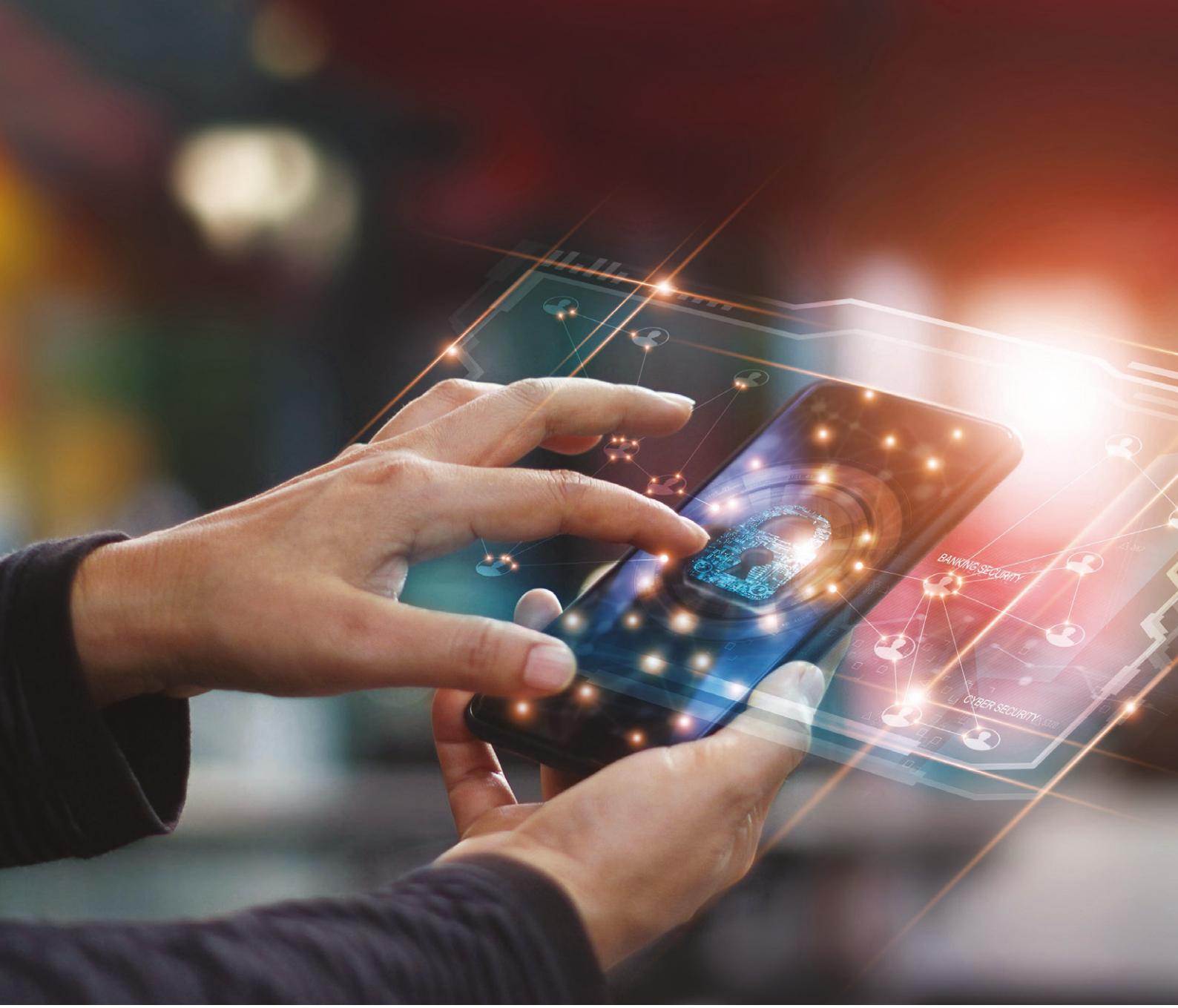
Construindo uma rede 'zero trust' com o melhor custo-benefício

Maximize a segurança da rede e minimize os custos

Resumo da Solução

Alcatel·Lucent Enterprise



Cibersegurança e confiança zero

A segurança cibernética é uma preocupação cada vez maior, à medida que a tecnologia continua avançando e o número e a complexidade das ameaças cibernéticas continuam aumentando. Existem ameaças que evoluem constantemente, e que tornam um desafio para as organizações prever e se defender contra elas, exigindo que os especialistas em segurança se mantenham atualizados com as últimas tendências e vulnerabilidades.

Com muitas fontes e vetores de ataque, como e-mails de phishing, engenharia social e vulnerabilidades de software, a defesa contra ameaças cibernéticas requer uma abordagem única para cada tipo de ataque.

Pode ser desafiador identificar e proteger todas as vulnerabilidades potenciais em um sistema complexo. É crucial para os especialistas em cibersegurança entender como os diferentes sistemas e redes funcionam juntos para desenvolver medidas de segurança eficazes.

O erro humano é uma causa comum de violações de cibersegurança e, até 2025, estima-se que a falha humana será responsável por mais da metade dos incidentes cibernéticos significativos.[1]

Atender a regulamentos e padrões de cibersegurança complexos, como o Regulamento Geral de Proteção de Dados (GDPR) e o Health Insurance Portability and Accountability Act (HIPAA), é outro desafio que requer conhecimento e expertise especializados.

1 Gartner® Predicts 2023: O Setor de Segurança Cibernética se concentra no Negócio Humano | Bitsight, Janeiro de 2023.

Processo de violação da segurança cibernética

A figura a seguir mostra as etapas que os invasores cibernéticos seguem para violar uma rede e roubar dados valiosos. Começa com a fase de reconhecimento, onde os invasores pesquisam, identificam e selecionam alvos, e procuram vulnerabilidades na rede.

A próxima etapa é a de preparação, onde os invasores determinam como comprometer um 'endpoint' alvo e entregar uma carga contaminada.

Depois disso vem a exploração, onde o invasor aciona a carga útil e escala privilégios no 'endpoint' comprometido para se mover lateralmente pela rede.

A próxima etapa é a de instalação, onde os invasores estabelecem acesso remoto e instalam malware para estabelecer persistência.

Na fase de comando e controle, os invasores estabelecem canais de comunicação criptografados de volta para servidores de comando e controle para direcionar remotamente o ataque e executar os objetivos.

A última etapa é a de movimento lateral e exfiltração, onde os invasores podem ter múltiplos objetivos, incluindo roubo de dados, destruição ou modificação de sistemas críticos e negação de serviço.

A chave para deter os invasores é detectar as diferentes etapas do ciclo de ataque precocemente, e interromper seu progresso.

Para evitar isso, você precisa adotar uma variedade de medidas, como gerenciamento de vulnerabilidades e patches, detecção e prevenção de malware, bloqueio de aplicativos e serviços de risco, registro e monitoramento de toda a atividade da rede, dos terminais e, claro, da nuvem.

Do lado da rede, você precisa implementar tecnologias que proporcionem um controle granular das aplicações e monitorem o tráfego entre zonas ou segmentos em um modelo 'zero trust'. O modelo de confiança zero opera com base no princípio de que tudo deve ser considerado "não confiável".

O conceito 'zero trust' foi desenvolvido em resposta ao aumento do número de ciberataques sofisticados nas redes de computadores. Tradicionalmente, as organizações têm confiado em soluções de segurança baseadas em um perímetro, como firewalls e software antivírus, para proteger suas redes. Entretanto, à medida que os ciberataques se tornaram mais avançados e complexos, essas soluções baseadas em um perímetro se mostraram insuficientes e, em vez disso, cada solicitação de acesso deve ser verificada e autenticada antes de conceder acesso aos recursos.

Fonte: XDR for Dummies, Edição Especial da Palo Alto Networks, 2022

Avançando com sua estratégia 'zero trust'

A Alcatel-Lucent Enterprise ajuda os clientes a se tornarem mais seguros e avançarem para um ambiente de confiança zero com simplicidade e eficiência de custos. Na ALE, entendemos a importância de implementar um modelo de confiança zero para garantir a segurança da rede e dos dados de nossos clientes. Oferecemos uma variedade de soluções projetadas para ajudar as organizações a implementar uma rede baseada em confiança zero e enfrentar os desafios apresentados pelas ameaças cibernéticas.

Fortalecimento da rede

Oferecemos uma **rede reforçada, interna e externamente**. Começa com uma infraestrutura segura, garantindo que o dispositivo em si não esteja comprometido. Nossa família de produtos Alcatel-Lucent OmniSwitch® opera com o sistema operacional Alcatel-Lucent (AOS) seguro, que usa código diversificado e seguro para proteger as redes contra possíveis vulnerabilidades e ataques. O código é continuamente atualizado para abordar ameaças atuais e futuras, com diversificação de software por meio da Randomização do Layout do Espaço de Endereço (ASLR) usada para proteger contra ataques de estouro de buffer. A Validação e Verificação Independente (IV&V) também é usada para analisar e testar o código-fonte do AOS em busca de vulnerabilidades potenciais, backdoors, malware e explorações do sistema. Especialistas em cibersegurança, de empresas independentes, conduzem os testes que são executados em imagens de software de disponibilidade geral, para garantir a integridade do software.

Aplicamos macro e microssegmentação para garantir o acesso à rede 'zero trust'. Ambos são componentes críticos de uma estratégia de segurança baseada em confiança zero. **Macrossegmentação** refere-se ao particionamento da rede em zonas ou domínios separados com base na função, no aplicativo usado ou grupo de usuários. Isso fornece um alto nível de segmentação de rede, permitindo que as organizações isolem ativos e recursos críticos do restante da rede. A **microssegmentação**, por outro lado, concentra-se na segmentação da rede em um nível mais granular, até o usuário ou dispositivo individual. Essa abordagem oferece um controle mais detalhado sobre o acesso à rede, permitindo que as organizações apliquem políticas de segurança no nível do usuário ou dispositivo individual.

O Shortest Path Bridging (SPB) e o **Universal Network Profiles** (UNP) fornecem uma solução poderosa para ajudar na macro e microssegmentação de redes, o que melhora a segurança e o desempenho ao limitar o escopo de possíveis ataques.

O SPB é um protocolo de rede da Camada 2 que permite o roteamento multi-path em redes grandes, simplificando a configuração e o gerenciamento da infraestrutura de rede. Recursos como a segmentação virtual de rede oferecem proteção adicional contra acesso não autorizado e ciberataques. Ao usar SPB em sua infraestrutura de rede, as organizações podem se beneficiar de mais eficiência e segurança de rede, ajudando a atender seus objetivos de negócios com confiança.

O ALE UNP é um controle de acesso baseado em perfil, um recurso poderoso dos switches Alcatel-Lucent Enterprise que permite que os administradores de rede criem e gerenciem perfis de usuário para acesso à rede com base na identidade, localização e dispositivo. Eles podem implementar o gerenciamento centralizado de políticas de rede, simplificando a configuração e aplicação de políticas. Ao implementar o ALE UNP, as organizações podem aprimorar sua visibilidade, segurança e controle de rede, além de melhorar o desempenho da rede, proteger ativos e reduzir o tempo de inatividade.

Juntos, SPB e UNP permitem que os administradores de rede gerenciem e protejam eficientemente a infraestrutura de rede para:

- Aplicar políticas de forma consistente, em toda a rede
- Segmentar e isoar dispositivos IoT de outros dispositivos
- Minimizar a superfície de ataque da rede

Autenticação robusta

A ALE oferece autenticação robusta por meio de um Gerenciador de Autenticação de Política Unificada (UPAM).

Um componente-chave da cibersegurança é a autenticação, que é o processo para verificar a identidade de um usuário, dispositivo ou sistema. Envolve a confirmação de que um usuário ou dispositivo é quem afirma ser, geralmente fornecendo alguma forma de identificação, como nome de usuário e senha.

A solução da ALE suporta diversos métodos de autenticação do usuário.

- **802.1X**, um protocolo de autenticação de rede, permite que dispositivos se conectem a uma rede segura fornecendo credenciais, como nome de usuário e senha. Quando um dispositivo tenta se conectar a uma rede usando o 802.1X, ele é autenticado primeiro antes de ser permitido o acesso à rede. Em um mundo ideal, o dispositivo é autenticado por meio do 802.1x. A autenticação gera um registro que pode ser compartilhado com um firewall.
- Se o dispositivo não for compatível com 802.1x, a autenticação de **endereço MAC** oferece uma opção. Um endereço MAC é um cartão de identificação digital para cada dispositivo em uma rede. Ele é único, identifica cada dispositivo e permite a comunicação entre eles, semelhante a uma etiqueta de nome para seu computador ou telefone.
- A ALE oferece suporte à **impressão digital de dispositivos e sistemas.** Se nenhum perfil for retornado com a autenticação 802.1X ou MAC, tentamos a identificação por impressão digital. A identificação, em segurança de computadores, é o processo de coleta de informações sobre um dispositivo ou sistema, como seu sistema operacional, software e portas abertas, para identificá-lo e categorizá-lo, e para avaliar riscos e vulnerabilidades potenciais. Também pode ser usado para mapear um perfil de dispositivo registrado no banco de dados do inventário IoT.
- A ALE também utiliza uma regra "catch all" padrão no caso de um perfil não ser retornado. A regra "catch all" pode permitir acesso limitado ou negar completamente o acesso se a autenticação principal falhar.

Para executar esses diferentes tipos de autenticação, é necessário um local para criar e gerenciar as credenciais de usuários e dispositivos. É necessário utilizar o UPAM, um componente da solução Unified Access da ALE. Ele fornece serviços centralizados de AAA - Autenticação, Autorização e Accounting (Contabilidade) para a rede. Permite que os administradores da rede criem e gerenciem perfis de usuário para acesso à rede, com base na identidade, localização, e outros. O UPAM pode ser configurado e gerenciado pelo Alcatel-Lucent OmniVista® Network Management System, permitindo que os administradores de rede definam e apliquem políticas de acesso à rede.

Capacidade de resposta a incidentes

Responder rapidamente aos incidentes é um fator-chave na minimização dos danos aos sistemas e redes, bem como na redução do tempo de inatividade causado por ataques de segurança, como o Ataque Distribuído de Negação de Serviço (DDoS).

Minimize os riscos, maximize a qualidade da experiência (QoE) e aprimore a segurança com o Alcatel-Lucent OmniVista Network Advisor. O **OmniVista Network Advisor** é um sistema inteligente e autônomo baseado em IA que oferece monitoramento da rede em tempo real, emite alertas à medida que os problemas surgem e sugere soluções para várias questões relacionadas à rede e à segurança, incluindo ataques DDoS. Ele realiza continuamente auditorias de configuração e análises de desempenho da rede para poder **identificar** possíveis problemas, **corrigir falhas** e **otimizar** a rede com mínima ou nenhuma intervenção de TI.

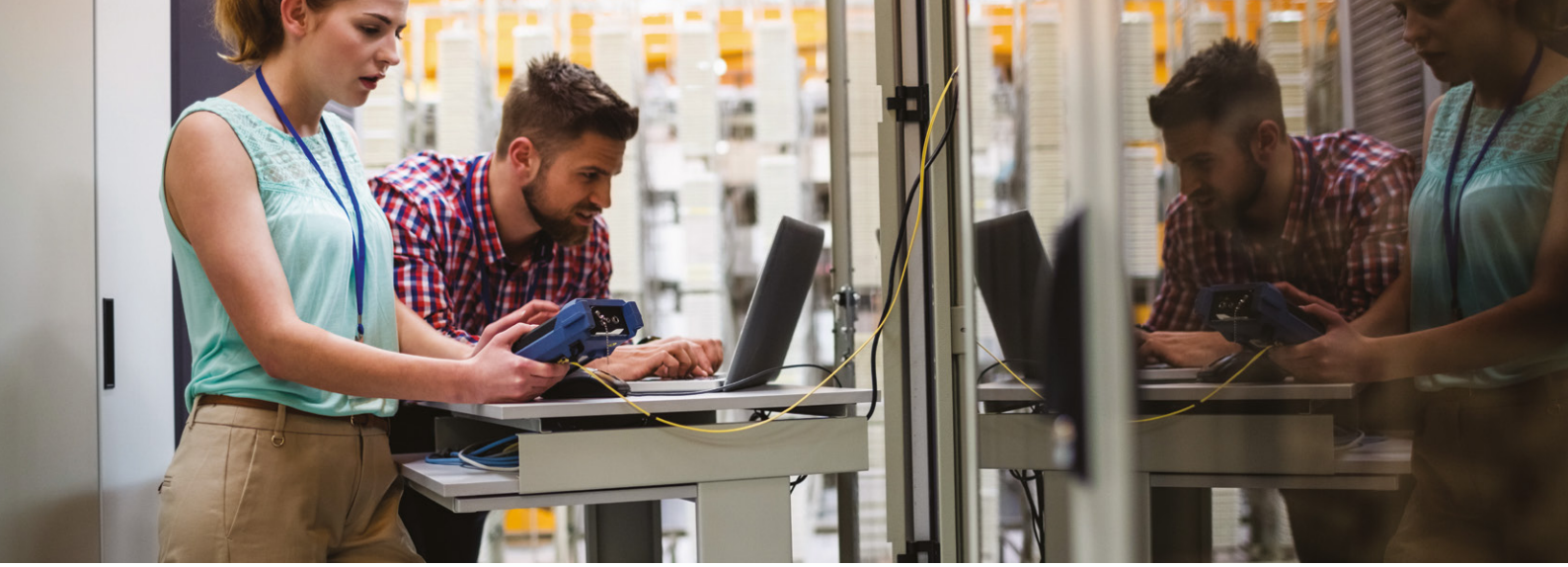
Parcerias e integrações

Um aspecto importante da autenticação é a integração com firewalls. Por exemplo, por meio da integração com a Fortinet, os usuários ou dispositivos autenticados nas redes LAN e/ou WLAN também podem ser autenticados simultaneamente no firewall da Fortinet.

Com a integração do firewall da Palo Alto Networks (PAN), os usuários ou dispositivos autenticados nas redes LAN e/ou WLAN também podem ser autenticados simultânea e perfeitamente no firewall PAN.

Nossa parceria com a Versa Networks permite acesso seguro a recursos críticos, independentemente da localização dos usuários, dados, aplicativos ou dispositivos. Isso é especialmente benéfico para empresas com escritórios regionais ou filiais remotas em relação ao local central ou data center. Ao contrário das redes WAN tradicionais, que exigem múltiplos hops de rede e podem incorrer em custos adicionais, SASE e SD-WAN fornecem uma solução econômica e segura na era de cliente-para-nuvem. Ao combinar essas duas soluções, as empresas podem simplificar a gestão da infraestrutura de TI e permitir o acesso seguro à Internet e aplicativos de negócios para cenários de trabalho de qualquer lugar, incluindo empresas, escritórios regionais/filiais e funionários remotos/móveis.

A oferta ALE-Versa Titan é uma solução abrangente que combina serviços Secure Access Service Edge (SASE) e SD-WAN da nuvem. Isso inclui o Versa Titan SD-WAN, que fornece SD-WAN entregue na nuvem para uma TI enxuta, bem como o Versa Secure Access (VSA), que possui recursos de firewall de próxima geração e bloqueio geográfico, juntamente com o Zero Trust Network Access (ZTNA) para cenários de trabalho de qualquer lugar. Além disso, o Versa Secure Web Gateway (SWG) fornece navegação segura na web e acesso a aplicativos da Internet (SaaS) para conectividade segura no escritório remoto/em casa. O portal web e o aplicativo Versa Titan oferecem serviços de rede e segurança integrados em uma única plataforma, com todos os componentes SASE fornecidos pelo mesmo fornecedor. Com um único repositório de políticas que abrange políticas de rede e segurança, as empresas podem simplificar a gestão de TI e garantir acesso seguro a recursos críticos.



A metodologia 'Zero Trust'

Para implementar um modelo de confiança zero, as organizações devem primeiro abordar os problemas em sua infraestrutura de segurança existente, como políticas inconsistentes, confiança implícita e dispositivos IoT vulneráveis. O objetivo é estabelecer o acesso à rede e o controle de acesso baseado em funções, segmentação e capacidades de monitoramento para combater esses problemas, com a segmentação adequada permitindo a divisão de recursos sensíveis e limitando o acesso apenas àqueles que o requerem. As funcionalidades de monitoramento e quarentena permitem que os clientes identifiquem e isolem ameaças potenciais.

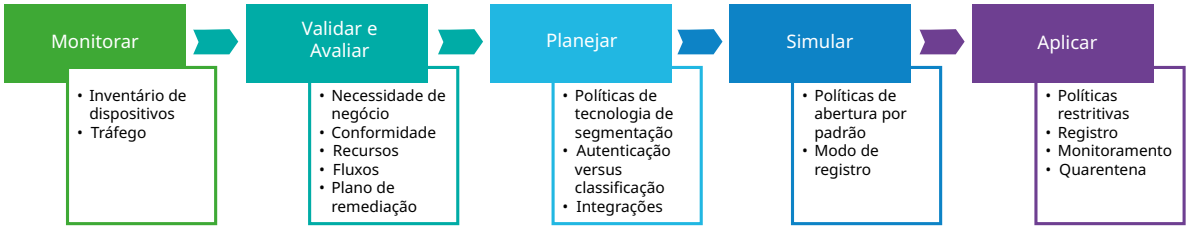
Uma metodologia simples, mas poderosa, para construir uma rede baseada em confiança zero com soluções ALE envolve várias etapas.

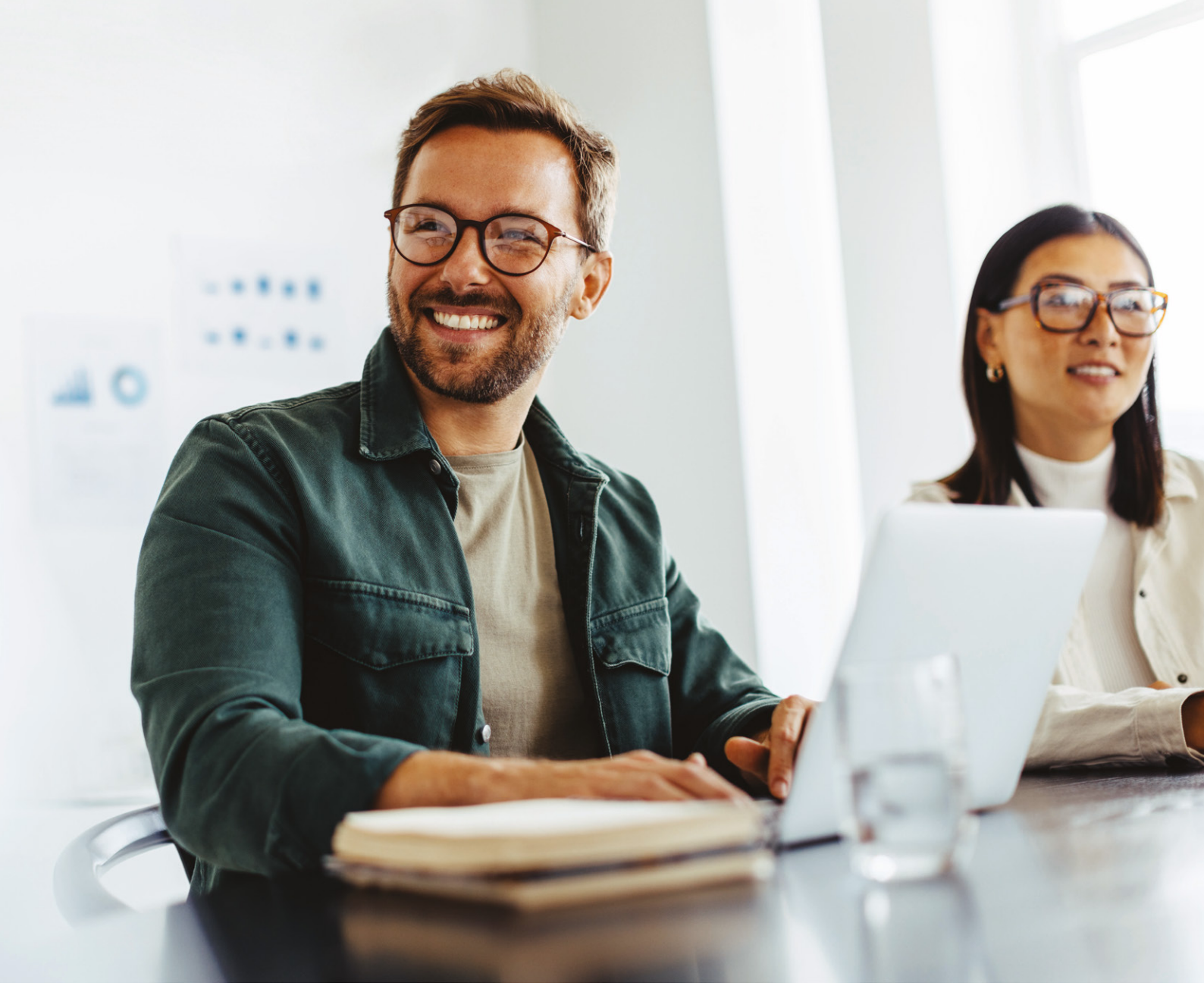
- **Monitorar**: o monitoramento deve ser realizado, incluindo inventário de dispositivos e tráfego
- **Validar e avaliar**: validação e avaliação envolvem a análise de necessidades de negócios, requisitos de conformidade, recursos e fluxos
- **Planejar**: um plano de correção deve ser criado com base nos resultados da avaliação. O planejamento inclui a seleção da tecnologia de segmentação e das políticas corretas, bem como considerar a autenticação versus classificação, e integrações.
- **Simular**: no estágio de simulação, as políticas são abertas por padrão e no modo de geração de registros, e outros recursos serão testados
- **Aplicar**: o estágio de aplicação envolve a implementação de políticas restritivas, registro, monitoramento e condução de medidas de quarentena

O Custo Total de Propriedade (TCO) abrange todas as despesas associadas à propriedade e operação de um produto ou serviço ao longo de sua vida útil. Isso inclui o preço de compra, manutenção, suporte e atualizações, entre outros. É importante selecionar soluções econômicas que ofereçam valor a longo prazo, o que pode mitigar excessos no orçamento e fornecer um retorno mais preciso sobre o investimento (ROI).

Considere a distinção entre o investimento inicial de capital e as despesas contínuas necessárias para manter o sistema licenciado e operacional. Enquanto alguns componentes, como firewalls, são puramente focados na segurança, outros componentes também são cruciais para construir uma estratégia de segurança mais aprofundada. Isso inclui gerenciamento de políticas, tecnologia eficiente de separação de caminho de rede (macro-microssegmentação avançada e automatizada), atribuição automática de rede virtual (VLAN), protocolo de criptografia de rede, visibilidade de aplicativos e validação independente e atestação do código do sistema operacional.

A estratégia de cibersegurança de rede da ALE aborda os elementos essenciais de segurança de rede mencionados acima sem custo, enquanto alternativas de outros fornecedores exigem expertise específica e inúmeros elementos e licenças para operação e manutenção. A abordagem da ALE oferece aos clientes benefícios econômicos substanciais, ao mesmo tempo que garante uma segurança cibernética forte e eficiente.





Conclusão

É evidente que a implementação de uma rede baseada em confiança zero para segurança robusta pode apresentar vários desafios, como complexidade e custos em termos de criação e manutenção. Entretanto, a ALE oferece uma abordagem única e econômica para esses problemas. Tecnologias avançadas de macro e microssegmentação, além dos outros componentes apresentados neste documento, oferecem um meio simples e acessível de implementar uma rede 'zero trust' que atende aos requisitos modernos de cibersegurança. Estamos comprometidos em ajudar nossos clientes a enfrentar suas preocupações com cibersegurança e acreditamos que nossa abordagem pode ajudar a alcançar esse objetivo.

As soluções ALE incluem nosso Intelligent Fabric (iFab) e UNP, resiliente e seguro, e controle de acesso à rede (NAC) robusto com UPAM, fornecendo controle de acesso baseado em perfil. Nossa solução inovadora OmniVista Network Advisor garante operação tranquila e rápida recuperação e prevenção de ataques. Além disso, somos parceiros de fornecedores SASE, como a Versa Networks, e integramos soluções de firewall, como o da Palo Alto Networks, para fornecer aos clientes soluções de segurança mais abrangentes e integradas.

Alcatel·Lucent Enterprise