Proteja e fortaleça seus negócios com a Alcatel-Lucent Enterprise

Lidando com a crescente complexidade das ameaças cibernéticas e com a evolução dos requisitos regulatórios

Folheto

Alcatel·Lucent
Enterprise

Introdução

À medida que as organizações passam por grandes mudanças em seus negócios, a segurança é uma área fundamental que está sendo alterada. O surgimento das tecnologias de IA interrompeu os modelos de segurança tradicionais, forçando uma reformulação de práticas antigas.

Em resposta, nossa equipe de especialistas em cibersegurança, redes, comunicações e nuvem uniu forças para compartilhar insights valiosos sobre os novos riscos que as empresas enfrentam e sobre como adicionar camadas essenciais de proteção para se manter à frente.

O cenário da cibersegurança

O ambiente de cibersegurança é definido pela rápida evolução tecnológica, ameaças mais sofisticadas e regulamentações mutáveis. Especialistas do setor destacam três tendências principais que agora moldam a cibersegurança empresarial:

1. O duplo papel da inteligência artificial
2. O aumento contínuo de ransomware e ataques à cadeia de suprimentos
3. A necessidade de uma gestão de identidade robusta em arquiteturas de confiança zero

O papel duplo da IA na cibersegurança

IA como arma para agentes mal-intencionados.

O uso malicioso da inteligência artificial surgiu como uma das ameaças mais significativas à segurança empresarial. Os cibercriminosos utilizam a IA para automatizar o reconhecimento, criar campanhas de phishing hiperpersonalizadas e desenvolver malware adaptável capaz de escapar dos sistemas de detecção tradicionais.

Ferramentas com tecnologia de IA analisam dados disponíveis publicamente para criar perfis de alvos, gerar áudio e vídeo deepfake convincentes e explorar vulnerabilidades com precisão cirúrgica. Um exemplo notável são os e-mails de phishing gerados por IA, que imitam estilos de comunicação legítimos e aumentam as taxas de sucesso em até 40% em comparação com os métodos tradicionais. Esses ataques tornam-se ainda mais graves com a comoditização das ferramentas de IA, que reduz a barreira de entrada para invasores menos qualificados.

A tecnologia de deepfake representa uma aplicação particularmente insidiosa da IA, permitindo que agentes mal-intencionados se façam passar por executivos ou colegas de confiança em chamadas de vídeo em tempo real para autorizar transações fraudulentas ou divulgar informações confidencias. Em um caso documentado, um vídeo deepfake de um diretor financeiro (CFO) instruindo uma transferência eletrônica resultou em uma perda de US$ 25 milhões para uma empresa multinacional. Tais incidentes ressaltam a necessidade de protocolos avançados de autenticação e treinamento de funcionários para reconhecer mídia sintética.

IA como mecanismo de defesa

Paradoxalmente, a IA também serve como espinha dorsal das defesas modernas de cibersegurança. Algoritmos de aprendizado de máquina analisam vastos conjuntos de dados para detectar anomalias, prever vetores de ataque e automatizar a resposta a incidentes. Por exemplo, os sistemas de segurança aprimorados por IA podem identificar vulnerabilidades de dia zero ao reconhecer padrões comportamentais sutis no tráfego de rede, reduzindo o tempo médio de detecção de semanas para horas. O Gartner afirma que as organizações que investem em plataformas de inteligência contra ameaças baseadas em IA sofrem 30% menos violações bem-sucedidas em comparação com aquelas que dependem de sistemas legados[1]. Os sistemas baseados em IA são especialmente eficazes na identificação de ameaças internas, monitorando o comportamento do usuário e sinalizando padrões de acesso incomuns, o que é cada vez mais crítico nos ambientes de trabalho remotos ou híbridos de hoje.

Desafios regulatórios e éticos

A natureza de uso duplo da IA gerou respostas regulatórias rigorosas. A Lei da UE sobre IA, promulgada em fevereiro de 2025, proíbe aplicações de IA de alto risco em áreas como a vigilância biométrica e exige transparência na tomada de decisões algorítmicas. As empresas agora precisam realizar auditorias de terceiros em sistemas de IA, documentar a procedência dos dados e garantir o uso ético — uma tarefa complexa, dada a opacidade de muitos modelos de aprendizado de máquina. As organizações estão criando comitês de ética de IA multifuncionais para navegar nesse cenário e fazendo parcerias com reguladores para moldar estruturas futuras.

Escalada de ataques de ransomware e cadeia de suprimentos

Visando fornecedores críticos

Os ataques de ransomware evoluíram de campanhas oportunistas para operações estratégicas direcionadas a fornecedores e prestadores de serviços essenciais. Os ataques de 2024 à CDK Global e à Change Healthcare demonstraram como comprometer um único fornecedor pode paralisar setores inteiros, custando bilhões em interrupções operacionais e esforços de recuperação. Hoje, os invasores se concentrarão cada vez mais em provedores de software como serviço (SaaS) e empresas de infraestrutura de nuvem, explorando seu papel centralizado em ecossistemas empresariais. Por exemplo, um ataque de ransomware a um grande fornecedor de armazenamento em nuvem pode bloquear o acesso de milhares de empresas aos seus dados simultaneamente, aumentando a influência da extorsão.

A proliferação de sistemas interconectados e a gestão insuficiente de riscos na cadeia de suprimentos facilitam esses ataques. Muitas empresas não têm visibilidade sobre as posturas de segurança de seus fornecedores, o que as deixa vulneráveis a falhas em cascata. O Gartner relata que 60% das organizações enfrentarão uma violação significativa na cadeia de suprimentos até 2026, causada por vulnerabilidades de terceiros em pipelines de DevOps e em frotas de dispositivos IoT[1].

Ecossistemas de Ransomware como Serviço (RaaS)

O surgimento de plataformas de ransomware como serviço democratizou o acesso a ferramentas de ataque avançadas, permitindo que até criminosos pouco qualificados realizem campanhas sofisticadas. Os operadores de RaaS fornecem malware personalizável, portais de pagamento e suporte de negociação em troca de uma parte dos resgates — normalmente de 20 a 30%. Esse modelo levou a um aumento de 150% nos incidentes de ransomware desde 2023, com pedidos médios de resgate excedendo US$ 5 milhões por incidente[2].

O ransomware moderno utiliza técnicas de ofuscação impulsionadas por IA, como código polimórfico e criptografia com atraso de tempo, para driblar mecanismos de detecção. Os invasores também exfiltram dados antes de implementar a criptografia, ameaçando vazar informações confidenciais, a menos que sejam pagos — uma tática conhecida como dupla extorsão. As empresas estão enfrentando essas ameaças por meio de backups isolados, soluções de armazenamento descentralizado e sistemas de verificação de integridade baseados em blockchain.

As organizações precisarão de tecnologia segura em todas as camadas para prevenir, conter e mitigar o impacto de ataques de ransomware e à cadeia de suprimentos.

1. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025
2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Gestão de identidade e o imperativo da confiança zero

A crise de identidade da máquina

À medida que as empresas adotam IA generativa, IoT e arquiteturas nativas da nuvem, as identidades de máquina, credenciais para dispositivos, APIs e cargas de trabalho automatizadas, ultrapassaram as identidades humanas em volume e risco. Em 2025, o Gartner identificou as máquinas não gerenciadas como um dos principais vetores de ataque, com chaves de API e contas de serviço comprometidas permitindo 45% das violações na nuvem[1]. Para enfrentar esse desafio, as empresas estão cada vez mais implementando ferramentas de gerenciamento de certificados que automatizam a rotação frequente de credenciais, fortalecendo suas políticas de privilégios mínimos e permitindo detectar comportamentos anormais das máquinas em tempo real.

Arquiteturas Zero Trust na prática

Estruturas de confiança zero, que pressupõem que nenhuma entidade humana ou mecânica seja inerentemente confiável, passaram de objetivos ambiciosos a necessidades operacionais. A implementação se concentra em autenticação contínua, microssegmentação e comunicações criptografadas. Por exemplo, uma rede de confiança zero pode exigir verificação biométrica para acesso a dados confidenciais, isolar ambientes de desenvolvimento de sistemas de produção e criptografar todo o tráfego leste-oeste dentro dos data centers.

O Instituto Nacional de Padrões e Tecnologia dos EUA (NIST), em uma avaliação de eficácia, aponta que as organizações que adotam uma arquitetura de confiança zero[2] reduzem os impactos das violações em 70%, em média. O sucesso depende da integração dos princípios de confiança zero na infraestrutura existente, um desafio para empresas com sistemas legados. As abordagens híbridas estão ganhando força, incluindo perímetros definidos por software para ativos locais e soluções de confiança zero nativas em nuvem.

Fatores humanos e ameaças internas

Segundo o Fórum Econômico Mundial, 95% dos incidentes de cibersegurança ocorrem devido a erro humano. Os ataques de phishing que aproveitam o conteúdo gerado por IA ignoram os filtros de e-mail com 30% mais eficácia do que os métodos tradicionais, enquanto os funcionários que expõem inadvertidamente credenciais em ferramentas colaborativas são responsáveis por 25% das violações. Ameaças internas são exacerbadas por erros de configuração de acesso manual à rede e trabalho remoto, onde dispositivos pessoais e redes desprotegidas criam pontos de entrada para invasores.

Tornou-se essencial capacitar os usuários para se protegerem melhor, ao mesmo tempo em que se reduz o impacto de políticas de segurança cada vez mais restritivas. Para administradores de rede e aplicativos, a automação de operações e a assistência ativa por meio de IA devem fornecer as ferramentas necessárias para proteger contra as consequências de possíveis configurações incorretas.

A abordagem ALE para proteger comunicações e produtos de rede

A abordagem da Alcatel-Lucent Enterprise em relação à segurança é garantir que as interações digitais sejam eficazes e estejam em conformidade com as regulamentações padrão do setor. A tecnologia digital está amplamente difundida, com a crescente adoção de dispositivos de IA e IoT que coletam dados para dar suporte a alertas em tempo real e planejamento futuro. Proteger e fortalecer as redes e comunicações que impulsionam os negócios atuais é vital para evitar interrupções de serviço. As soluções ALE para comunicações empresariais e infraestrutura de rede implementam a cibersegurança de ponta a ponta porque é a única maneira de garantir que a segurança seja aplicada de forma abrangente. Essa abordagem à cibersegurança ajuda empresas e instituições públicas a:

- Prevenir ataques cibernéticos, implementando a cibersegurança em todos os aspectos do design do produto para reduzir a superfície de ataque.
- Proteger-se contra ataques cibernéticos, implementando os mais recentes padrões de segurança e melhores práticas em todos os componentes da solução para aumentar a resistência.
- Reagir a ataques cibernéticos permitindo ações rápidas e adequadas para limitar o impacto e melhorar a resiliência, caso ocorra um ataque.

Como fabricante de produtos baseados em hardware e software, a abordagem de cibersegurança da ALE se concentra nas áreas descritas abaixo para atingir vulnerabilidades potenciais no cenário de ameaças cibernéticas.

1. Segurança desde a concepção

Historicamente, a maioria dos projetos de soluções era motivada pela necessidade de novos recursos, e a segurança era uma consideração essencial, mas secundária. Com a mudança do cenário, as prioridades tradicionais do design se inverteram. Os requisitos de cibersegurança agora devem orientar os designs das soluções. Soluções de hardware e software seguras por padrão levam em consideração a segurança em todas as etapas da definição, desenvolvimento e entrega do produto. Todo o hardware e sistemas operacionais são reforçados, a proteção contra negação de serviço (DoS) é integrada e as soluções implementam as melhores práticas de cibersegurança mais importantes para o setor.

2. Segurança de acesso à rede baseado em confiança zero

As estratégias de segurança que proporcionam confiança com base na localização do usuário dentro do firewall corporativo, nas credenciais que ele insere ou no aplicativo ou dispositivo que utiliza não são mais adequadas, mesmo quando vários mecanismos de segurança são combinados. Hoje, nenhum usuário, dispositivo ou aplicativo deve ter confiança implícita. O modelo de segurança de acesso à rede zero trust (ZTNA) ajuda as organizações a combater eficazmente as ameaças, que evoluem constantemente. A ZTNA não confia em nenhum usuário, dispositivo ou aplicativo, independentemente da localização. A ALE aplica o conceito de ZTNA permitindo a aplicação de políticas baseadas em funções, controle de acesso (Unified Policy Authentication Manager-UPAM) com base na localização e segmentação dinâmica entre usuários, dispositivos e aplicativos (por padrão, com, Shortest Path Bridging SPB, User Network Profiles-UNP) — sejam eles gerenciados ou não.

3. Macro e microssegmentação

A macro e a microsegmentação permitem uma abordagem granular e altamente controlada da cibersegurança para todos os usuários, dispositivos e aplicativos que acessam a rede. A macrossegmentação separa usuários, dispositivos e aplicativos de acordo com seu domínio funcional, para que não possam se comunicar com elementos em outros macrossegmentos. Por exemplo, os aplicativos de comunicação unificada e colaboração em um macrossegmento não podem se comunicar com tecnologias de segurança, como câmeras de CCTV e sistemas de fechaduras de portas, em um segundo macrossegmento. Ou com sensores e controles de iluminação, aquecimento e ar-condicionado em um terceiro macrossegmento.

A microssegmentação define como os usuários, dispositivos e aplicativos dentro de um macrossegmento podem interagir uns com os outros, e geralmente é regida por políticas de segurança específicas. Por exemplo, uma câmera de vigilância não deve ter permissão para interagir com uma fechadura de porta, muito embora estejam no mesmo macrossegmento relacionado à segurança.

4. Criptografia de ponta a ponta

Funcionários, clientes, parceiros e fornecedores podem estar em qualquer lugar nas organizações modernas. E as soluções que eles usam para se comunicar e colaborar podem estar instaladas no prédio em que trabalham, do outro lado da cidade ou em um data center do outro lado do mundo. Em todos os casos, as pessoas devem ser capazes de trocar informações com segurança e confidencialidade usando voz, vídeo e texto. Para garantir que apenas os participantes da conversa possam acessar as informações trocadas, cada conversa deve ser totalmente criptografada desde a origem até o destino. Isso significa que cada elemento de hardware e software envolvido nas comunicações de ponta a ponta deve ter mecanismos de criptografia aprovados por agências de segurança incorporados nativamente.

5. Certificações de segurança e privacidade e conformidade com as regulamentações

Há alguns anos, as certificações e acreditações de segurança mais rigorosas eram exigidas apenas para produtos de segurança, como firewalls, ou setores como o de defesa. Hoje, os padrões específicos de segurança devem ser aplicados a todos os produtos de tecnologia, em todos os setores. É fundamental verificar se certificações e acreditações reconhecidas respaldam as alegações de cibersegurança.

Veja aqui alguns exemplos de conformidade a serem procurados:

- Padrões globais de segurança e privacidade, como ISO 27001
- Normas de segurança e privacidade específicas do setor, como o Health Insurance Portability and Accountability Act (HIPAA) nos EUA e Hébergeurs de Données de Santé (HDS) para hospedagem de dados de saúde na França
- Regulamentos regionais de segurança e privacidade, como o Regulamento Geral sobre a Proteção de Dados (RGPD) e a Diretiva NIS 2 na União Europeia

6. Testes de segurança contínuos e especializados

Assim como os padrões de segurança, os processos especializados de testes de segurança, antes reservados aos produtos de segurança, agora são obrigatórios nas soluções de comunicações unificadas e colaboração. Os testes de penetração são um exemplo primordial. Esses testes simulam ataques cibernéticos para revelar vulnerabilidades de segurança, de modo que possam ser abordadas de forma proativa antes que ocorram problemas. Para se manter à frente das ameaças cibernéticas em um cenário em constante evolução, testes de penetração motivados exclusivamente por requisitos de cibersegurança devem ser realizados continuamente. Os fornecedores de tecnologia dedicados a ajudar seus clientes a manter a máxima cibersegurança devem fornecer os recursos, as ferramentas e a experiência necessários para realizar testes de penetração contínuos.

7. Soberania de dados

A soberania de dados se tornou uma preocupação significativa para a maioria das empresas que precisam proteger sua propriedade intelectual, preservar a confiança dos clientes e garantir uma vantagem competitiva. Com a adoção de novas tecnologias, como a nuvem e, mais recentemente, a IA, a abertura dos sistemas de comunicação das organizações para o mundo externo nunca foi tão importante, e a segurança do acesso à rede é igualmente crítica. Algumas empresas optarão por uma solução de nuvem pública que atenda às suas necessidades e, ao mesmo tempo, limite a superfície de ataque interna do seu sistema de informações. Outros optarão por uma abordagem mais tradicional, com aplicativos de comunicações unificadas hospedados em sua rede privada, no local ou em uma nuvem privada dedicada. Independentemente da escolha do cliente, a ALE está apta a fornecer seus produtos e serviços em todos os modelos de implantação, assegurando a soberania sobre dados críticos.

8. Operações inteligentes e automação de segurança

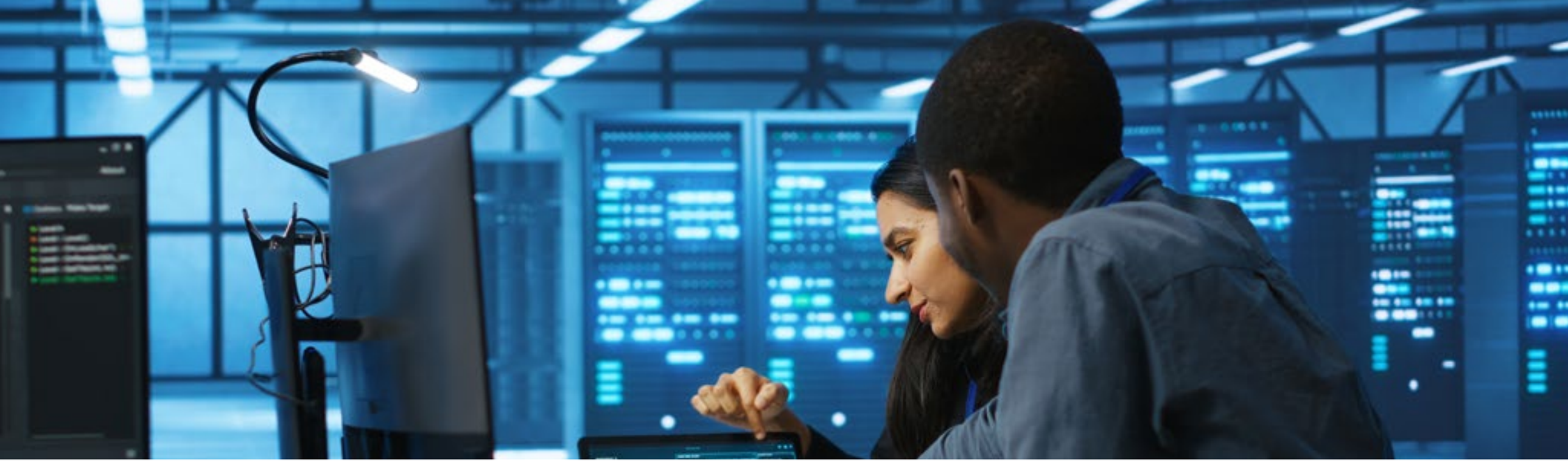
O pacote OmniVista e o Network Advisor da ALE oferecem segurança operacional avançada por meio de monitoramento em tempo real, auditorias de configuração e automação na resposta a ameaças. Com AIOps incorporados, anomalias de rede são detectadas proativamente e correções guiadas são fornecidas, geralmente exigindo um único clique para resolver problemas de QoE ou conformidade. Isso reduz erros humanos, acelera a resposta a incidentes e garante a conformidade com as políticas em ambientes complexos.

9. Conectividade segura em qualquer lugar

A ALE oferece suporte a SD-WAN segura para empresas distribuídas e trabalho remoto, combinando visibilidade de rede, segurança e otimização de desempenho, alinhando-se aos modelos modernos de trabalho de qualquer lugar. Com a criptografia MACsec, a integridade e a confidencialidade dos dados são preservadas em ambientes WAN multisite.

10. Cadeia de abastecimento de software confiável

A ALE aplica medidas rigorosas para proteger sua cadeia de fornecimento de software, incluindo imagens de firmware assinadas, processos de inicialização seguros, sistemas operacionais reforçados e validação independente de código-fonte. Essas práticas limitam a exposição a ameaças baseadas em software e garantem ambientes de implantação confiáveis.



Por que a ALE é o fornecedor confiável para proteger sua infraestrutura de rede e sua plataforma de comunicações empresariais

Embora muitos fornecedores de tecnologia enfatizem a cibersegurança, nem todos possuem o conhecimento abrangente necessário para implementar uma segurança completa. A Alcatel-Lucent Enterprise vai além dos outros fornecedores para implementar todas as melhores práticas necessárias para a cibersegurança de ponta a ponta.

Estamos comprometidos com os padrões mundiais:

- Seguimos as melhores práticas e recomendações do National Institute of Science and Technology (Instituto Nacional de Ciência e Tecnologia, NIST) ao realizar avaliações de risco em novos recursos e ao implementar funções de cibersegurança, como criptografia nativa, em nossos produtos
- Aplicamos as normas ISO 27001 a todas as nossas soluções
- Apoiamos a ZTNA, segmentação de rede granular e políticas de segurança concretas para reduzir o risco de atividades não autorizadas
- Executamos testes altamente especializados e específicos de segurança — como testes de penetração — em todos os nossos produtos.
- Garantimos que nossos produtos obtenham as principais certificações do setor, como HDS, HIPAA, Lei de Direitos Educacionais e Privacidade da Família (FERPA) e FIPS 140-2 para governo e defesa.
- Consideramos as certificações regionais para nossos produtos, como CSPN da ANSSI na França, ENS na Espanha, C5 na Alemanha e ANATEL no Brasil
- Cumprimos as regulamentações regionais de segurança e privacidade, como o GDPR, CRA e a Diretiva NIS 2 da União Europeia

Como especialistas reconhecidos em cibersegurança, contribuímos para as propostas da União Europeia em relação às diretrizes de cibersegurança. Também aproveitamos nossa experiência para ajudar nossos clientes a escolher e implementar, com o menor TCO (redução de 30-50%), a combinação certa de soluções seguras de comunicação e rede para suas necessidades e treinar seus funcionários nas melhores práticas de cibersegurança. Nossa abordagem abrangente à arquitetura Zero-Trust permite que nossos clientes demonstrem às suas seguradoras que estão adotando uma abordagem proativa e, geralmente, se beneficiem de um desconto de até 20-30% em seu seguro de segurança cibernética.

Conclusão

As tendências de cibersegurança de 2026 exigem uma mudança de paradigma na estratégia empresarial. As organizações devem conciliar o papel duplo da IA como ameaça e apoiadora, investir em cadeias de suprimentos resilientes para resistir a ataques de ransomware e reestruturar sistemas de gerenciamento de identidade para um mundo de confiança zero. A conformidade regulatória, o uso ético da IA e a colaboração entre setores serão essenciais para mitigar riscos. À medida que as superfícies de ataque se expandem com a adoção da computação de ponta e da IoT, as empresas que priorizam defesas adaptativas, capacitação dos funcionários e a busca proativa por ameaças estarão mais bem posicionadas para prosperar nesse cenário volátil.

O caminho a seguir exige inovação tecnológica e o suporte e a experiência de um fabricante confiável como a ALE.

Saiba mais

Para saber mais, visite ALE Security Solutions. Se deseja falar com um de nossos especialistas em segurança, entre em contato conosco.

www.al-enterprise.com O nome e logotipo da Alcatel-Lucent são marcas comerciais da Nokia usadas sob licença pela ALE. Para ver outras marcas comerciais usadas por empresas afiliadas da ALE Holding, acesse www.al-enterprise.com/en/legal/trademarks-copyright. Todas as outras marcas são de propriedade de seus respectivos proprietários. As informações apresentadas estão sujeitas a alterações sem prévio aviso. Nem a ALE Holding, nem qualquer de suas afiliadas, assumem qualquer responsabilidade pelas imprecisões aqui contidas. © Copyright 2026 ALE International, ALE USA Inc. Todos os direitos reservados em todos os países. DID25080602PT-BR (Janeiro de 2026)

Alcatel·Lucent Enterprise