



Protegendo as soluções de Comunicações Unificadas e Colaboração

O que é necessário no mundo atual de constantes mudanças

Whitepaper

Alcatel•Lucent 
Enterprise

Índice

- | Um foco mais sólido em cibersegurança
- | Seis áreas-chave para uma cibersegurança abrangente
- | Alcance seus objetivos de negócios com menos risco
- | Cibersegurança: Incorporada à mentalidade do provedor de tecnologia

Um foco mais sólido na segurança cibernética

Ao longo dos últimos anos, quase todas as empresas e organizações governamentais mudaram a forma como seus funcionários se comunicam, colaboram e compartilham informações. Embora a rápida mudança para apoiar os funcionários que trabalham em casa tenha sido crucial para manter a continuidade dos negócios durante a pandemia, ela teve um preço: o perímetro da rede agora se estende muito além dos limites tradicionais do escritório, aumentando significativamente a área de ataque da organização.

Os riscos associados aos perímetros de rede estendidos não desaparecerão tão cedo. De acordo com o Gartner, 39% dos trabalhadores do conhecimento de todo o mundo trabalharão em modelos híbridos remotos e presenciais até o final de 2023. Nos Estados Unidos, esse número chega a 51%.¹

As perturbações geopolíticas aumentaram ainda mais os riscos de cibersegurança. A Agência da União Europeia para a Cibersegurança chamou a invasão da Rússia à Ucrânia de "mudança de jogo" para o domínio cibernético global.² De acordo com a Association of Ukrainian IT Outsourcing Companies (Associação das Empresas Ucranianas de Terceirização de TI), uma em cada cinco empresas da Fortune 500 contou com desenvolvedores de software no país em 2022.³

Ao mesmo tempo, o impacto social dos ataques cibernéticos está aumentando. Em 2022, vimos grandes ataques cibernéticos à infraestrutura cívica crítica, causando uma emergência nacional na Costa Rica,⁴ e contínuo direcionamento às organizações de saúde.⁵

As organizações já não podem adiar as melhorias em cibersegurança

Estima-se que o crime cibernético custou à economia global € 5,5 trilhões em 2021, com danos que devem ultrapassar € 10 trilhões até 2025.⁶ O problema é tão grave que a União Europeia está criando um Ato de Resiliência Cibernética e emitiu uma versão significativamente aprimorada de sua Diretiva de Segurança de Rede e Informação (NIS) para proteger consumidores e empresas que comprem ou usam produtos ou software com um componente digital.⁷ Os Estados Unidos também estão implementando medidas para fortalecer a cibersegurança, incluindo o Decreto Executivo 14028, que incentiva as agências a adotar princípios de cibersegurança de confiança zero e ajustar as arquiteturas de rede em conformidade.⁸

À medida que empresas e governos buscam realizar a transformação digital e apoiar de forma mais permanente modelos de trabalho flexíveis, eles não têm escolha a não ser fortalecer a cibersegurança. As soluções que suas equipes utilizam para se comunicar, colaborar e compartilhar informações devem incorporar as melhores práticas em cibersegurança em todos os níveis e em todos os aspectos de funcionalidade.

¹ [O Gartner prevê que 39% dos trabalhadores do conhecimento em todo o mundo trabalharão em modelos híbridos até o final de 2023](#), Gartner, Março de 2023.

² [Geopolítica volátil abala as tendências do Panorama de Ameaças Cibernéticas de 2022](#), Agência da União Europeia para a Cibersegurança, Novembro de 2022.

³ [Uma em cada cinco empresas da Fortune 500 dependem da Ucrânia para suas necessidades de desenvolvimento de software em 2022](#), Iniciativa Ucraniana Hi-Tech, Outubro de 2022.

⁴ [Os 13 ataques cibernéticos mais caros de 2022: Retrospectiva](#), Inteligência de Segurança, Dezembro de 2022.

⁵ [Revisão de 2022: um ano agitado para a cibersegurança](#), Forbes, Dezembro de 2022.

⁶ Nova proposta de cibersegurança da União Europeia visa combater o crime cibernético. Fórum Econômico Mundial, Setembro de 2022.

⁷ [Lei de Resiliência Cibernética da UE](#), Comissão Europeia, Setembro de 2022.

⁸ [Decreto executivo para melhorar a segurança cibernética do país](#), Agência de Segurança Cibernética e de Infraestrutura.

Whitepaper

Protegendo as soluções de Comunicações Unificadas e Colaboração





Seis áreas principais para uma segurança cibernética abrangente

As soluções de comunicação unificada e colaboração devem implementar a cibersegurança de ponta a ponta, pois é a única maneira de garantir que a segurança seja aplicada de maneira abrangente. Uma abordagem de ponta a ponta para a cibersegurança ajuda empresas e governos 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**, tomando ações rápidas e adequadas para limitar o impacto e melhorar a resiliência, caso ocorra um ataque.

Para determinar se as soluções de comunicação unificada e colaboração implementam a cibersegurança de ponta a ponta, devem ser realizadas avaliações das soluções nas áreas descritas abaixo. Ao focar nessas áreas, é possível garantir que as avaliações das soluções sejam abrangentes, visando vulnerabilidades-chave em todo o panorama de ameaças cibernéticas.

Seguro desde o design

1 Historicamente, a maioria dos designs de soluções era orientada pela necessidade de novos recursos, e a segurança era considerada um ponto importante, porém secundário. Com a mudança no cenário, as prioridades de design tradicionais se inverteram, e os projetos das soluções atuais devem ser orientados pelos requisitos de cibersegurança.

Soluções de hardware e software que possuem segurança por design 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 Denial of Service (DoS) é incorporada, e as soluções implementam as melhores práticas em cibersegurança, mais relevantes para o setor. Por exemplo, uma solução de comunicação unificada e colaboração para organizações de segurança interna atenderá aos padrões de alta resiliência e confidencialidade exigidos por essas organizações.

2 Segurança Zero Trust Network Access (ZTNA)

Estratégias de segurança que apresentam confiança com base na localização do usuário dentro do firewall corporativo, nas credenciais inseridas ou no aplicativo ou dispositivo em uso, não são mais adequadas - mesmo quando vários mecanismos de segurança são combinados. Hoje, nenhum usuário, dispositivo ou aplicativo deve ter confiança implícita.

Soluções de comunicação unificada e colaboração que implementam um modelo de segurança Zero Trust Network Access (ZTNA) ajudam as organizações a combater efetivamente as ameaças, que evoluem constantemente. A ZTNA não confere confiança a nenhum usuário, dispositivo ou aplicativo, não importa onde estejam localizados. Baseia-se em cinco afirmações principais:

- A rede é hostil
- Ameaças externas e internas estão sempre presentes
- A localização e a identificação não são suficientes para determinar a confiança
- Todo dispositivo, usuário e fluxo de rede deve ser autenticado e autorizado
- As políticas de rede e de segurança devem ser dinâmicas e usar o maior número possível de fontes de dados



3 Macro e microssegmentação

A macro e microssegmentação permitem uma abordagem granular e altamente controlada, para a cibersegurança de todos os diferentes 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 muito específicas. Por exemplo, uma câmera de vigilância não deve ter permissão para interagir com uma fechadura de porta, apesar de estarem no mesmo macrossegmento relacionado à segurança.

4 Criptografia nativa de ponta a ponta

Nas organizações modernas, funcionários, clientes, parceiros e fornecedores podem estar localizados em qualquer lugar do mundo. 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 a eles.

5 Certificações e creditações de segurança e privacidade

Apenas alguns anos atrás, as certificações e creditações de segurança mais rigorosas eram exigidas apenas para produtos de segurança, como firewalls, ou em setores específicos, como defesa. Hoje, os padrões específicos de segurança devem ser aplicados a todos os produtos de tecnologia, em todos os setores.

É extremamente importante verificar se as alegações de cibersegurança são respaldadas por certificações e creditações reconhecidas. Veja aqui alguns exemplos de conformidade a serem procurados:

- **Padrões globais de segurança e privacidade**, como ISO 27001 para segurança da informação, ISO 27017 para ambientes em nuvem mais seguros e protegidos, ISO 27018 para proteção de informações pessoalmente identificáveis em ambientes em nuvem, e Common Criteria Evaluation Assurance Level (EAL) 2 ou superior para segurança de sistemas de computadores.
- **Normas de segurança e privacidade específicas do setor**, como o Health Insurance Portability and Accountability Act (HIPAA) nos EUA e Hôbergeurs de Données de Santé (HDS) para hospedagem de dados de saúde na França
- **Normas regionais de segurança e privacidade**, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia

6 Testes de segurança contínuos e especializados

Assim como as normas de segurança, os processos de testes de segurança especializados, que antes eram reservados apenas para produtos de segurança, agora são obrigatórios em soluções de comunicação unificada 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 manterem à frente das ameaças cibernéticas em um cenário em constante evolução, os testes de penetração orientados exclusivamente por requisitos de cibersegurança devem ser realizados de forma contínua.

Os provedores de tecnologia que se dedicam a ajudar seus clientes a manter a máxima cibersegurança devem fornecer os recursos, ferramentas e expertise necessários para realizar testes de penetração contínuos.



Alcançar metas empresariais com menos riscos

As soluções de comunicações unificadas e colaboração que implementam o conjunto completo de medidas de cibersegurança descritas na seção anterior oferecem às empresas e organizações governamentais a liberdade e flexibilidade para impulsionar suas atividades, ao mesmo tempo em que minimizam os riscos e garantem a conformidade. Elas podem:

- **Empoderar os funcionários** para colaborar e compartilhar informações com segurança e confidencialidade, usando qualquer mídia e qualquer dispositivo, de qualquer local
- **Melhorar a experiência do cliente** com comunicações enriquecidas, informativas e envolventes, tomadas de decisão mais rápidas, processos de negócios automatizados e a capacidade de detectar problemas proativamente antes que eles afetem o cliente
- **Aumentar a excelência operacional e a agilidade** usando a infraestrutura digital que é implantada onde faz mais sentido para a organização — no local ou em uma nuvem híbrida, privada ou pública — ao mesmo tempo em que adere a rígidas políticas de privacidade de dados e garante a conformidade com os dados regulamentos de privacidade

Os exemplos a seguir destacam apenas algumas das oportunidades possíveis, e que podem ser facilmente adaptadas para outras necessidades e setores.

Criar um ambiente de trabalho digital flexível para capacitar os funcionários.

Com a combinação certa de soluções de comunicação e colaboração, os funcionários podem trabalhar de maneira mais rápida e flexível, mantendo total conformidade com as regulamentações do setor.

- **No setor da saúde**, uma força de trabalho altamente móvel pode colaborar e compartilhar informações, mantendo total conformidade com as normas de segurança de dados. A equipe pode trocar informações e atualizações facilmente, e obter rapidamente a assistência necessária. A equipe médica pode usar comunicações seguras em tempo real para melhorar os resultados dos pacientes e a eficiência do fluxo de trabalho. A equipe não médica pode acelerar os processos e respostas a problemas de manutenção que possam afetar a segurança dos pacientes e da equipe.
- **No setor de educação**, os professores podem oferecer experiências de aprendizagem remota mais ricas e envolventes, com mais oportunidades para os alunos participarem de atividades, colaborarem em projetos e interagirem usando a mídia de sua preferência. O controle abrangente de acesso e as políticas automatizadas mantêm a integridade dos dados, e a análise de dados prioriza as comunicações críticas e os recursos de rede.
- **Em organizações governamentais**, a equipe pode trocar informações de forma segura entre equipes dispersas. Elas podem compartilhar telas, controlar remotamente o desktop de outra pessoa e trocar arquivos grandes para melhorar a colaboração. Também podem interagir com segurança com cidadãos por meio de aplicativos baseados na web ou móveis, usando voz, vídeo, chat ou mensagens instantâneas.
- **No setor de transporte**, o local de trabalho digital permite que os funcionários usem seus próprios dispositivos enquanto trabalham, implementam processos mais eficientes e fornecem serviços aprimorados aos passageiros, como a capacidade de trabalhar enquanto viajam. Protocolos de comunicação seguros, instalações protegidas e código diversificado protegem os dados em toda a rede.

Conectar tudo, para melhorar a experiência do cliente

Conectar pessoas, objetos e aplicativos com segurança e com comunicações em tempo real permite às empresas e organizações governamentais:

- Fornecer aos funcionários os dispositivos, tecnologias e dados de que precisam para melhorar o suporte aos clientes, minimizando o risco de erro humano ou falta de conhecimento comprometer a segurança.
- Usar dispositivos integrados e seguros para se comunicar e colaborar com clientes em movimento, com acesso total às soluções de gerenciamento de relacionamento com o cliente (CRM).
- Aumentar a proteção, o controle e a visibilidade sobre uma variedade crescente e diversificada de dispositivos da Internet das Coisas (IoT).
- Manter os sistemas de comunicação e colaboração atualizados para evitar o risco de aplicativos desatualizados aumentarem a superfície de ataque e exporem vulnerabilidades.
- Implementar controles de acesso eficazes e criptografia de ponta a ponta em todas as plataformas.

O gerenciamento unificado de rede permite que todas as plataformas de comunicação, aplicativos e dispositivos IoT sejam gerenciados de forma abrangente. A gestão unificada da rede:

- Simplifica as tarefas de gerenciamento em redes com e sem fio e dispositivos IoT, reduzindo os custos de gerenciamento de rede, otimizando o desempenho da rede e aumentando a eficiência operacional.
- Acelera a solução de problemas em ambientes de tecnologia cada vez mais diversificados para reduzir o risco de interrupções de serviço e tempo de inatividade

O gerenciamento unificado de rede em todos os setores oferece uma série de benefícios. Por exemplo:

No setor de saúde, as soluções de IoT podem rastrear a localização de equipamentos essenciais, como cilindros de oxigênio, carrinhos de emergência, monitores de pacientes, suportes de soro e cadeiras de rodas para melhorar a segurança e a eficiência. As conexões entre pessoas, objetos e aplicativos também podem ser usadas para acionar alarmes que notificam a equipe médica sobre as necessidades dos pacientes, mau funcionamento de equipamentos e podem alertar a todos na instalação sobre situações perigosas.

No setor de educação, há um novo potencial para conectar dispositivos e aplicativos inteligentes no campus, com múltiplas camadas de segurança, a fim de proteger os ativos da instituição de outros dispositivos com segurança insuficiente que acessam a rede. As instituições educacionais também podem utilizar a técnica de obtenção de impressões digitais de dispositivos IoT para identificar características dos dispositivos, como tipo, fabricante, modelo e sistema operacional, a fim de simplificar e acelerar a configuração da rede de IoT e o registro dos dispositivos.



Aumente a excelência operacional e a agilidade

Com a flexibilidade de implantar soluções de comunicação e colaboração unificadas de forma segura nas instalações ou em um ambiente híbrido, privado ou de nuvem pública, empresas e organizações governamentais podem se beneficiar das tecnologias digitais de acordo com seus objetivos e mandatos. Cada organização pode alcançar novos níveis de excelência operacional ao mesmo tempo em que atende aos requisitos específicos da indústria, adotando modelos em nuvem para melhorias operacionais e de agilidade, como:

- **Setor de saúde,** onde os registros digitais podem ser utilizados para melhorar o cuidado ao paciente e aumentar a eficiência, com a plena confiança de que as informações pessoais estão sendo armazenadas de forma segura em um data center certificado na nuvem.
- **Na área da educação,** onde o corpo docente, funcionários e estudantes têm acesso a aplicativos e serviços baseados em nuvem de qualquer lugar, de forma segura e sensível à privacidade. E os departamentos de TI podem reduzir o tempo e os custos associados à implantação, suporte e atualização da ampla variedade de aplicativos.
- **No setor público,** é possível tratar comunicações confidenciais com alta disponibilidade e protegê-las com mecanismos incorporados de prevenção de Denial of Service (DoS) e hardware e sistemas operacionais reforçados em termos de segurança.
- **No setor de transportes,** onde a alteração dos recursos de comunicação pode criar situações perigosas, tornando essenciais as soluções resilientes

Cibersegurança: incorporada à mentalidade do provedor de tecnologia

Embora muitos provedores de tecnologia não façam a cibersegurança, nem todos têm o conhecimento abrangente para implementar a segurança de ponta a ponta.

A Alcatel-Lucent Enterprise vai além de outros fornecedores ao implementar todas as melhores práticas necessárias para a cibersegurança de ponta a ponta. Desta forma:

- 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 recursos de segurança cibernética, como criptografia nativa, em nossas soluções
- Temos a certificação Common Criteria EAL2+ (Avaliação de Garantia de Nível 2 ou superior).
- Aplicamos as normas ISO 27001 a todas as nossas soluções baseadas em nuvem
- Apoiamos a ZTNA, segmentação de rede granular e políticas de segurança altamente específicas para reduzir o risco de atividades não autorizadas
- Executamos testes específicos de segurança altamente especializados, como testes de penetração, em todos os nossos produtos
- Garantimos que nossos produtos obtenham as principais certificações do setor, como HDS, HIPAA e Lei de Privacidade e Direitos Educacionais da Família (FERPA) como Rainbow by Alcatel-Lucent Enterprise

Como reconhecidos especialistas em cibersegurança, contribuimos para as propostas da União Europeia em relação às diretrizes de cibersegurança. Também aproveitamos nossa expertise para ajudar nossos clientes a escolher e implementar a combinação certa de soluções seguras de comunicações unificadas e colaboração, de acordo com suas necessidades, além de treinar seus funcionários nas melhores práticas de cibersegurança.

Saiba mais

Para saber como podemos ajudar sua organização a aproveitar ao máximo as soluções seguras de Comunicações na Era Digital, [visite nosso site](#) ou [entre em contato conosco hoje mesmo](#).

A Alcatel-Lucent Enterprise é uma empresa confiável, no mundo todo

As organizações líderes em todos os setores contam com nossas soluções seguras de comunicações da era digital para atingir seus objetivos, incluindo:

- [Metropolis e cidade de Perpignan](#), na França, onde autoridades governamentais estão implementando um plano estratégico de transição digital que inclui videoconferência e comunicações por voz para funcionários, suporte para aplicativos de IoT e novo conteúdo e serviços para os residentes, turistas e funcionários municipais de Perpignan.
- A [Universidade Newman](#) nos EUA, uma instituição católica de artes liberais, forneceu aos funcionários capacidades de telefonia móvel que não requerem números de telefone diretos, além de disponibilizar à equipe de TI uma plataforma única e intuitiva baseada em nuvem para gerenciar, provisionar e monitorar toda a infraestrutura de rede.
- O [Hospital Kingsway](#) na Índia implementou soluções de infraestrutura de comunicações em tempo real que mantêm a equipe clínica e administrativa conectada, permitindo otimizar os cuidados e aprimorar a experiência do paciente.
- O [Grupo J.Malucelli](#), no Brasil, modernizou sua rede com uma solução convergente de voz e dados que inclui telefonia em nuvem, assim como redes LAN e Wi-Fi com gerenciamento em nuvem para simplificar e reduzir o custo das comunicações para várias das empresas do grupo.