



OPINIÃO

O SASE e a quebra da assimetria tecnológica nas PMEs

Ian Ramone (*)

O mercado de tecnologia empresarial segue uma lógica histórica. Grandes empresas costumam ser as primeiras a acessar infraestruturas mais avançadas, criar equipes especializadas e investir em operações mais complexas. Essa disparidade gerou, ao longo dos anos, uma assimetria tecnológica em que organizações de grande porte possuem maior capacidade de proteção digital.

A cibersegurança foi, por muito tempo, um dos exemplos mais claros dessa diferença. Enquanto grandes corporações adotavam arquiteturas resilientes, monitoramento contínuo e políticas avançadas de proteção, muitas PMEs ainda dependiam de soluções pontuais, VPNs tradicionais e modelos centralizados de segurança com baixa escalabilidade.

O ambiente empresarial evoluiu mais rapidamente do que os modelos tradicionais de segurança conseguiram acompanhar. A lógica baseada exclusivamente em perímetro e data centers centralizados deixou de ser suficiente diante do avanço do trabalho híbrido, das aplicações em nuvem e das operações distribuídas.

Desta forma, o SASE (Secure Access Service Edge) começa a transformar a forma como empresas de todos os portes acessam tecnologias avançadas de conectividade e segurança.

Mais do que consolidar diversas soluções em uma arquitetura integrada, o modelo redefine como usuários, aplicações e dados são protegidos em operações cada vez mais distribuídas.

O fim da segurança concentrada no data center

Por muitos anos, o tráfego corporativo precisava ser roteado pelo data center central para que as políticas de segurança fossem aplicadas. O modelo funcionava bem quando usuários, aplicações e operações estavam concentrados no ambiente corporativo, mas passou a apresentar limitações em cenários híbridos e distribuídos.

As VPNs tradicionais continuam tendo relevância em determinados contextos, porém começaram a demonstrar limitações relacionadas à escalabilidade, experiência do usuário, visibilidade e complexidade operacional.

O SASE propõe uma abordagem diferente ao aproximar os mecanismos de segurança do ponto de acesso do usuário. Em vez de depender exclusivamente de estruturas centralizadas de inspeção, a validação ocorre de forma distribuída na borda da rede, reduzindo latência e simplificando o acesso remoto seguro.

Com isso, equipes, filiais e operações remotas conseguem acessar aplicações críticas de forma mais segura e eficiente, sem a necessidade de arquiteturas excessivamente complexas.

Zero Trust redefine a confiança digital

Outro elemento central dessa transformação é o modelo Zero

Trust, baseado no princípio de que nenhum acesso deve ser considerado confiável automaticamente.

Identidade, contexto, dispositivo, localização e comportamento passam a ser continuamente avaliados antes que o acesso seja autorizado. Dependendo das políticas definidas pela organização e do nível de risco identificado, acessos fora do padrão podem gerar validações adicionais, restrições ou bloqueios automáticos.

Historicamente, apenas organizações com operações maduras de segurança e grandes equipes especializadas conseguiam implementar monitoramento contínuo e respostas automatizadas em larga escala.

Com a evolução das plataformas integradas de segurança, muitas dessas capacidades passaram a se tornar mais acessíveis, automatizadas e viáveis também para empresas de menor porte.

Menos complexidade e mais competitividade

O desafio das equipes de TI deixou de ser apenas bloquear ameaças. A complexidade operacional gerada por ferramentas desconectadas passou a ocupar um papel central nas estratégias de segurança.

Gerenciar soluções isoladas para rede, acesso remoto, proteção de endpoints e ambientes em nuvem aumenta riscos operacionais, reduz visibilidade e dificulta respostas rápidas a incidentes.

Ao integrar conectividade e segurança em uma arquitetura mais inteligente e centralizada, o SASE reduz a fragmentação operacional e simplifica o gerenciamento da infraestrutura.

A segurança digital também passou a influenciar diretamente a competitividade das empresas, especialmente em processos de integração com cadeias de fornecimento, adequação regulatória e relacionamento com grandes organizações.

A segurança deixa de acompanhar apenas o tamanho da empresa

Com a adoção do SASE, a segurança corporativa começa a ser construída de forma diferente. Pequenas e médias empresas passam a ter acesso a recursos avançados de proteção, monitoramento e controle que antes eram restritos a organizações com grandes orçamentos e estruturas complexas.

Isso reduz uma barreira histórica do setor de tecnologia. A cibersegurança deixa de ser limitada apenas à capacidade de investimento das grandes corporações e passa a operar de forma mais acessível, escalável e alinhada ao modelo distribuído das empresas modernas.

No cenário atual, baseado em nuvem, mobilidade e conectividade constante, proteger usuários, aplicações e dados deixou de ser apenas uma necessidade técnica e passou a ser um fator estratégico de competitividade, independentemente do porte da empresa.

(*) Diretor comercial da N&DC.

A loucura da inteligência artificial: data centers em tendas

Fatos exóticos seguem acontecendo na área de inteligência artificial: agora, a Meta surpreendeu ao adotar uma estratégia inusitada: instalou um data center dentro de um conjunto de tendas gigantes.

Alexander_Kuzmin_CANVA



lares operarão alimentados por energia gerada por turbinas a gás instaladas nas proximidades.

A pressa na expansão da infraestrutura coincide com os desafios que a Meta enfrenta para disponibilizar seus novos modelos de IA ao mercado; o Wall Street Journal disse que o lançamento do modelo mais recente da companhia, o “Muse Spark”, tem sofrido sucessivos adiamentos.

A Meta projeta investir até US\$ 145 bilhões em bens de capital e infraestrutura de data centers. Esse valor astronômico, contudo, não têm agradado a Wall Street, refletindo-se em uma queda de 5% nas ações da empresa neste ano. Alojor chips de última geração em tendas surge, portanto, como uma alternativa para tentar conter os custos dessa corrida bilionária.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnit@gmail.com.

Profissionalização da gestão é novo divisor de águas para quem quer vender pela Internet

Realizado na sede do Mercado Livre, em Osasco (SP), o Magis5 Day reuniu sellers, executivos e parceiros do ecossistema digital para discutir os principais desafios da escala no e-commerce brasileiro.



Claudio Dias, CEO da Magis5

O evento reforçou uma percepção recorrente entre operações de médio e grande porte. A expansão no e-commerce moderno exige uma estrutura operacional integrada, previsível e orientada por dados, superando a visão ultrapassada de focar apenas no aumento bruto de vendas.

Segundo Claudio Dias, CEO da Magis5, o objetivo foi elevar o nível de governança das grandes operações. “A principal mudança do mercado está na transição do seller operacional para um modelo de gestão empresarial. Hoje, quem cresce sem estrutura perde margem, eficiência e capacidade de escala”, afirmou durante o encontro.

A programação priorizou discussões práticas sobre reforma tributária, futuro da gestão de negócios digitais, e-commerce e marketplace, logística, reputação e integração tecnológica no Mercado Livre.

Governança, Selo Platinum e dados

A empresa também destacou sua atuação como parceira Platinum do Mercado Livre, certificação concedida a parceiros tecnológicos do ecossistema, fator que amplia proximidade com atualizações da

plataforma e estabilidade operacional para sellers conectados ao hub.

“É um nível de governança que faz diferença principalmente para quem já opera em grande escala”, explica o CEO.

A programação reuniu empreendedores digitais e gestores de e-commerce que operam em alto volume dentro do Mercado Livre, com discussões voltadas à logística, reputação, automação, gestão financeira e integração de sistemas.

Durante o Magis5 Day, a empresa organizou uma agenda dividida em três frentes de conteúdo para sellers e decisores do setor:

O poder das Lojas Oficiais — painel voltado aos impactos estratégicos e operacionais das Lojas Oficiais para sellers em expansão.

Talks Estratégicos com a Digital Growth — sessão interativa sobre logística, conversão e gargalos enfrentados por operações em escala.

Ecossistema Magis5 & Sankhya — discussão sobre integração tecnológica, gestão corporativa e oportunidades geradas após a entrada da empresa no ecossistema Sankhya.

"O encontro também marcou as discussões sobre a nova fase da empresa após a integração ao ecossistema da Sankhya. Detalhamos para nossos clientes e parceiros o que esse movimento de mercado representa para a evolução do setor e quais novas oportunidades tecnológicas surgirão daqui para a frente", detalha o executivo.

Entre os temas que devem dominar as discussões está a necessidade de profissionalização das operações. Para o hub, o principal divisor de águas no e-commerce atual é a transição do vendedor para um modelo de gestão empresarial.



News@TI

ricardosouza@netjen.com.br

Consulta global sobre atualização do padrão de segurança para pagamentos

@OPCI Security Standards Council (PCISSC), fórum global responsável pelo desenvolvimento dos principais padrões de segurança da indústria de pagamentos, abriu um novo ciclo de RFC (Request for Comments) do PCI DSS (Payment Card Industry Data Security Standard), padrão internacional voltado à proteção de dados de cartões de pagamento. O processo colaborativo tem início no dia 3 de junho e permite que empresas e organizações do mundo todo contribuam com sugestões relacionadas à evolução dos padrões de segurança (https://www.pcisecuritystandards.org/).

Debates focados em IA, negócios e transformações do setor financeiro

@O Itaú Unibanco retorna ao Web Summit Rio como um dos principais parceiros da conferência e reforça, pelo quarto ano consecutivo, sua posição entre os protagonistas das conversas sobre inovação, inteligência artificial e evolução do mercado financeiro. O encontro acontece até 11 de junho, no Riocentro, reunindo lideranças globais de tecnologia, negócios e empreendedorismo. Com participação ampliada e uma programação voltada à transformação dos negócios na era da IA, o banco promoverá discussões sobre inovação, bem-estar financeiro, empreendedorismo e os reflexos das novas tecnologias na forma como pessoas e empresas se relacionam com o dinheiro.

Editorias

Economia: Nelson Tucci (nelson.tucci@netjen.com.br)
Mercado/Negócios/Tecnologia/Agronegócios/ Espaço empresarial: Ricardo Souza (ricardosouza@netjen.com.br);
Livros: Ralph Peter (ralphpeter@agenteliterarioralph.com.br)
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.

Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Jornal Empresas & Negócios Ltda

Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.