

Fortinet: cinco aspetos a considerar para o SASE na Era da IA

Lisboa, Portugal, 30 de setembro de 2026

À medida que o Unified SASE se generaliza, a atenção começa a deslocar-se das promessas de marketing para a aplicação prática. A questão já não é saber que fornecedores afirmam oferecer convergência, mas quais conseguiram, efetivamente, integrar as funcionalidades de rede e de segurança numa única arquitetura. Neste contexto, a Fortinet identifica cinco aspetos essenciais para uma integração SASE bem-sucedida.

1. Os custos de integração de que ninguém fala

Há uma realidade que os relatórios nem sempre explicam: a maioria das soluções SASE de um fornecedor único não está verdadeiramente integrada. Em muitos casos, resulta sobretudo da agregação de diferentes tecnologias através de aquisições.

Mesmo que a organização receba só uma fatura, continua a ter de gerir políticas e fluxos de trabalho operacionais distintos. É daqui que resultam os chamados “custos de integração”, custos operacionais ocultos associados à gestão de uma plataforma composta por diferentes soluções, e não concebida de raiz como um todo.

2. O que significa realmente a “Era da IA”

Há vários anos que o setor debate o papel da inteligência artificial na cibersegurança. Grande parte dessa discussão centra-se na utilização da IA para detetar ameaças. No entanto, a IA é hoje, em simultâneo, uma nova superfície de ataque, um acelerador operacional e um desafio em matéria de governação.

1. **IA como superfície de ataque:** A chamada “Shadow AI” deixou de ser apenas um conceito. De acordo com o Gartner CIO and IT Executive Survey 2025, a adoção de inteligência artificial generativa, ou GenAI, deverá atingir os 73% em 2026*, permanecendo uma parte significativa desta utilização sem qualquer controlo. Na prática, isto significa que os colaboradores podem introduzir dados sensíveis em modelos públicos de IA, enquanto diferentes sistemas recorrem a APIs externas de inteligência artificial sem o conhecimento ou a supervisão das equipas de TI.

2. **Observabilidade da IA nas comunicações entre agentes:** À medida que os fluxos de trabalho baseados em agentes de IA se tornam mais comuns nas empresas, o modelo de segurança precisa de ir além das tradicionais interações entre utilizadores e aplicações. Torna-se essencial compreender o que fazem os agentes de IA, com quem comunicam, que dados processam e quais os recursos a que acedem. Sem esta visibilidade, as organizações podem perder o controlo sobre interações automatizadas que envolvem informação, sistemas e processos críticos.

3. **Segurança da GenAI no ponto de utilização:** A utilização de ferramentas como o ChatGPT e o Copilot pelos colaboradores é cada vez mais frequente. A verdadeira questão está nos dados que são introduzidos ou carregados nessas plataformas, incluindo código-fonte, informação de clientes, dados financeiros ou documentação relacionada com processos de fusões e aquisições. A informação sensível pode, assim, sair das organizações através de *prompts* de IA sem ser detetada. Para a maioria dos sistemas de segurança, este tráfego aparenta ser legítimo, o que dificulta a identificação de potenciais fugas de dados. Neste contexto, a integração de capacidades de *Data Loss Prevention* (DLP) torna-se fundamental para identificar, monitorizar e impedir a exposição indevida de informação sensível através de aplicações e serviços baseados em IA.

3. A vantagem do hardware

Os fornecedores *cloud-native* apostaram que os recursos de computação normalizados eliminariam a necessidade de *hardware* desenvolvido para fins específicos. Essa premissa revelou-se correta no contexto da *cloud*, mas não necessariamente no que respeita ao desempenho.

Quando um fornecedor de SSE não disponibiliza capacidades de SD-WAN, as organizações têm de recorrer a uma solução de terceiros, suportando continuamente os respetivos custos de integração. Por outro lado, quando um fornecedor disponibiliza SSE com funcionalidades de SD-WAN limitadas, acaba por fragilizar a sua proposta global.

Para as organizações que necessitam de desempenho consistente e de uma aplicação uniforme das políticas de segurança nas filiais, no *edge*, nos centros de dados e na *cloud*, o número de fornecedores capazes de responder a todos estes requisitos reduz-se rapidamente.

4. Uma única abordagem não responde a todas as redes

Uma oferta SASE disponibilizada exclusivamente através da *cloud* pode parecer simples: instalar agentes em todos os dispositivos, encaminhar o tráfego através dos pontos de presença, ou PoPs, do fornecedor e considerar o processo concluído. No entanto, os ambientes empresariais raramente correspondem a este cenário simplificado.

A rede de uma organização será, muito provavelmente, composta por uma combinação de portáteis geridos, dispositivos não geridos utilizados por prestadores externos, filiais onde não se justifica instalar *appliances* completos, utilizadores remotos que não podem ou não querem instalar agentes, cargas de trabalho de IA com requisitos rigorosos de latência e aplicações distribuídas por *clouds* privadas e públicas e por centros de dados *on-prem*. Muitas organizações continuam também a operar em ambientes híbridos, onde coexistem infraestruturas tradicionais, recursos *cloud*, utilizadores remotos e aplicações críticas. Neste contexto, uma estratégia SASE eficaz deve oferecer flexibilidade suficiente para proteger utilizadores, aplicações e dados independentemente da sua localização.

Uma arquitetura SASE que não consiga acomodar todos estes elementos não pode ser considerada verdadeiramente “*unified*”. Trata-se apenas de uma solução parcial, concebida para um ambiente ideal que, na prática, poderá nunca existir.

5. A experiência digital tornou-se um indicador de segurança

O último aspeto a considerar é a convergência entre segurança e experiência do utilizador, não como uma funcionalidade opcional, mas como uma necessidade operacional.

A degradação do desempenho é frequentemente o primeiro sinal visível de um problema de segurança. Pode tratar-se de um *endpoint* comprometido que afeta o desempenho da rede, de uma política mal configurada que acrescenta latência a uma aplicação SaaS crítica ou de uma anomalia de DNS que se manifesta inicialmente como um problema de conectividade e só mais tarde é identificada como um ataque.

Uma plataforma SASE unificada proporciona visibilidade abrangente sobre o *endpoint*, a rede e as aplicações, através da mesma plataforma que gere e aplica as políticas de segurança. Desta forma, as equipas de operações deixam de ter de alternar entre uma ferramenta de *Digital Experience Monitoring*, ou DEM, e uma consola de segurança, passando a dispor de uma única visão integrada. Esta visibilidade permite determinar

rapidamente se a origem de um problema se encontra no dispositivo do utilizador, na conectividade de rede ou na própria aplicação.

Quando a segurança e a experiência do utilizador partilham o mesmo modelo de dados, as organizações não só conseguem resolver os problemas mais rapidamente, como também identificar implicações de segurança associadas a falhas na experiência digital que, de outro modo, poderiam ser desvalorizadas como simples ruído operacional das TI.

Conclusão

O mercado de SASE está a consolidar-se progressivamente em torno de plataformas, em detrimento de soluções pontuais e isoladas. Por esse motivo, as organizações não devem limitar-se a perguntar: “Este fornecedor disponibiliza SASE?”. A questão determinante deve ser: “Quem desenvolveu a arquitetura e quem foi responsável pela sua integração?”.

Nos últimos meses, a Fortinet continuou a expandir a sua plataforma Unified SASE com inovações nas áreas da segurança baseada em IA, das operações autónomas, da convergência da experiência digital e da flexibilidade de implementação.

Paralelamente, as organizações enfrentam uma crescente escassez de profissionais especializados em cibersegurança, tornando essenciais capacidades de automação, análise assistida por IA e serviços especializados de monitorização e resposta que permitam reforçar a proteção sem aumentar a complexidade operacional.

Acima de tudo, manteve a sua principal vantagem arquitetural: a integração das redes e da segurança num único sistema operativo e numa estrutura de gestão unificada. Esta abordagem ajuda a explicar o crescimento do Fortinet Unified SASE face a outras soluções que continuam a depender da interligação de componentes originalmente desenvolvidos de forma separada.