CLOUDFLARE

ARTIGO TÉCNICO

Simplificamos nossa forma de proteger aplicativos SaaS

Como proteger seus usuários e dados com uma abordagem Zero Trust

Conteúdo

Introdução

No ambiente distribuído da atualidade, os aplicativos do tipo software como Serviço (SaaS) possibilitaram às organizações uma maior flexibilidade para apoiar funcionários e prestadores de serviços corporativos no mundo inteiro. Alguns dos mais notáveis pacotes de aplicativos SaaS no momento incluem a comunicação (entrega de e-mails, plataformas de chat), a produtividade (documentos, planilhas) e a colaboração (armazenamento on-line). A Gartner prevê que até 2025 85% das empresas estarão administrando seus negócios com um princípio de nuvem em primeiro lugar — com o SaaS sendo o veículo de acesso preferencial para as implantações da administração.[1]

No entanto, embora os aplicativos SaaS permitam que as organizações se mantenham mais ágeis, a migração para a nuvem vem acompanhada de riscos de segurança e desempenho, especialmente no caso das organizações que precisam lidar com diversas soluções pontuais projetadas para operar independentemente umas das outras. Com a exiguidade de tempo decorrente de sua obrigação de implementar e administrar dezenas, senão centenas desses aplicativos, as equipes de segurança, rede e TI lutam para ganhar visibilidade em toda a empresa e têm dificuldades para lidar com as falhas de segurança e conectividade decorrentes de serviços que não foram inerentemente projetados para trabalhar juntos.

Como resultado, muitas organizações são levadas a buscar maneiras melhores de consolidar seus produtos de segurança dentro de seu panorama de SaaS de modo a aumentar a eficiência, reduzir a complexidade administrativa e de implementação e receber um suporte consolidado.

A Gartner prevê que, em 2025, 80% das empresas adotarão soluções de fornecedor único que unifiquem a web, serviços em nuvem e acesso privado a aplicativos a partir de uma plataforma de serviços de segurança de borda (SSE).[2]

Ao iniciar a jornada para uma segurança de SaaS simplificada, devemos levar em conta diversos fatores importantes. A forma como as forças de trabalho funcionam e se comunicam atualmente demanda uma abordagem de segurança simples e escalável, projetada para se manter à frente dos riscos que surgem continuamente, reduzir os incidentes decorrentes de aplicativos SaaS e facilitar a tarefa das equipes de segurança de monitorar e evitar ameaças às respectivas organizações.

Continue lendo para descobrir como uma plataforma Zero Trust — que integre os recursos de agentes de segurança de acesso à nuvem (CASBs) e de segurança de e-mails em nuvem (CES) — oferece o caminho mais fácil para deter perdas de dados, phishing, ransomware, TI invisível e movimentos laterais em toda a organização.

[1] Gartner, "Forecast Analysis: Information Security and Risk Management, Worldwide". Analistas: Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. 12 de agosto de 2021. Gartner. [2] Gartner, "Predicts 2022: Consolidated Security Platforms Are the Future". Analistas: Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. 1º de dezembro de 2021. Gartner.

A evolução do CASB

Uma segurança de SaaS abrangente requer diversas tecnologias cruciais para que as equipes de segurança possam ganhar visibilidade de todo o seu panorama de SaaS, monitorar e mitigar ameaças com facilidade e proteger o acesso a dados e sistemas confidenciais. Um dos componentes mais importantes de qualquer estratégia de segurança SaaS é um agente de segurança de acesso à nuvem, ou CASB, que fornece controle de segurança dos dados e visibilidade dos serviços e aplicativos de uma organização hospedados em nuvem.

Segurança SaaS 101: CASB

O CASB SaaS permite que as equipes de TI e segurança vejam todas as suas configurações de dados e atividades de usuários a partir de um único painel de controle. Seus recursos variam conforme o provedor, mas, de modo geral, incluem os seguintes atributos[3]:

- **Proteção de dados:** os CASBs protegem os dados confidenciais e evitam que saiam dos sistemas controlados pela empresa.
- **Controle de acesso:** os CASBs ajudam a controlar o que os usuários podem ver e fazer dentro dos aplicativos controlados pela empresa. Também podem fornecer recursos de verificação para garantir que os usuários são quem dizem ser.
- **Detecção de TI invisível:** os CASBs ajudam a identificar sistemas e serviços não autorizados (geralmente conhecidos como "TI invisível") que os funcionários usam para fins comerciais. Ao catalogar esses sistemas, os CASBs conseguem detectar e mitigar riscos de segurança desconhecidos anteriormente.
- **Proteção contra ameaças:** os CASBs usam a detecção antimalware, o uso de sandboxes, a inspeção de pacotes e outras tecnologias para ajudar a bloquear vazamentos de dados e ataques externos.
- **Gerenciamento de posturas:** os CASBs fornecem à equipes de segurança informações sobre as análises de dados de comportamento de usuários e o controle sobre as posturas de aplicativos, de modo que seja possível pesquisar movimentos e rastrear ameaças com facilidade em todo o seu ambiente de SaaS.
- **Conformidade:** os CASBs ajudam as organizações a cumprir as exigências regulatórias (por exemplo, SOC 2, HIPAA, GDPR etc.) ao identificar configurações inadequadas e, ao fazê-lo, evitam as respectivas multas e penalidades por violações de conformidade.

[3] Essa lista de recursos que podem estar incluídos em uma oferta de CASB não pretende ser exaustiva.

Entenda os desafios do CASB moderno

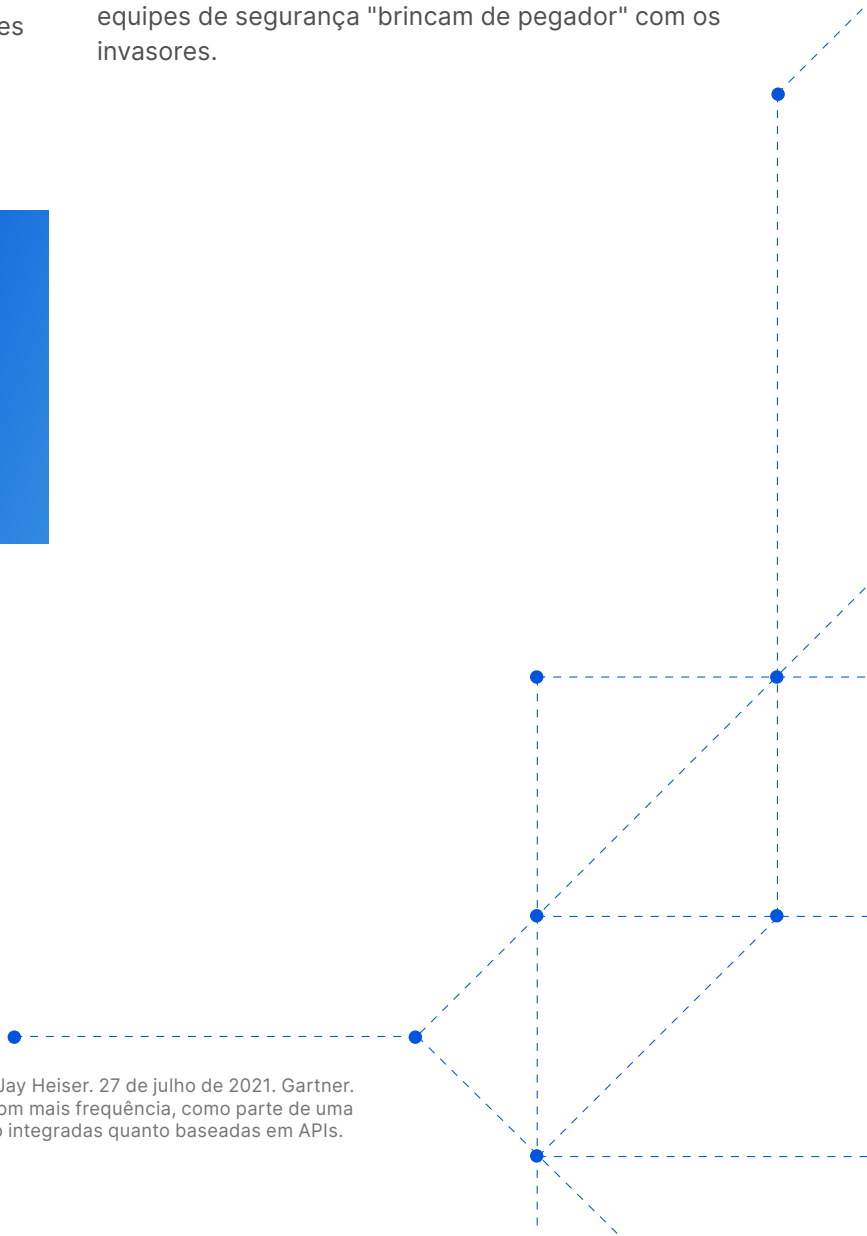
À medida que a adoção de SaaS aumenta, também aumenta a superfície de ataque que as organizações precisam proteger. Em vez de um único banco de dados contendo dados importantes, os dados agora se encontram dispersos entre aplicativos que são gerenciados por terceiros (por exemplo, Dropbox, Google Drive etc.) — independentemente de você ter ou não criado sandboxes para seu uso corporativo.

Embora ajudem a proteger os dados da empresa e os usuários dentro dos aplicativos de SaaS, ainda assim os CASBs não constituem uma solução perfeita para captar todas as ameaças. Devido ao fato de o volume de dados importantes sendo processados com o uso de aplicativos SaaS ter aumentado, os invasores visam cada vez mais esses aplicativos com o objetivo de realizar violações de dados e outras ameaças. Simples inadequações de configuração e erros de usuários também podem deixar uma porta aberta para esses ataques:

A Gartner prevê que mais de 99% das violações em nuvem até 2025 serão provocadas por configurações inadequadas e erros cometidos por usuários que poderiam ter sido evitados.[4]

Quando se trata de prever e remediar configurações de usuários inadequadas e ataques modernos a SaaS, os CASBs ainda costumam falhar. Para solucionar isso, alguns fornecedores começaram a oferecer serviços de gerenciamento de posturas de segurança de SaaS ou em nuvem (CSPM or SSPM[5]), projetados para rastrear erros de configuração e conformidade no painel de controle. No entanto, isso não ocorre de maneira ampla, deixando muitas organizações sem os recursos de detecção e remediação necessários.

Além disso, algumas ofertas de CASB não conseguem identificar as violações de dados antes que ocorram, resultando em um aumento dos custos de remediação e da perda de dados à medida que as equipes de segurança "brincam de pegador" com os invasores.



[4] Gartner, “Hype Cycle for Cloud Security, 2021". Analistas: Tom Croll, Jay Heiser. 27 de julho de 2021. Gartner.
[5] Esses serviços e recursos costumam ser oferecidos lado a lado ou, com mais frequência, como parte de uma oferta de produtos de CASB, fornecendo proteção de aplicativos tanto integradas quanto baseadas em APIs.

O problema com a implementação e integração do CASB

À medida que os fornecedores de SaaS reforçam a capacidade dos recursos de segurança incorporados oferecidos, dois grandes obstáculos permanecem: a integração e a visibilidade. Esses fornecedores tornam os dados acessíveis e fáceis de consumir, mas ainda deixam a cargo das organizações o ônus de consolidar os recursos de segurança de forma que sejam fáceis de administrar. Para as organizações que adotam diversas soluções pontuais, o rastreamento de ameaças nas várias plataformas se torna mais difícil quando essas soluções não foram projetadas para se integrar entre si e apresentam diferentes níveis de visibilidade.

Isso aumenta a complexidade do ambiente de aplicativos, de forma que até mesmo os ataques mais básicos se tornam mais difíceis de mitigar: tudo o que os invasores precisam fazer é identificar falhas das plataformas de segurança para realizar ataques sem serem detectados. Com um CASB, as organizações podem acessar seus produtos de segurança no mesmo lugar, o que lhes dá maior visibilidade e melhores recursos de mitigação em toda a sua pilha de segurança.

Mesmo assim, os CASBs constituem apenas uma das peças de uma estratégia de segurança SaaS mais ampla. Para abranger todo o panorama de SaaS, as organizações precisam agregar seus recursos de CASB com outras tecnologias Zero Trust sem adicionar uma complexidade desnecessária nem forçar as equipes de segurança a manter e configurar manualmente cada ferramenta. O controle bem-sucedido de SaaS em grande escala não pode ser um processo manual: a automação é um complemento necessário para as plataformas de gerenciamento de SaaS e ferramentas de CASB, permitindo que as organizações mitiguem com eficácia uma ampla gama de ameaças sem correr o risco de erros e configurações inadequadas de usuários e de exaurir suas equipes.

A evolução da segurança de e-mails

Como ocorreu com a maioria dos serviços de SaaS, a comunicação por e-mail como um aplicativo corporativo essencial para as organizações também evoluiu. Com a migração para a nuvem e o trabalho remoto, mais organizações estão se voltando para soluções de e-mail em nuvem dentro do Microsoft 365 e do Google Workspace — um percentual de até 70% das organizações em todo o mundo, de acordo com a Gartner.[6]

Consequentemente, o aplicativo de e-mail é um dos mais amplamente adotados entre as opções de SaaS, constituindo, também, uma das maiores superfícies de ataque, atraindo phishing, malware, falsificação, comprometimento de e-mails corporativos (BEC) e outras ameaças modernas.

No entanto, a proteção de e-mails contra os ataques pode constituir uma tarefa pesada e entediante para as equipes de segurança, especialmente considerando que os invasores continuam a empregar as mais sofisticadas táticas contra funcionários ingênuos. Para salvaguardar os usuários de dados contra essas ameaças, os chefes de segurança devem pensar em integrar o e-mail em sua plataforma de segurança de SaaS de forma a aumentar a visibilidade e proporcionar uma proteção simplificada e mais consistente.

Segurança SaaS 101: segurança de e-mails

A segurança de e-mails moderna abrange uma série de ferramentas, processos e técnicas de proteção de contas e conteúdo de e-mails contra ataques maliciosos e acesso não autorizado. Alguns dos tipos mais comuns de tecnologias de segurança de e-mails incluem os seguintes:

- **Gateways seguros de e-mail (SEG):** os SEGs processam e filtram o tráfego SMTP e requerem que as organizações alterem seu registro MX para que aponte para o seu agente de transferência de e-mails.
- **Segurança de e-mails na nuvem (CES):** a CES analisa o conteúdo de e-mails (por meio de APIs de acesso aos provedores de e-mail em nuvem) sem necessidade de alterar o registro MX (Observação: a Gartner se refere a essa categoria como "ICES", ou "CES integrada").
- **Relatórios e Conformidade da Autenticação de Mensagens Baseada em Domínio (DMARC):** o DMARC autentica os e-mails verificando uma Sender Policy Framework (SPF, estrutura de política de domínio de remetentes) e registros DKIM (E-mail Identificado por DomainKeys). Dentro desse sistema, os e-mails rejeitados pelas verificações de SPF ou DKIM são marcados como spam ou impedidos de chegar ao destinatário pretendido.
- **Proteção de Dados de E-mail (EDP):** as soluções de EDP utilizam criptografia para ajudar a evitar perdas acidentais de dados e acesso não autorizado ao conteúdo de e-mails.

---

[6] Gartner, “Market Guide for Email Security". Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de outubro de 2021. Gartner.

Entenda os desafios da segurança de e-mails moderna

Originalmente entregues por meio de plataformas de software no local, o e-mail está migrando progressivamente para sistemas de entrega nativos da nuvem. Várias organizações adotaram pacotes de produtividade ricos em recursos como o Microsoft 365 e o Google Workspace, que permitem que os usuários trabalhem e colaborem de forma mais eficaz.

Como o e-mail já vem sendo usado há um longo tempo, mesmo os usuários mais casuais estão cientes de algumas das ameaças mais prevalentes que podem encontrar ao utilizar e-mails, incluindo e-mails suspeitos, links maliciosos e muito mais. Como resultado, as estratégias dos invasores evoluíram de forma a tornar mais difícil a diferenciação entre as mensagens legítimas e maliciosas. Essas ameaças combinadas passam por vários canais de comunicação de forma a parecerem mais legítimas (por exemplo, vishing, smishing etc.) e costumam ser bem-sucedidas em suas tentativas de enganar os usuários e levá-los a fornecer informações confidenciais.

O aumento no uso de e-mails também deixa as organizações vulneráveis a violações: após ganhar acesso à conta de e-mail de uma pessoa, fica fácil para o invasor se mover lateralmente dentro de uma organização e comprometer ou roubar dados confidenciais. E, embora os provedores de e-mail em nuvem ofereçam recursos incorporados limitados, projetados para mitigar ameaças comuns como spam, malware e phishing, esses recursos são notoriamente fracos para proteger contra ataques de remetentes internos comprometidos se movimentando lateralmente de uma caixa de entrada para outra.

Para combater essas ameaças, as soluções de segurança de e-mails também estão evoluindo. As plataformas de e-mail nativas da nuvem oferecem um nível básico de recursos de segurança incorporados que podem lidar com spam e ataques de malware comuns.

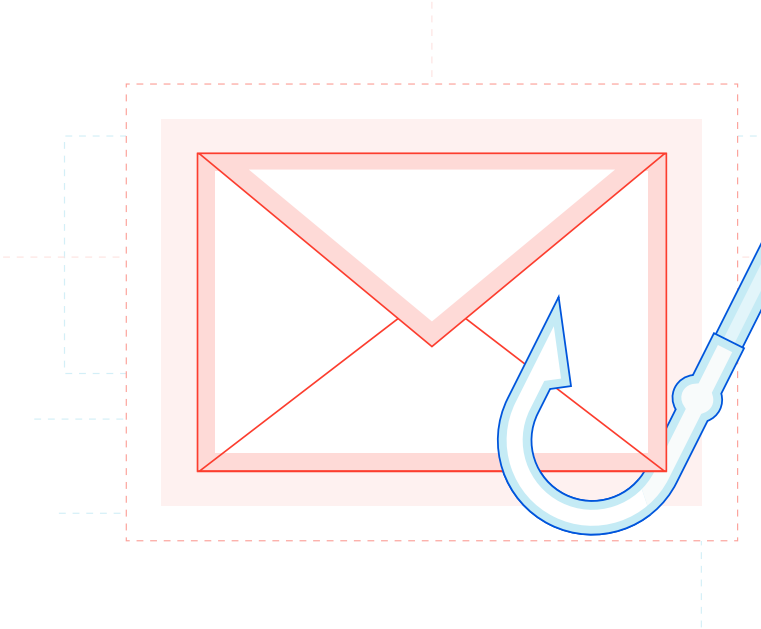
Até 2023, a Gartner estima que pelo menos 40% de todas as organizações irão se apoiar nessa proteção incorporada, em vez de adotar ferramentas separadas como o SEG.[7]

Muitas organizações optam por simplificar sua pilha de segurança de e-mails ignorando o SEG e, em vez disso, buscando ofertas de segurança que detenham ataques avançados de phishing e BEC e, ao mesmo tempo, se integrem estritamente com seu ambiente de e-mail na nuvem por meio de APIs.[8]

[7] Gartner, “Market Guide for Email Security". Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de outubro de 2021. Gartner. [8] Gartner, “Market Guide for Email Security".

O problema com a implementação e integração da segurança de e-mails

Embora permitam às organizações uma certa tranquilidade, esses recursos incorporados estão longe de serem suficientes para combater as ameaças modernas contra e-mails. Categorias inteiras de ataques — como spear phishing, BEC e muitas outras — requerem plataformas de segurança dedicadas que não são oferecidas pelos provedores de e-mails. Além disso, as soluções de segurança de e-mails obsoletas não são projetadas para escalar, combater desafios nativos da nuvem ou detectar ataques altamente direcionados.



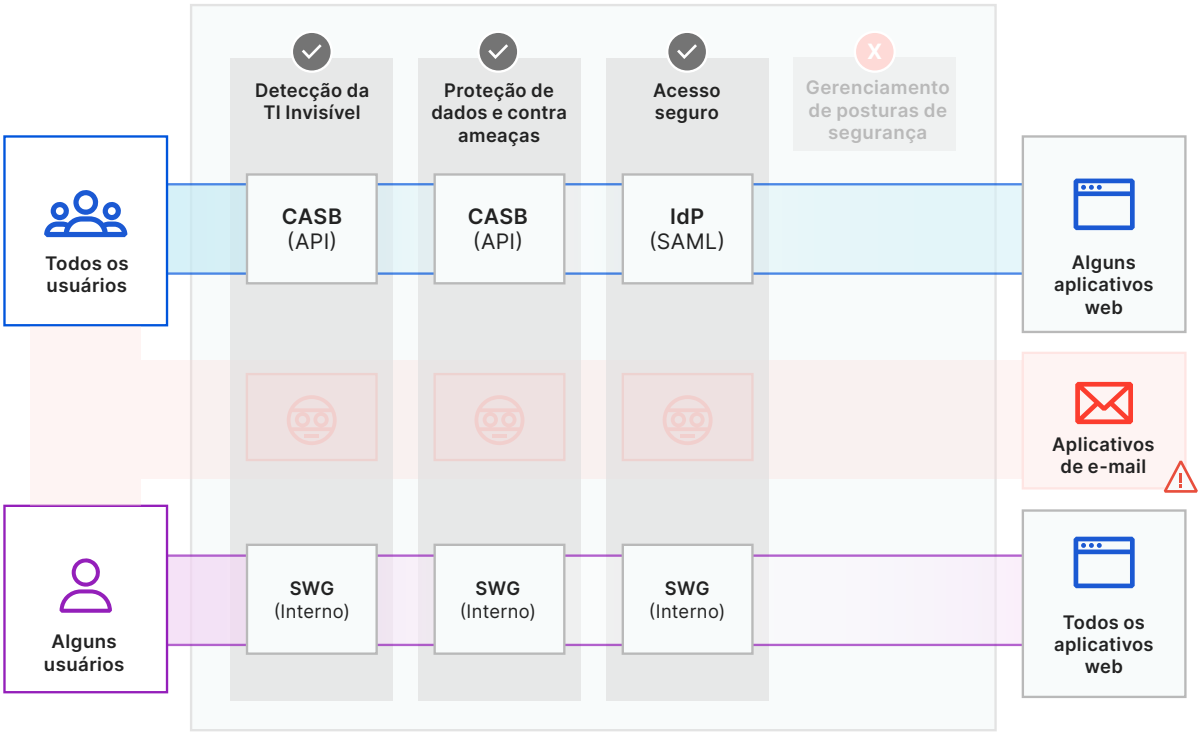
Mesmo quando selecionam ferramentas de segurança de e-mails que são projetadas para detectar ameaças modernas, as equipes de segurança podem ter que enfrentar problemas adicionais, como exigências complexas de configuração, processos demorados de implantação e desafios entediantes de manutenção de políticas. Por exemplo, os produtos de SEG são notoriamente difíceis de implantar contra ataques de e-mail, já que não é factível (nem escalável) manter uma lista cada vez mais longa de políticas para deter todas as variantes de ataques. A detecção avançada de ataques requer um uso de algoritmos em ampla escala que apenas serviços nativos da nuvem estão equipados para lidar.

Para proteger os sistemas de e-mail corporativos contra esses ataques sem sobrecarregar as equipes de segurança, sobrepor produtos de hardware obsoletos ou depender dos funcionários para detectar todas as mensagens maliciosas, as organizações precisam adotar uma abordagem Zero Trust que integre recursos de segurança de e-mail nativos da nuvem e reduza a confiança implícita em comunicações baseadas em e-mail.

Uma melhor abordagem da segurança de SaaS

Os aplicativos SaaS, das plataformas de comunicação aos sistemas de entrega de e-mails, constituem uma parcela considerável das operações de negócios da atualidade. Mas protegê-los contra ameaças cada vez mais complexas pode ser um pesadelo para as equipes de segurança, que costumam ficar encarregadas de tentar equilibrar numerosas ferramentas que não foram projetadas para se integrar nativamente entre si nem são capazes de proporcionar visibilidade de todo o panorama de SaaS de uma organização.

Segurança SaaS tradicional

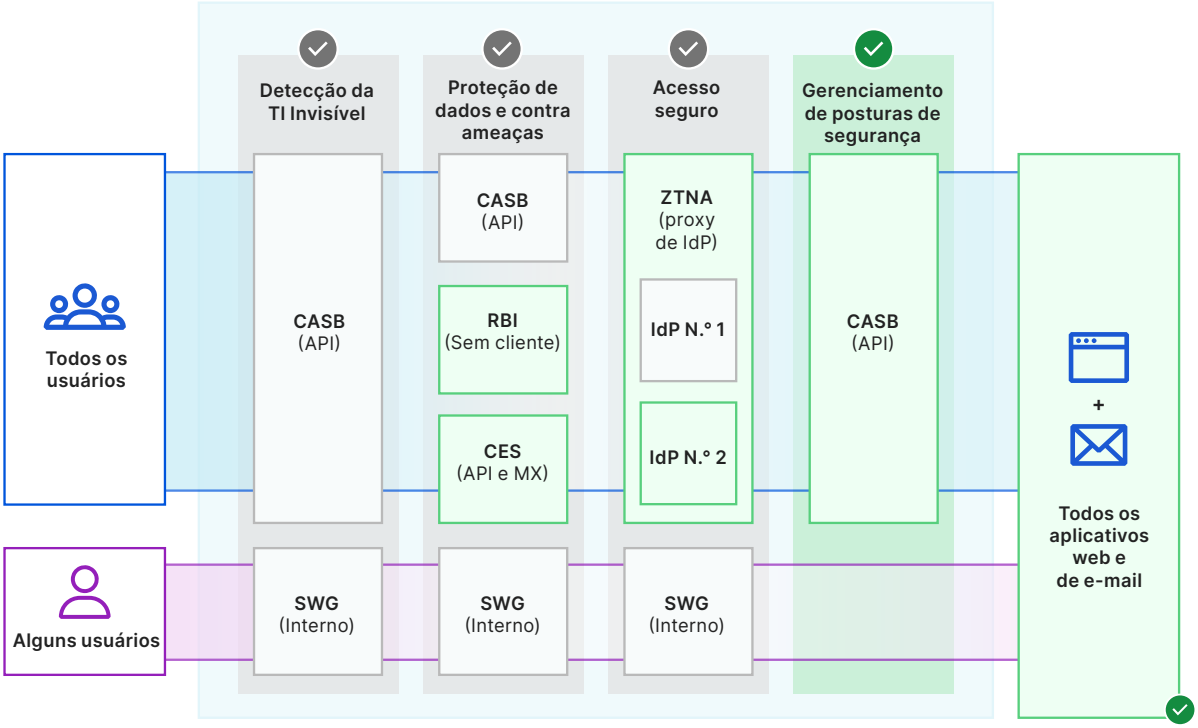


SWG = Gateway Seguro da Web | CASB = Agente de Segurança de Acesso à Nuvem | IdP = Provedor de Identidade

À medida que os fornecedores elaboravam ferramentas de segurança SaaS mais consistentes, as equipes de segurança e de TI eram encarregadas de combinar essas soluções, as melhores da categoria, para proteger seus dados e aplicativos. Isso costumava requerer um tempo e recursos internos consideráveis para implementar e gerenciar e, embora as soluções pontuais fossem capazes de abordar as ameaças em nível individual, não existia uma plataforma abrangente que fornecesse um suporte multifornecedor e visibilidade em toda a organização.

Muitas medidas de segurança SaaS tradicionais também costumavam falhar ao tentar estender suas proteções às plataformas de e-mail, deixando as organizações vulneráveis a ataques direcionados que replicavam fluxos de trabalho críticos para os negócios e também a invasores que se faziam passar por usuários e parceiros confiáveis e conseguiam contornar com facilidade os sistemas de classificação de e-mails e controles integrados existentes. Sem uma integração nativa entre essas soluções e sem visibilidade de todo o cenário de ameaças, a proteção dos aplicativos contra ameaças modernas deixava ainda mais lacunas para as equipes de segurança solucionarem.

Segurança SaaS moderna



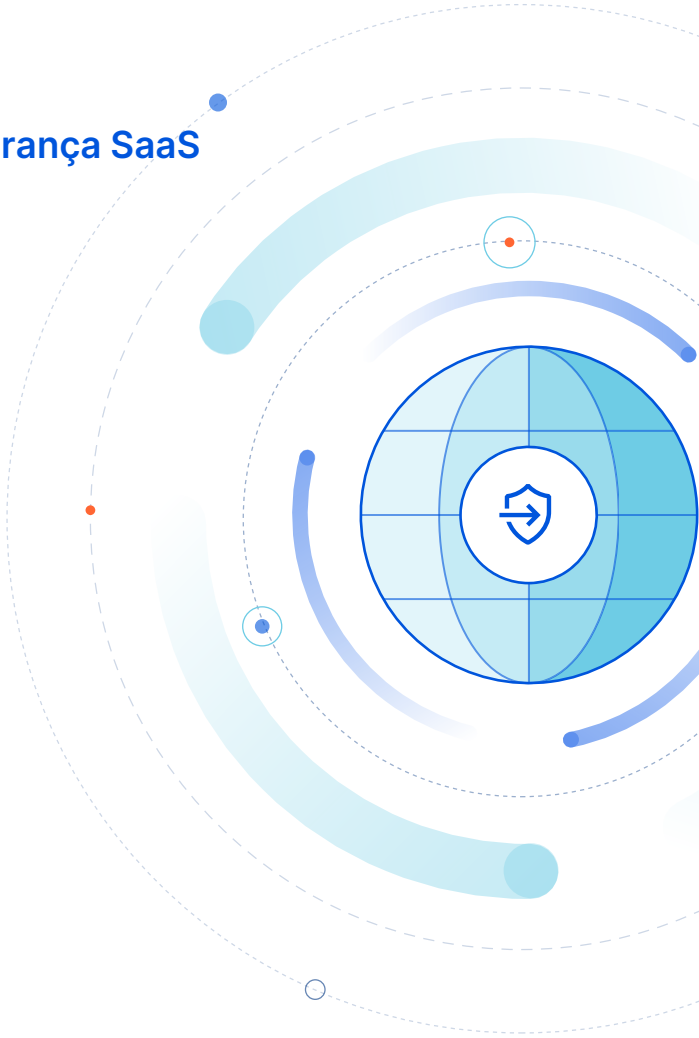
SWG = Gateway Seguro da Web | CASB = Agente de Segurança de Acesso à Nuvem | IdP = Provedor de Identidade | RBI = Isolamento do Navegador Remoto CES = Segurança de E-mail em Nuvem | ZTNA = Acesso à Rede Zero Trust

Para preencher as lacunas deixadas pelas soluções tradicionais de gerenciamento e segurança de SaaS, as organizações precisam de uma proteção contra ameaças moderna, que tenha sido projetada para proteger aplicativos e dados a partir de uma única plataforma nativa da internet. Um componente crítico dessa abordagem moderna é um gerenciamento consistente de posturas de segurança, que permita às equipes de segurança determinar melhor como os usuários devem acessar recursos cruciais, além de ganhar visibilidade e controle das ameaças internas e externas.

Em vez de requerer que as organizações operem ferramentas de soluções únicas para remediar ameaças individuais, a plataforma de segurança de SaaS pode verificar os aplicativos para detectar anomalias de configuração, permissões e compartilhamento e, em seguida, capacitar as equipes de segurança a gerenciar o acesso aos aplicativos, mitigar ataques aos e-mails, bloquear ameaças internas e o compartilhamento arriscado de dados e muito mais.

Essa abordagem não apenas fornece aos aplicativos SaaS uma proteção mais abrangente e mais consistente, como também capacita as organizações a pouparem tempo fazendo uma triagem de tickets, automatizando processos de segurança e se concentrando em iniciativas estratégicas, em vez de se preocupar com vazamento de dados, ataques, configurações manuais e manutenção.

Como aplicar a abordagem Zero Trust à segurança SaaS



Para desenvolver a abordagem certa da segurança de SaaS é preciso uma visão abrangente das ameaças modernas contra SaaS e nuvem, mas a responsabilidade de adaptar as soluções existentes às necessidades de uma organização pode ser pesada para as equipes de segurança e TI. Em vez de combater as ameaças em nível individual, ou de confiar em uma colcha de retalhos de ferramentas isoladas em silos, as organizações precisam de uma plataforma de segurança que seja simplificada, fácil de gerenciar e capaz de prever e mitigar as ameaças modernas.

Embora sejam componentes essenciais de uma estratégia de segurança SaaS, tanto o CASB quanto os recursos de segurança de e-mails em nuvem foram projetados para funcionar melhor dentro de uma arquitetura Zero Trust, na qual todas as peças de tecnologia funcionam melhor em conjunto do que funcionariam se estivessem isoladas. Quando implementada corretamente, essa organização em camadas também ajuda a aliviar problemas adjacentes ao eliminar lacunas de segurança, preservando a largura de banda da equipe de segurança e automatizando a vigilância de ameaças.

Como a Cloudflare protege seus aplicativos SaaS

A Cloudflare oferece o caminho mais fácil para a proteção de todo o seu panorama de SaaS, facultando às organizações o controle de como seus usuários acessam recursos críticos e da forma como mantêm esses recursos protegidos contra ataques externos e internos, além de monitorar e mitigar riscos em tempo real.

* Cadastre-se na nossa lista de espera de DLP

Proteja seus aplicativos SaaS com a Zero Trust da Cloudflare

Pata proteger os dados em trânsito, a Zero Trust da Cloudflare coloca os controles de acesso (ZTNA), o gateway (SWG) e o isolamento do navegador (RBI) na frente da nuvem e de aplicativos SaaS para apoiar e operar como uma arquitetura de implantação interna de CASB.

Para proteger os dados em repouso dentro dos aplicativos SaaS, integrações impulsionadas por APIs fáceis de configurar são utilizadas para verificar continuamente seus aplicativos de uso intensivo em busca de vulnerabilidades e possíveis ameaças.

Combine a segurança de e-mails da Area 1 da Cloudflare com a Zero Trust da Cloudflare

A segurança de e-mails da Area 1 da Cloudflare é um fornecedor ICES representativo que oferece maior flexibilidade às organizações, dependendo das respectivas necessidade de segurança de e-mails. Isso é feito com uma integração por meio de API que atua como um gateway para verificar, filtrar e isolar o tráfego de e-mails internamente por meio de alterações do registro MX.

A Area 1 rastreia a internet preventivamente para descobrir infraestruturas de ataque e campanhas de phishing, protegendo os clientes contra ataques de phishing dias antes de alcançarem as caixas de entrada dos destinatários.

Para saber mais sobre como a Cloudflare ajuda a proteger aplicativos SaaS, acesse https://www.cloudflare.com/products/zero-trust.

Fontes

1. Gartner, “Forecast Analysis: Information Security and Risk Management, Worldwide”. Analistas: Shailendra Upadhyay, Mark Driver, Christian Canales, Ruggero Contu, Lawrence Pingree, Elizabeth Kim, John A. Wheeler, Nat Smith, Rahul Yadav, Swati Rakheja, Dave Messett, Mark Wah, Shawn Eftink. 12 de agosto de 2021. Gartner.

2. Gartner, “Predicts 2022: Consolidated Security Platforms Are the Future”. Analistas: Charlie Winckless, Joerg Fritsch, Peter Firstbrook, Neil MacDonald, Brian Lowans. 1° de dezembro de 2021. Gartner.

4. Gartner, “Hype Cycle for Cloud Security, 2021”. Analistas: Tom Croll, Jay Heiser. 27 de julho de 2021. Gartner.

6. Gartner, “Market Guide for Email Security”. Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de outubro de 2021. Gartner.

7. Gartner, “Market Guide for Email Security”. Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de outubro de 2021. Gartner.

8. Gartner, “Market Guide for Email Security”. Analistas: Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer. 7 de outubro de 2021. Gartner.

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV:BDES-3303.2022JUN24