Resumo da Solução

Cinco Casos de Uso CASB que Você Deveria Conhecer

De Deena Thomchick, Diretora Geral de Gerenciamento de Produtos, Segurança na Nuvem

Ninguém quer uma ilha de segurança que esteja desconectada do resto de suas soluções. Esse documento detalha como você deve pensar para juntar as peças.

O cenário atual é uma corrida desenfreada. Funcionários e organizações adotam aplicativos e serviços na nuvem em um ritmo acelerado devido à produtividade, colaboração e conveniência que oferecem. E por que agiriam de forma diferente?

Se você tem um problema, provavelmente há um aplicativo na nuvem que pode resolvê-lo. Além disso, o movimento a nível corporativo que se distancia de licenças de software tradicionais para plataformas na nuvem como o Office 365, G Suite, Salesforce, etc., oferece o benefício adicional de um modelo financeiro de Opex ao invés de Capex para seus custos de software.

Mas nem tudo é um mar de rosas. Também existem riscos.

No último ano, as organizações, em média, descobriram que seus funcionários usavam 1.232 serviços na nuvem diferentes e a maioria desses aplicativos não estava adequada para uso corporativo. Para os aplicativos na nuvem autorizados que são monitorados, 20% dos arquivos na nuvem estavam em risco de exposição devido ao comportamento de compartilhamento de risco e muitos desses arquivos continham dados relacionados à conformidade, como PII, PCI e PHI. 47% das organizações identificaram comportamento de alto risco dos usuários e 71% dessas instâncias de comportamento de alto risco indicaram tentativas de exportar dados.

Neste cenário surgiram os Agentes de Segurança de Acesso à Nuvem (CASBs - Cloud Access Security Brokers), a categoria de segurança que mais cresce, de acordo com o Gartner. Os CASBs são projetados especificamente para descobrir e monitorar o uso de aplicativos na nuvem, fornecer proteção contra perda de dados (DLP - Data Loss Protection) para aplicativos na nuvem e proteger as organizações contra ameaças que usam aplicativos na nuvem.

Uma solução completa de CASB é uma boa ideia, mas o Gartner recomenda que as empresas adotem uma implantação independente de CASB. A recomendação é que as organizações planejem integrar seu CASB com sua infraestrutura de segurança e processos de SOC existentes.

Uma excelente ideia. Ninguém quer uma ilha de segurança que esteja desconectada do resto de suas soluções de segurança. Mas como você começa a juntar as peças?

Há cinco casos de uso de integração que podem aumentar drasticamente a eficácia de um CASB e, ao mesmo tempo, diminuir a complexidade do gerenciamento dos riscos associados ao uso de aplicativos e serviços na nuvem. Chamamos essa abordagem integrada de segurança na nuvem de CASB 2.0.

1 Caso de Uso

O acesso à na nuvem permite que os usuários estejam em praticamente qualquer lugar do mundo e ainda sejam produtivos. No modelo original de TI, proteger os dispositivos de um funcionário exigiria uma conexão que retornasse a um local centralizado.

Uma solução mais moderna aproveita os agentes de segurança de acesso baseados na nuvem e os métodos de autenticação de dois fatores, e assim permite que os usuários tragam seus sistemas prediletos para portabilidade, enquanto ainda fornece à equipe de segurança a capacidade de ver os dados e verificar os usuários que acessam esses dados.

2 Caso de Uso

Integre seu CASB à sua solução corporativa de DLP na nuvem. Seus dados em aplicativos são inspecionados na própria nuvem, com base nas mesmas políticas de DLP utilizadas para todos os outros locais onde você rastreia seus dados. Com essa abordagem, seu CASB é a conexão com todos os seus aplicativos e transações na nuvem, e usa um mecanismo de inspeção DLP que está na nuvem, mas o gerenciamento centralizado da solução corporativa de DLP é onde você controla as políticas de DLP e as ações de resposta para os dados na nuvem. Dessa forma, seus dados nunca saem da nuvem. E você pode aplicar as mesmas políticas de DLP e ações de resposta aos seus dados na nuvem que você já usa para dados nos endpoints, no datacenter ou na rede. Sua alternativa seria gerenciar dois sistemas DLP separados ou tentar gerenciar uma abordagem ICAP extremamente complicada. Sugerimos evitar isso ao máximo, a menos que você tenha muito tempo adicional em suas mãos.

3 Caso de Uso

Integre seu CASB com autenticação de usuário. Controle o acesso a aplicativos na nuvem, ao integrar seu CASB com soluções de autenticação multifator de usuário e Single Sign On (SSO). Em um nível básico, a integração com SSO e MFA ajuda seu CASB a garantir melhor segurança de acesso para seus aplicativos na nuvem.

Com modelos de integração comuns, isso funciona fundamentalmente para controlar o início da sessão de aplicativo na nuvem de um usuário. No entanto, se você tiver uma integração mais profunda entre o CASB e o MFA, onde o CASB pode enviar comandos ao seu MFA e receber respostas mesmo depois que uma sessão de nuvem for iniciada, sua segurança é aprimorada ao bloquear as atividades maliciosas na nuvem sem bloquear atividades legítimas na nuvem.

Nesse cenário, imagine que você tenha um usuário que já tenha sido autenticado no Office 365, mas de repente eles começam a carregar ou baixar muitos arquivos estranhos, ou acessem de uma localização incomum. O que sua solução de CASB pode fazer? Isoladamente, ela pode bloquear essa atividade anormal ou permitir que ocorra, mas com um MFA integrado pode exigir uma rodada adicional de autenticação no meio da sessão para garantir que esse seja realmente o usuário autorizado. Se o usuário concluir a autenticação, a ação poderá ser permitida, caso contrário, a ação será bloqueada. Dessa forma, ações legítimas são habilitadas enquanto ações acionadas por malware ou hackers são negadas.

4 Caso de Uso

Integre seu CASB com criptografia, DLP e autenticação do usuário. Proteja os dados e gerencie os direitos digitais para visualização de dados em aplicativos na nuvem como parte de uma solução que protege seus dados onde quer que estejam. Considere uma solução em que seus dados confidenciais sejam automaticamente criptografados com base em uma classificação DLP automática no momento em que um usuário envia os dados para uma conta na nuvem. Em seguida, qualquer usuário que deseje visualizar ou baixar esse arquivo deve passar uma verificação de autenticação do usuário para garantir que possua permissão para ver esses dados. E esse requisito de criptografia e autenticação permanece com o arquivo mesmo depois de ter sido baixado de uma conta na nuvem e enviado para outro usuário (colega, parceiro, fornecedor, cliente, etc.). Finalmente, sua solução acompanha quem tem acesso a esse arquivo em qualquer lugar e oferece a capacidade de revogar esse acesso em qualquer momento no futuro.

5 Caso de Uso

Integre seu CASB com proteção avançada contra ameaças. Impeça que ataques avançados de malware usem suas contas na nuvem, ao integrar o CASB com proteção contra ameaças de classe empresarial. Proteja suas contas na nuvem com o mesmo nível de proteção que você usa atualmente em seus endpoints para detectar e mitigar infecções de malware avançadas. Disponibilize a proteção avançada contra ameaças com sandbox na nuvem para detectar ameaças avançadas que podem tentar se espalhar através de uploads, downloads, sincronizações de contas e compartilhamentos de aplicativos na nuvem.

Nem todas as soluções de CASB oferecem atualmente todas essas opções de integração e nem todas as soluções de segurança corporativa podem suportar esse nível de integração CASB. As soluções da Symantec são projetadas para fornecer uma ciberdefesa integrada para as organizações que desejam otimizar o uso de soluções integradas. Aqui estão alguns links para ajudá-lo com mais informações:

Secure Web Gateway (SWG) for the Cloud Generation
CloudSOC Security for Cloud Apps – Securlets | Symantec
Symantec Shadow Data Report

Sobre Deena Thomchick

Deena é uma entusiasta de segurança e profissional de tecnologia com 25 anos de experiência, uma executiva sênior do grupo de produtos CASB da Symantec. Além de seu foco atual na segurança na nuvem, seu histórico inclui trabalho com criptografia, ATP, segurança de rede e segurança de endpoints.

Sobre a Symantec

A Symantec Corporation (NASDAQ: SYMC) é líder mundial em soluções de cibersegurança e ajuda organizações, governos e indivíduos a proteger seus dados mais importantes onde quer que estejam. Organizações em todo o mundo buscam a Symantec para soluções estratégicas e integradas para se defender contra ataques sofisticados em endpoints, nuvem e infraestrutura. Da mesma forma, uma comunidade global de mais de 50 milhões de pessoas e famílias dependem da suíte de produtos Norton e LifeLock da Symantec para proteger suas vidas digitais em casa e todos seus dispositivos. A Symantec opera uma das maiores redes civis de ciberinteligência do mundo, possibilitando a proteção contra as ameaças mais avançadas. Para mais informações, visite **www.symantec.com** ou conecte-se conosco no **Facebook**, **Twitter** e **LinkedIn**.

Symantec™ 350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**

SYMC_ 5_CASB_Use_Cases_You_Should_Know_v1a