Relatório de Ameaças à Segurança na Nuvem (CSTR)
Volume 1 | Junho 2019

Adaptando-se à Nova Realidade da Evolução de Ameaças na Nuvem

Sumário Executivo

Symantec™

Introdução

Embora o uso de aplicativos de Software como Serviço (SaaS) esteja crescendo e as cargas de trabalho migrem cada vez mais para plataformas IaaS, como AWS e Azure, ainda persiste o uso de nuvens privadas, bem como o armazenamento de dados e aplicativos. O ambiente de TI híbrido desafia os paradigmas de segurança atuais, acrescentando complexidade e aumentando o esforço das organizações para acompanhar essa tendência.

De março a junho de 2019, a Symantec entrevistou 1.250 líderes de segurança em todo o mundo para entender o cenário de segurança na nuvem, o escopo e uso de dados de Shadow IT, e avaliar a maturidade das práticas de segurança à medida que as empresas migram para a nuvem. Em comparação com dados de telemetria agregados e de fontes de dados anonimizados da Symantec, o que encontramos foi revelador e muitas vezes extremamente alarmante.

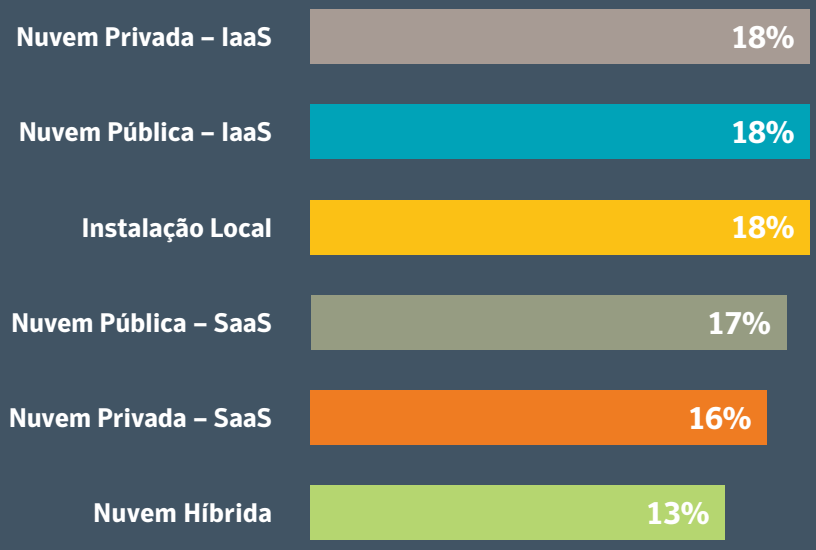
Symantec

Seção

01

O Momento Crítico Chegou. Poucos Estão Prontos.

Uma das maiores revelações de nossa pesquisa é que as empresas estão armazenando dados em mais de um ambiente.



53%
AVANÇAM COM A IMPLEMENTAÇÃO DA NUVEM

69%
ARMAZENAM ALGUNS DADOS LOCALMENTE

A Visibilidade é Nebulosa

A maioria das organizações de TI e Operações de Segurança (SecOps) não sabe que seu portfólio na nuvem está crescendo rapidamente ou o que está sendo usado.

Em média, as organizações relatam que mais da metade (53%) de sua carga de trabalho migrou à nuvem. No entanto, apenas uma pequena minoria (3%) transferiu todas elas.

A visibilidade dessas cargas de trabalho é um problema. A grande maioria dos entrevistados (93%) relatam problemas em controlá-las.

452

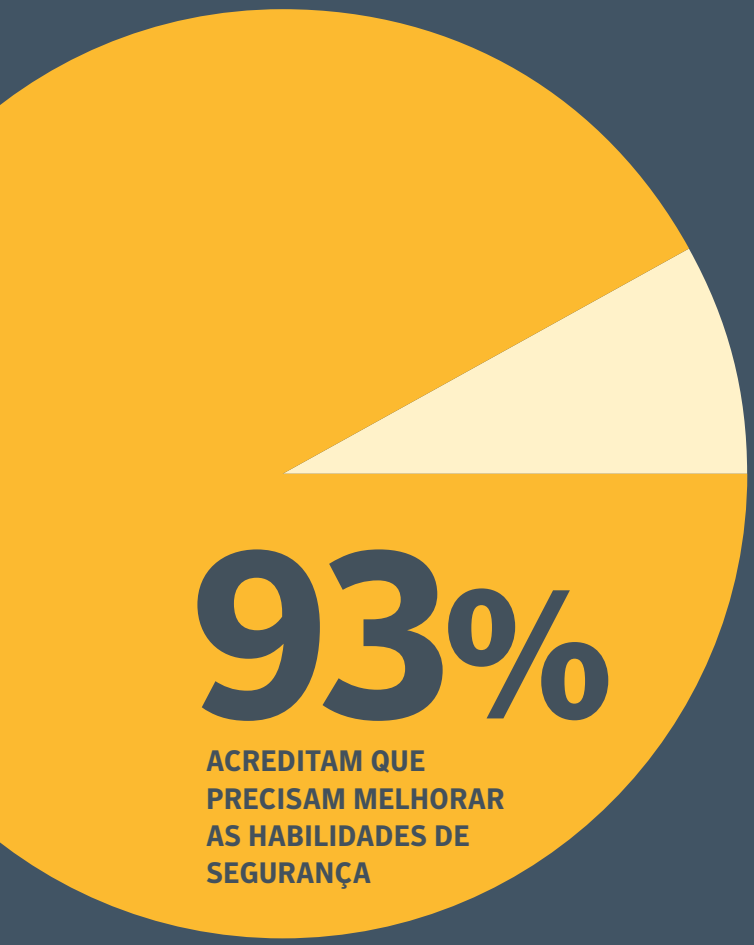
PERCEPÇÃO

1807

APLICATIVOS NA NUVEM

REALIDADE

Segundo os entrevistados, uma organização comum acredita que seus colaboradores estão usando 452 aplicativos na nuvem. No entanto, de acordo com os dados da própria Symantec, o número real é de 1.807 aplicativos de Shadow IT em uso por organização, número quase quatro vezes maior.



93%

ACREDITAM QUE PRECISAM MELHORAR AS HABILIDADES DE SEGURANÇA

A Capacidade está Maximizada

Dos entrevistados, 49% confirmaram que a força de trabalho de segurança na nuvem é inadequada para lidar com todos os alertas recebidos.

A falta de pessoal qualificado e de habilidades de segurança é o principal culpado: a maioria disse que precisa melhorar as habilidades de segurança na nuvem (92%), enquanto 84% confirmaram que precisavam adicionar pessoas na equipe para eliminar a deficiência.

Práticas Imaturas Prevalecem

A maturidade da maioria das organizações na nuvem não avança tão rapidamente quanto a expansão da implementação de novos aplicativos - um obstáculo confirmado por mais da metade (54%) dos entrevistados. Setenta e três por cento (73%) culpam práticas de segurança imaturas, incluindo o uso de contas pessoais, além da falta de serviços de Autenticação Multifator (MFA) ou Prevenção de Perda de Dados (DLP), por pelo menos um incidente na nuvem. Apenas 1 em cada 10 entrevistados disseram que conseguem analisar adequadamente o tráfego na nuvem.

73%

CULPAM PRÁTICAS DE SEGURANÇA IMATURAS POR PELO MENOS UM INCIDENTE NA NUVEM

28%

DOS EMPREGADOS SE ENVOLVEM EM ALGUM TIPO DE COMPORTAMENTO DE ALTO RISCO

TO ENHANCE CLOUD SECURITY SKILLS

O Comportamento dos Colaboradores Representa Riscos

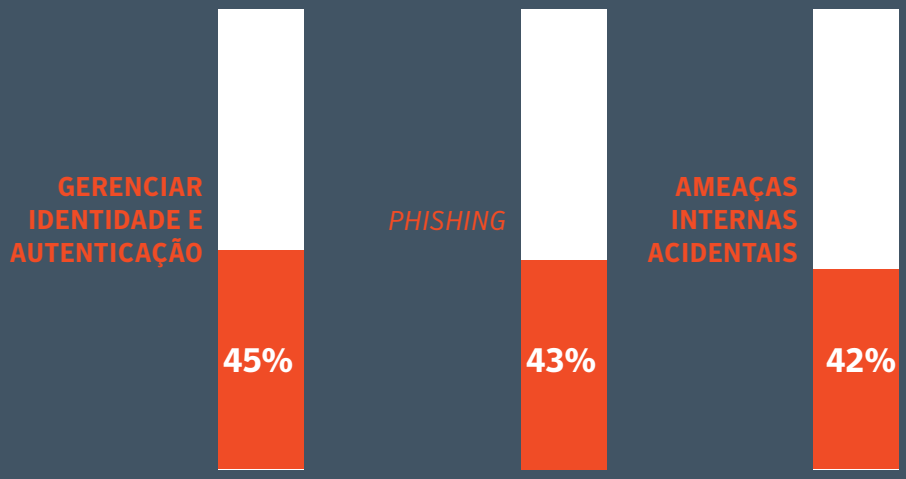
As empresas subestimam o impacto do uso indevido de aplicativos na nuvem por colaboradores: 28% deles se envolvem em algum tipo de comportamento de alto risco.

Seção

02

Principais Ameaças

As três maiores categorias de ameaças emergentes no futuro, de acordo com os entrevistados, são:



De acordo com os dados internos da Symantec, de quase 33.000 aplicativos avaliados pelo Business Readiness Rating - BRR, que é baseada em mais de 80 atributos de segurança, menos de 1% dos aplicativos têm esses requisitos integrados necessários para o uso corporativo constante, enquanto 39% não são adequados. A maioria exibe apenas alguns controles de segurança necessários.

Os Dados de Shadow se propagam nos serviços SaaS autorizados e não autorizados. Mais da metade dos entrevistados (52%) disseram que o aumento do uso de aplicativos na nuvem para armazenar e compartilhar dados corporativos confidenciais era um problema. A grande maioria (93%) informou que lida com usuários que compartilham arquivos na nuvem contendo dados confidenciais e relacionados à conformidade, enquanto, em média, 35% dos arquivos na nuvem são compartilhados em excesso.

Ainda mais preocupantes são os efeitos que podem ocorrer com uma abordagem negligente nos controles de segurança. A pesquisa relata que 68% dos entrevistados viram evidências diretas ou prováveis de que seus dados tinham sido colocados à venda na Dark Web.

Riscos de Servidores Mal Configurados, *Malware* e Acesso Não Autorizado

Os entrevistados da pesquisa dizem que quase dois terços dos incidentes de segurança investigados nos últimos doze meses ocorreram no nível da nuvem, e quase um terço dos incidentes foram classificados como somente na nuvem.

Ameaças Internas

Os incidentes na nuvem que resultam de ameaças de fontes internas - intencionais, inadvertidas ou através de credenciais comprometidas - são uma grande preocupação para 48% dos entrevistados. Além disso, 21% deles disseram que o problema estava aumentando em intensidade.

Práticas de segurança imaturas geram falhas sérias e maior volume de incidentes com ameaças de fontes internas. A pesquisa da Symantec identificou que 65% das organizações negligenciam a implementação de Autenticação Multifator (MFA) como parte da configuração de IaaS e 80% não usam criptografia.

65%

NÃO IMPLEMENTAM AUTENTICAÇÃO MULTIFATOR COMO PARTE DA CONFIGURAÇÃO DE IAAS

Cibercriminosos

A pesquisa da Symantec mostra que 16% do tráfego de *outbound web* pode vir de servidores comprometidos, direcionados a domínios conhecidos de comando e controle de bots ou outros ataques de *malware*. Os resultados da pesquisa confirmam isso, com as organizações entrevistadas classificando uma média de 11 visitas a websites por semana como de alto risco e 11 como maliciosas. Embora os números não chamem a atenção imediatamente, se fizermos as contas, os resultados somam cerca de 572 visitas de alto risco ou maliciosas a websites, o que aumenta significativamente a exposição corporativa.

Os dispositivos da Internet das Coisas (IoT) estão se tornando rapidamente outro importante vetor de ataque. De acordo com os entrevistados, o número de dispositivos IoT que causaram incidentes de IaaS cresceu para sete em cada dez organizações no ano passado.

572

VISITAS DE ALTO RISCO OU MALICIOSAS A WEBSITES POR ANO

Seção

03

Melhores Práticas para Desenvolver a Maturidade da Segurança na Nuvem

Mais da metade dos entrevistados confirmou que suas práticas de segurança na nuvem não eram maduras o suficiente para atender às demandas do uso crescente de aplicativos na nuvem e quase três quartos afirmaram ter sofrido um incidente de segurança na infraestrutura baseada na nuvem devido a essa imaturidade. Os dados próprios da Symantec confirmam que 85% dos clientes não estão usando as melhores práticas do Centro de Segurança da Internet (CIS).

As empresas que continuam a se envolver ou a acelerar a adoção de serviços na nuvem sem um plano para amadurecer suas práticas de segurança o fazem por sua própria conta e risco. As organizações devem considerar essas etapas principais para reforçar sua postura de segurança na nuvem:

Desenvolver uma Estratégia de Governança com Suporte de um Centro de Excelência na Nuvem (CCoE)

Adotar um Modelo de Zero Trust

Promover a responsabilidade compartilhada

Aproveitar automação e inteligência artificial sempre que possível

Seção

04

Conclusão
Organizações Subestimam seus Riscos na Nuvem

A heterogeneidade do ambiente empresarial moderno, abrangendo diversas plataformas na nuvem e instaladas localmente, adicionou um conjunto mais amplo de vulnerabilidades e vetores de ataque. As enormes falhas de visibilidade deixam as organizações sem saber o volume e a localização de dados e cargas de trabalho, dificultando a identificação e a mitigação dos riscos de segurança crescentes.

Muitas empresas não reconhecem a falha de percepção na segurança da nuvem e amplamente subestimam as ameaças atuais, ficando vulneráveis a comprometimentos de contas e exposições de dados que representam riscos financeiros e de reputação substanciais. O investimento em plataformas de cibersegurança para a nuvem que otimizam a automação e a inteligência artificial para complementar recursos humanos limitados é uma forma clara de aprimorar as defesas e aplicar os princípios de governança de dados. Além da tecnologia, é hora de recalibrar a cultura e adotar as melhores práticas de segurança no nível de recursos humanos - o que não é fácil, considerando todos os desafios do gerenciamento de mudanças. É a combinação de ambos que garantirá que a empresa esteja suficientemente protegida hoje e, mais importante, para o amanhã, quando ninguém realmente sabe o que esperar do futuro.

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.

Sede Mundial da Symantec
350 Ellis Street
Mountain View, CA 94043
Estados Unidos da América
+1 650 527–8000
+1 800 721–3934

Para escritórios regionais e números de contato específicos, por favor visite nosso website.
Para falar com um Especialista de Produto nos EUA, ligue grátis 1 (800) 745 6054.

Symantec.com

Symantec™