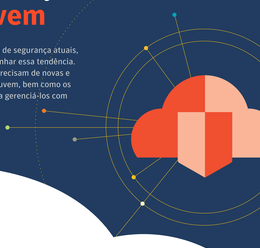
Symantec.

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

A migração atual para a nuvem desafia os paradigmas de segurança atuais, aumentando o esforço das organizações para acompanhar essa tendência. Para manter a visibilidade e o controle, as empresas precisam de novas e automatizadas soluções de segurança baseadas em nuvem, bem como os conjuntos de habilidades e processos necessários para gerenciá-los com eficiência.

Você pode fazer o download do relatório completo aqui



A Visibilidade é Nebulosa

De acordo com 1.250 líderes de segurança entrevistados pela Symantec em todo o mundo, 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.

452 PERCEPÇÃO

1807 APLICATIVOS NA NUVEM

REALIDADE

Maior Complexidade

A nuvem agora É o centro dos negócios

É na nuvem que as cargas de trabalho, dados e funções de negócios de missão crítica ocorrem atualmente. A segurança deve acompanhar.

53%

DE TODA CARGA DE TRABALHO PROCESSADA MIGROU À NUVEM.

A segurança não consegue acompanhar

A adoção da nuvem segue rápido demais e as empresas têm dificuldades para gerenciar o aumento da complexidade e perda de controle.

54%

CONCORDAM QUE A MATURIDADE DE SEGURANÇA NA NUVEM DE SUA ORGANIZAÇÃO NÃO É CAPAZ DE ACOMPANHAR A RÁPIDA EXPANSÃO DOS NOVOS APLICATIVOS NA NUVEM.

Visibilidade limitada

A complexidade como a TI é implementada (nuvem pública, privada, híbrida e instalações locais) cria problemas de visibilidade.

93%

RELATAM PROBLEMAS EM CONTROLAR TODAS AS CARGAS DE TRABALHO NA NUVEM.

Perda de controle

A nuvem facilita a perda de controle dos dados.

93%

TÊM PROBLEMAS RELACIONADOS AO COMPARTILHAMENTO EXCESSIVO DE ARQUIVOS QUE CONTÊM DADOS CONFIDENCIAIS NA NUVEM.

Ameaças Inesperadas

Aumento de movimentos laterais e ataques através de ambientes na nuvem

As empresas geralmente subestimam a escala e a complexidade das ameaças na nuvem. A percepção geral é de que violações de dados, ataques de DDOS e injeções de *malware* na nuvem são os incidentes mais comuns.

64%

DOS INCIDENTES DE SEGURANÇA NA NUVEM OCORREM DEVIDO AO ACESSO NÃO AUTORIZADO (PORTA ABERTA PARA MOVIMENTO LATERAL), DE ACORDO COM OS DADOS DA SYMANTEC.

Ameaças internas

Aqueles que estão mais próximos da organização (fontes internas e de confiança com acesso privilegiado a dados protegidos) representam alguns dos maiores riscos.

#3

AMEAÇA ACIDENTAL DE FONTES INTERNAS É TERCEIRA NA LISTA DE AMEAÇAS À INFRAESTRUTURA DA NUVEM

Dados à venda

Há evidências significativas de dados à venda na Dark Web.

68%

OBSERVARAM EVIDÊNCIAS DIRETAS OU PROVÁVEIS QUE SEUS DADOS TINHAM SIDO COLOCADOS À VENDA. TRINTA E UM POR CENTO (31%) NÃO ACREDITAM QUE SEUS DADOS CORRAM QUALQUER RISCO.

Segurança Imatura

Autenticação Multifator

Práticas de segurança imaturas geram maior volume de incidentes com ameaças de fontes internas.

65%

NEGLIGENCIAM A IMPLEMENTAÇÃO DE AUTENTICAÇÃO MULTIFATOR (MFA) COMO PARTE DA CONFIGURAÇÃO DO IAAS E 80% NÃO USAM CRIPTOGRAFIA, DE ACORDO COM OS DADOS DA SYMANTEC.

Cultura e comportamento

enfrentam dificuldades para acompanhar a mudança para a nuvem.

85%

DOS CLIENTES NÃO UTILIZAM AS MELHORES PRÁTICAS DO CENTRO DE SEGURANÇA DA INTERNET (CIS), SEGUNDO DADOS INTERNOS DA SYMANTEC.

Higiene deficiente de senhas

é sintomática do comportamento geral de segurança negligente.

#1

SENHAS FRACAS (37%) E HIGIENE DEFICIENTE DE SENHAS (34%) ESTÃO NO TOPO DA LISTA DE COMPORTAMENTOS PREJUDICIAIS.

MELHORES PRÁTICAS PARA

Desenvolver a Maturidade da 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

Saiba mais sobre a constante mudança no cenário de segurança na nuvem

Faça o Download do Relatório de Ameaças na Nuvem

Symantec.