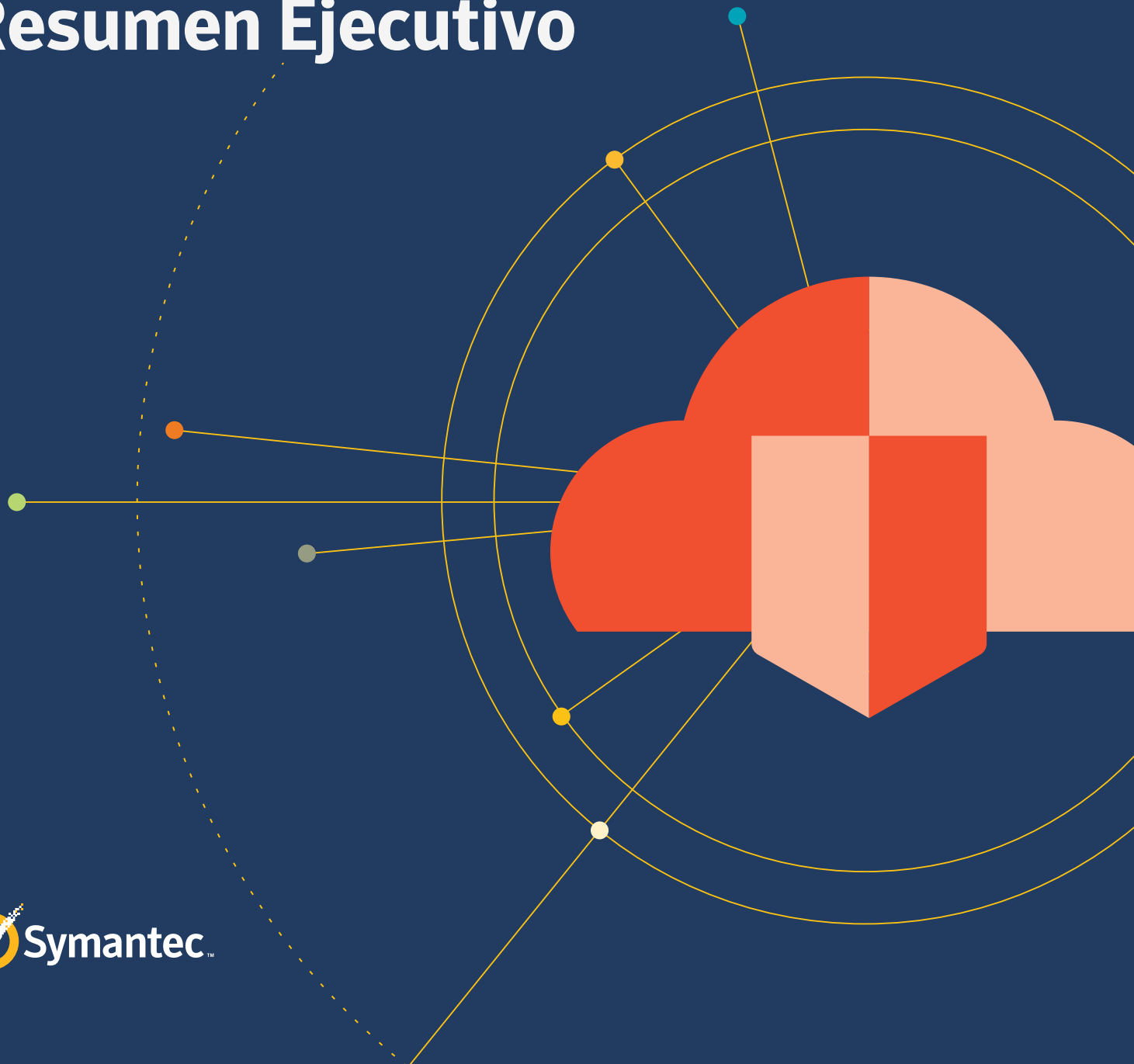
Informe sobre las Amenazas para la Seguridad en la Nube (CSTR)
Volumen 1 | Junio 2019

Adáptese a la Nueva Realidad en Evolución de las Amenazas en la Nube

Resumen Ejecutivo



Symantec™

Introducción

Si bien el uso de aplicaciones de software como servicio (SaaS) está proliferando, y las cargas de trabajo están migrando cada vez más a las plataformas IaaS como AWS y Azure, persisten las aplicaciones locales, el almacenamiento y las nubes privadas. El entorno de TI híbrido resultante está desafiando los paradigmas de seguridad existentes, creando complejidad y aumentando el esfuerzo de las organizaciones para acompañar esta tendencia.

Symantec encuestó a 1.250 líderes de seguridad en todo el mundo en el otoño de 2019 para comprender el cambiante panorama de la seguridad en la nube, el alcance de Shadow IT y el uso de Datos de Shadow IT, y para evaluar la madurez de las prácticas de seguridad a medida que las empresas migran a la nube. Comparado con datos de telemetría agregados y anónimos de las fuentes de datos de Symantec, lo que encontramos fue revelador y bastante alarmante.

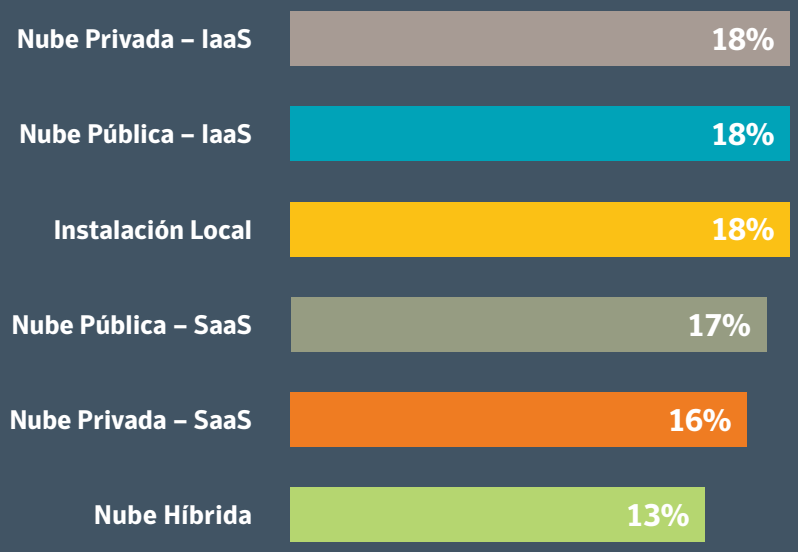
Symantec

Sección

01

El Momento Crítico Llegó. Pocos Están Listos.

Una de las conclusiones más importantes de nuestra encuesta externa es que las empresas almacenan datos en más de un entorno.



53%
AVANZAN EN LA IMPLEMENTACIÓN DE LA NUBE

69%
ALMACENAN ALGUNOS DATOS LOCALMENTE

La Visibilidad está Nublada

La mayoría de las organizaciones de TI y Operaciones de Seguridad no sabe qué tan rápido está creciendo su portafolio en la nube o lo que se está utilizando.

La mayoría de las cargas de trabajo también se ha desplazado a la nube. En promedio, las organizaciones informan que más de la mitad (53 %) de su carga de trabajo ha migrado a la nube. Sin embargo, solo una pequeña minoría (3 %) ha transferido todas sus cargas de trabajo a una plataforma en la nube.

La visibilidad de estas cargas de trabajo en la nube es un problema. Una abrumadora mayoría de los encuestados (93 %) reporta problemas para mantener un registro de todas las cargas de trabajo en la nube.

452

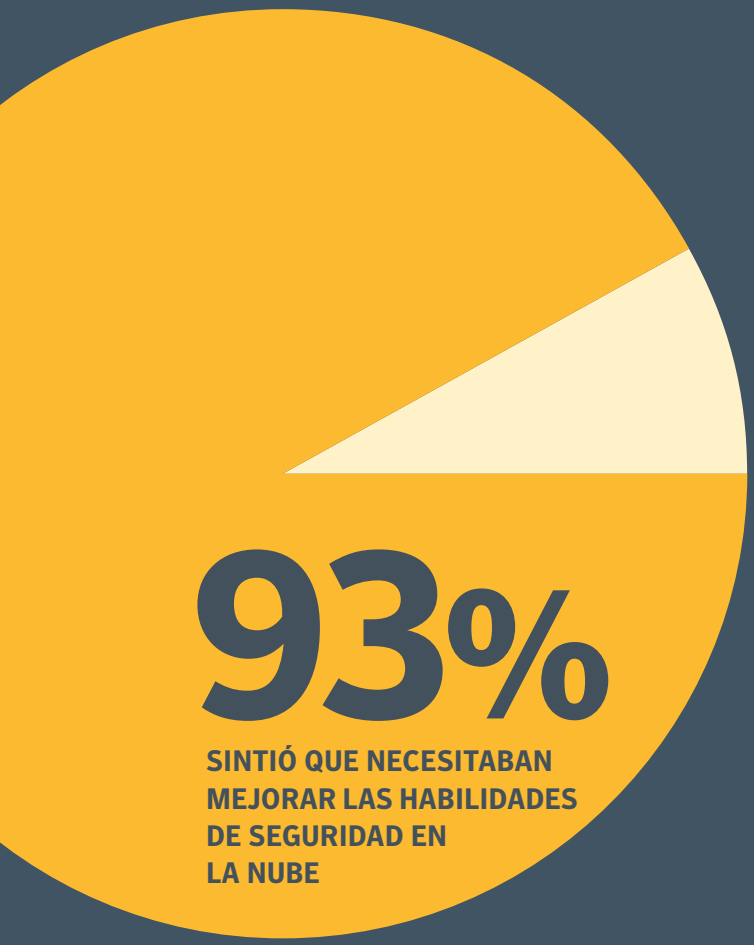
PERCEPCIÓN

1807

APLICACIONES EN LA NUBE

REALIDAD

Según los encuestados, la organización promedio cree que sus empleados utilizan 452 aplicaciones en la nube. Sin embargo, según los datos propios de Symantec, la cantidad real de aplicaciones de Shadow IT en uso por organización es casi cuatro veces más grande, de 1.807.



93%

SINTIÓ QUE NECESITABAN MEJORAR LAS HABILIDADES DE SEGURIDAD EN LA NUBE

La Capacidad está Sobrecargada

El cuarenta y nueve por ciento (49 %) de los encuestados confirmaron que su personal de seguridad en la nube es inadecuado para hacer frente a todas las alertas entrantes.

La falta de personal de seguridad y de habilidades es el principal culpable: la mayoría de los encuestados ha dicho que necesitan mejorar las habilidades de seguridad en la nube (92 %), mientras que un 84 % confirmó que necesitaban agregar personal para eliminar la brecha.

Prácticas Inmaduras Prevalecen

La madurez en la nube de la mayoría de las organizaciones no está avanzando tan rápidamente como la expansión de las nuevas aplicaciones en la nube que se están implementando, un obstáculo confirmado por más de la mitad (54 %) de los encuestados en la encuesta externa. El setenta y tres por ciento (73 %) culpa a las prácticas de seguridad inmaduras, incluido el uso de cuentas personales y la falta de servicios de autenticación multifactor (MFA) o de prevención de pérdida de datos (DLP), por lo menos por un incidente en la nube. Solo 1 de cada 10 encuestados dice que puede analizar adecuadamente el tráfico de la nube.

73%

CULPA A LAS PRÁCTICAS DE SEGURIDAD INMADURAS PARA POR LO MENOS UN INCIDENTE EN LA NUBE

28%

DE LOS EMPLEADOS SE INVOLUCRA EN ALGUNA CLASE DE COMPORTAMIENTO DE ALTO RIESGO

El Comportamiento de los Empleados Presenta Riesgos

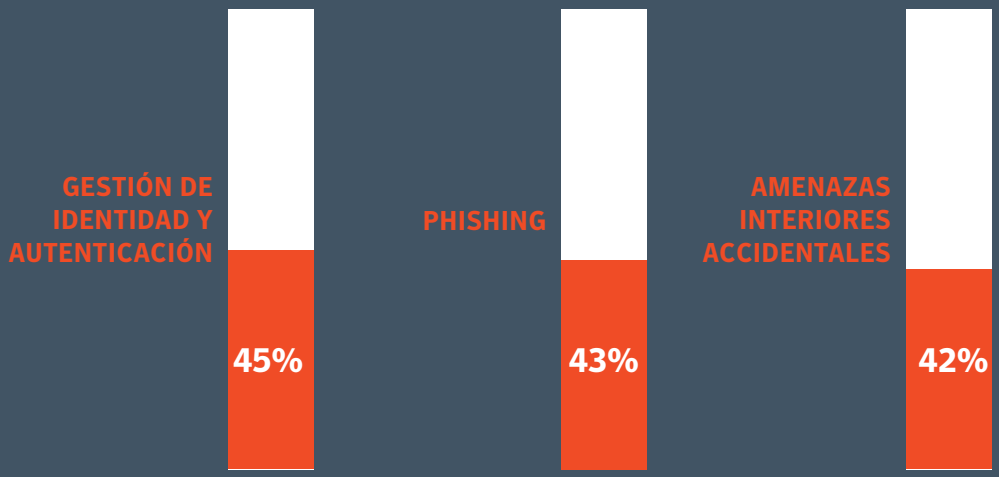
Las empresas subestiman el impacto en la seguridad del mal uso que hacen los empleados de las aplicaciones en la nube. La encuesta externa estima que 28 % de los empleados se involucra en algún tipo de comportamiento de alto riesgo. La investigación de Symantec nuevamente ilustra cómo la realidad supera las percepciones de la encuesta: 85 % de las organizaciones más grandes (más de 1.000 empleados) informaron sobre algunos usuarios de alto riesgo, y 30 % de ellos tenía 100 o más usuarios de alto riesgo.

Sección

02

Principales Amenazas

Las tres categorías de amenazas más elevadas que surgen en el futuro, según los encuestados externos, son:



De acuerdo con los datos internos de Symantec, de las casi 33.000 aplicaciones evaluadas por Business Readiness Rating (BRR), que se basa en más de 80 atributos de seguridad, menos de 1 % tiene la seguridad incorporada necesaria para el uso comercial constante, mientras que un 39 % no es adecuada en absoluto para el uso comercial. La mayoría exhibe sólo algunos controles de seguridad necesarios.

Los Datos de Shadow están proliferando dentro de los servicios SaaS autorizados y no autorizados. Más de la mitad de los encuestados externos (52 %) dijo que era un problema el mayor uso de aplicaciones en la nube para almacenar y compartir datos corporativos confidenciales. La gran mayoría (93 %) dijo que lidian con los usuarios que comparten archivos de la nube que contienen datos confidenciales y relacionados con el cumplimiento, mientras que en promedio un 35 % de los archivos de la nube se comparte de forma excesiva.

Más preocupantes son los efectos que pueden ocurrir a partir de este enfoque negligente de los controles de seguridad. La encuesta externa informa que el 68 % de los encuestados ha observado evidencias directas o probables de que sus datos estaban a la venta en la Web Oscura.

Riesgos de Servidores Mal Configurados, Malware y Acceso No Autorizado

Los encuestados dicen que casi dos tercios de los incidentes de seguridad investigados en los últimos doce meses se han producido a nivel de la nube, y casi un tercio de todos los incidentes se han clasificado como solamente en la nube.

Amenazas Internas

Los incidentes en la nube que resultan de amenazas de fuentes internas, ya sea intencional, involuntario o mediante credenciales comprometidas, son una preocupación importante para un 48 % de los encuestados. Así mismo, un 21 % de los encuestados dijo que el problema estaba aumentando en intensidad.

Las prácticas de seguridad inmaduras están creando brechas serias e impulsan incidentes más altos de amenazas internas. La investigación de Symantec encontró que un 65 % de las organizaciones se niegan a implementar la autenticación de múltiples factores (MFA) como parte de la configuración de IaaS y un 80 % no utiliza cifrado.

65%

NO DESPLEGA LA AUTENTICACIÓN MULTIFACTOR COMO PARTE DE LA CONFIGURACIÓN DE IAAS

Criminales Fuera de su Entorno

La investigación de Symantec muestra que un 16 % del tráfico web saliente puede provenir de servidores comprometidos, dirigidos a dominios conocidos de comando y control que controlan bots u otros ataques de malware. Los resultados de la encuesta externa lo confirman, con las organizaciones que respondieron que calificaron un promedio de 11 visitas a sitios web por semana como riesgosas y 11 como maliciosas. Si bien los números no llaman la atención de inmediato, si se hacen los cálculos, los resultados suman aproximadamente 572 visitas de sitios web de alto riesgo o maliciosas al año, lo que aumenta significativamente la exposición corporativa.

Los dispositivos de Internet de las cosas (IoT) se están convirtiendo rápidamente en otro importante vector de ataque. Según los encuestados de la encuesta externa, la cantidad de dispositivos de IoT que causaron incidentes de IaaS aumentó para siete de cada diez organizaciones en el último año.

572

VISITAS DE SITIOS WEB DE ALTO RIESGO O MALICIOSAS AL AÑO

Sección

03

Mejores Prácticas para Construir la Madurez de la Seguridad en la Nube

Más de la mitad de los encuestados en la investigación externa confirmaron que sus prácticas de seguridad en la nube no eran lo suficientemente maduras para satisfacer las demandas del creciente uso de las aplicaciones en la nube, y casi tres cuartos dijeron que experimentaron un incidente de seguridad en la infraestructura basada en la nube debido a esta inmadurez. Muchos malos hábitos pasan desapercibidos hasta que se produce un incidente, agravado por la falta de visibilidad en el entorno de la nube, y menos de la mitad de los encuestados realizan un análisis posterior de los incidentes para mejorar su práctica de seguridad en la nube. Los datos propios de Symantec confirman que un 85 % de los clientes no están utilizando las mejores prácticas del Centro de Seguridad de Internet (CIS).

Las compañías que continúan comprometiéndose o acelerando los servicios en la nube sin un plan para madurar sus prácticas de seguridad lo hacen bajo su propio riesgo. Las organizaciones deben considerar estas etapas principales para reforzar su postura de seguridad en la nube:

Desarrollar una estrategia de gobernabilidad respaldada por un Centro de Excelencia en la Nube (CCoE)

Adoptar un Modelo de Zero Trust

Promover la responsabilidad compartida

Aprovechar la automatización y la inteligencia artificial siempre que sea posible

Sección

04

Conclusión
Las Organizaciones Subestiman sus Riesgos en la Nube

La heterogeneidad del entorno empresarial moderno, que abarca diversas plataformas en la nube e instaladas localmente, ha agregado un conjunto más amplio de vulnerabilidades y vectores de ataque. Las enormes brechas de visibilidad dejan a las organizaciones en la oscuridad sobre la cantidad y la ubicación de los datos y las cargas de trabajo, lo que hace que sea más difícil identificar y mitigar los riesgos crecientes de seguridad.

Muchas empresas no están reconociendo la falla de percepción en la seguridad de la nube y ampliamente subestiman las amenazas actuales, quedando vulnerables a los compromisos de cuentas en la nube y las exposiciones de datos que representan sustanciales riesgos financieros y de reputación. La inversión en plataformas de seguridad cibernética en la nube que aprovechan la automatización y la inteligencia artificial para complementar recursos humanos limitados es una forma clara de automatizar las defensas y hacer cumplir los principios de gobernabilidad de datos. Más allá de la tecnología, es hora de reajustar la cultura y adoptar las mejores prácticas de seguridad a nivel humano, lo cual no es una tarea fácil teniendo en cuenta todos los desafíos de la gestión del cambio. Es una combinación de ambos factores lo que garantizará que la empresa esté suficientemente protegida hoy y, lo que es más importante, mañana, cuando nadie realmente sabe lo que el futuro puede traer.

Acerca de Symantec

Symantec Corporation (NASDAQ: SYMC) es líder mundial en soluciones de ciberseguridad y ayuda a las compañías, gobiernos e individuos a proteger sus datos más importantes en cualquier lugar Compañías en todo el mundo buscan a Symantec para soluciones estratégicas e integradas para defenderse contra ataques sofisticados en endpoints, en la nube e infraestructura.

De la misma forma, una comunidad global de más de 50 millones de personas y familias dependen de la suite de productos Norton y LifeLock de Symantec para proteger sus vidas digitales en casa y en todos sus dispositivos. Symantec opera una de las redes civiles de ciberinteligencia más grande del mundo, lo que le permite ver y proteger contra las amenazas más avanzadas. Para más información, visite www.symantec.com o síganos en Facebook, Twitter y LinkedIn.

Sede Mundial de Symantec
350 Ellis Street
Mountain View, CA 94043
EE.UU.
+1 650 527–8000
+1 800 721–3934

Para escritorios regionales y números de contacto específico, por favor acceda a nuestra página web. Para hablar con un Especialista en Productos en EE.UU., llame gratis 1 (800) 745 6054.

Symantec.com

Symantec