ORACLE

Las 5 principales tendencias de seguridad en la nube

Liderando el cambio con confianza

Adáptate a los cambios con total seguridad

En un panorama de cambio en la tecnología y las prioridades de las empresas, la única constante es la necesidad de proteger la información esencial. La pandemia ha llevado a los distintos sectores a adaptar y rediseñar sus operaciones, y casi un tercio de las organizaciones señalan que con en esta situación ha aumentado considerablemente su adopción de servicios en la nube1. El 55 % de las organizaciones afirma que después de la pandemia, la mayoría de los empleados seguirán teletrabajando al menos un día a la semana[2]. Teniendo esto en cuenta, las empresas deben invertir en una nube segura para seguir siendo competitivas.

En 2020, los líderes de TI se enfrentaron a desafíos sin precedentes para modernizar la infraestructura clave sin aumentar los costes ni sacrificar la seguridad. Adquirieron nuevos niveles de responsabilidad, garantizaron la seguridad de los sistemas y aportaron más valor estratégico.

Tanto para migrar cargas de trabajo a una nube pública, como para habilitar nuevos niveles de automatización o reducir la complejidad, resulta importante contar con una sólida estrategia de ciberseguridad. Oracle cuenta con décadas de experiencia en la protección de datos y aplicaciones, y nos comprometemos a ofrecer una nube más segura con Oracle Cloud Infrastructure (OCI), fortaleciendo la confianza y protegiendo los datos más valiosos.

Ir un paso por delante resulta crucial. Por ello compartimos las tendencias de seguridad cuyo impacto se espera que sea mayor en los próximos años, destacando cómo puede ayudar Oracle a satisfacer las necesidades de seguridad de las organizaciones.

[1] Encuesta ICT Enterprise Insights Survey 2020–2021 de Omdia

[2] PwC 2020 U.S. Remote Work Survey

1

Tendencia 1

El teletrabajo está aumentando la necesidad de contar con un enfoque de confianza cero en seguridad

2

Tendencia 2

Mayor inversión en seguridad inteligente

3

Tendencia 3

Automatización segura de DevOps

4

Tendencia 4

Los CISO tienen más responsabilidades que nunca

5

Tendencia 5

Una mejor gestión de la seguridad requiere mayores niveles de visibilidad

Tendencia 1

El teletrabajo está aumentando la necesidad de contar con un enfoque zero trust en seguridad

Los ciberataques han aumentado un 47 %3, en parte debido al teletrabajo.

La pandemia de COVID-19 ha acelerado la migración a la nube, que ya venía produciéndose a un ritmo intenso, al tiempo que ha creado nuevas oportunidades para las amenazas. El rápido aumento del número de empleados que trabajan desde casa, combinado con reuniones virtuales y una mayor dependencia del comercio electrónico, han expuesto a muchas organizaciones a ataques de ciberseguridad que aprovechan el uso ampliado de los servicios en la nube.

Hasta el 70 % de las empresas se enfrentan a desafíos de higiene cibernética en los puntos de conexión, y están informando de un aumento del 47 % en los ataques de ciberseguridad, como los intentos de suplantación de identidad. La descentralización y la rápida adopción de servicios en la nube exigen mayores precauciones. Sin embargo, las empresas utilizan una media de 573 aplicaciones de TI ocultas, muchas de ellas no autorizadas, lo que a menudo conlleva configuraciones inadecuadas y un uso sin supervisión. Con muchos empleados trabajando ahora fuera de los límites físicos de las empresas, resulta fácil pasar por alto las señales de aviso de personas malintencionadas con acceso privilegiado. Mientras tanto, las configuraciones incorrectas en la nube se están convirtiendo en la mayor fuente de fraude: en los últimos 24 meses, las cuentas con privilegios excesivos han supuesto la principal amenaza (el 44 %).

Un enfoque zero trust en cuanto a la seguridad en la nube desempeñará un papel fundamental en la gestión de las amenazas a medida que aumente el flujo de datos de las organizaciones hacia el exterior del perímetro de red habitual. De hecho, el 87 % de las organizaciones desea implementar una arquitectura zero trust tras la COVID-19. Con un enfoque zero trust, no hay ningún nivel de confianza predefinido asignado a un usuario, carga de trabajo, dispositivo o red. Este enfoque se debe aplicar desde la arquitectura hasta la aplicación. Cada solicitud de acceso debe ser validada en función de todos los puntos de datos disponibles, incluida la identidad de usuario, el dispositivo y la ubicación. Este contexto adicional utiliza varios factores para sustentar un enfoque basado en políticas que aplica la autenticación de dos factores. En esta se sigue el principio de privilegio mínimo, y los usuarios solo reciben los privilegios y niveles de acceso necesarios para las funciones específicas de su puesto.

[3] Wipro's State of Cybersecurity Report 2020

Aumento de los ataques de ciberseguridad en un 47%

El 87%

de las organizaciones desea una arquitectura de confianza cero tras la COVID-19

El 70%

de las empresas se enfrenta a desafíos de higiene cibernética en los puntos finales

Modelo zero trust con OCI

1

LA DIFERENCIA QUE MARCA ORACLE

Oracle Cloud Infrastructure Security

El riesgo que suponen las amenazas constantes se reduce integrando en la arquitectura de seguridad de la nube el aislamiento de espacios empresariales y el acceso con privilegios mínimos.

La seguridad de virtualización de red aislada está diseñada para evitar el movimiento lateral de amenazas y actores maliciosos.

La gestión integrada de identidades y acceso permite controlar fácilmente quién accede a los recursos en la nube.

Ofrecemos acceso seguro con autenticación de usuario y conexión única (SSO) desde una variedad de dispositivos y ubicaciones, así como autenticación basada en riesgos y prevención proactiva de fraudes en tiempo real.

La computación sensible al contexto recopila y utiliza los datos de identidad, dispositivo y ubicación.

Tendencia 2

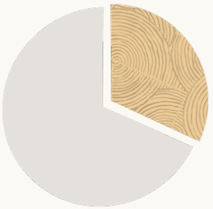
Mayor inversión en seguridad inteligente

La inteligencia artificial y el machine learning se han convertido en requisitos fundamentales para las tecnologías de ciberseguridad, más allá de la simple detección de malware.

Si bien las organizaciones están ajustando sus presupuestos como resultado de la pandemia, aún están dispuestas a invertir en inteligencia artificial (IA) y machine learning como elementos centrales de su estrategia de seguridad. De hecho, 9 de cada 10 encuestados señalan que estas tecnologías son fundamentales para su estrategia de seguridad en la nube, y para el 32 % de las organizaciones, la inversión en ciberseguridad con IA será una prioridad en los próximos 12 a 18 meses.

La IA y el machine learning se han estado utilizando en gran medida para detectar y evitar amenazas (p. ej., nuevas variantes de malware, exploits o ataques de suplantación de identidad). Sin embargo, la expansión de los servicios en la nube está fomentando usos aún más variados de la IA y el machine learning, más allá de detectar malware. En las nubes de última generación, las funciones de seguridad automatizadas pueden reducir el tiempo y los recursos necesarios para gestionar manualmente el acceso de los usuarios, al tiempo que se reducen los errores humanos. Asimismo, entre el 40 y el 45 % de las personas cree que la IA puede superar a los analistas de seguridad en la identificación de acciones fraudulentas, el mantenimiento de controles de configuración, la identificación de actividades de usuario anómalas y la evaluación y priorización de los eventos de seguridad.

Se prevé que la escasez mundial de personal de ciberseguridad alcance los 1,8 millones de puestos vacantes para 2022. Esta es una de las principales razones por las que el el 88 % de las cargas de trabajo se actualizará de forma autónoma en los próximos tres años, aprovechando la automatización y la inteligencia avanzadas. Al apoyarse más las organizaciones en la IA y el machine learning, los equipos de ciberseguridad ganarán una herramienta fundamental para prevenir vulneraciones, al tiempo que tendrán más tiempo para centrarse en la innovación que impulsa el negocio.



EL 32%
de las organizaciones prioriza la ciberseguridad con IA

ENTRE EL 40 Y EL 45 %
de las personas cree que la IA puede superar a los analistas de seguridad

EL 88%
de las cargas de trabajo se actualizarán de forma autónoma

Leer el informe de IDC

LA DIFERENCIA QUE MARCA ORACLE

Oracle Autonomous Database y Oracle Autonomous Linux

Autonomous Database

Autoprotección: automatiza la protección y seguridad de los datos; aplica parches automáticamente a la base de datos, y ayuda a evitar ataques o accesos no autorizados con cifrado de extremo a extremo “siempre activo”.

Autorreparación: protege contra tiempos de inactividad con una recuperación rápida y automática de interrupciones sin tiempo de inactividad. La autonomía basada en IA ejecuta diagnósticos y minimiza las interrupciones operativas.

Reduce los costes de administración de la seguridad hasta un 55%

Autonomous Linux

Aplicación de parches sin tiempo de inactividad del núcleo del sistema operativo y las bibliotecas del espacio del usuario claves, sin reinicio ni tiempo de inactividad programado.

> La IA y el machine learning no solo mejoran la colaboración: también facilitan el cambio constante. La capacidad de adaptación de forma rápida y a escala es una ventaja competitiva y, en el caso de la ciberseguridad, puede ser una cuestión de supervivencia.

accenture

Tendencia 3

Automatización segura de DevOps

A medida que DevOps se vuelve más automatizado, el 46 % de las organizaciones desea que se utilicen controles de seguridad para la integración continua en DevSecOps.

Con la evolución empresarial en 2020, se ha incrementado la demanda de nuevas aplicaciones. Esta demanda ha aumentado a una velocidad tal, que las organizaciones están produciendo aplicaciones más rápido de lo que pueden introducir nuevos controles de seguridad en los marcos existentes y los programas de cumplimiento. De este modo, se genera un desfase. Para paliarlo, las empresas deben automatizar la seguridad de su ciclo de vida de producción. Evitarán así ineficiencias y sobrecargas, al tiempo que se protegen contra posibles exposiciones si los servicios entran en producción antes de que se implante la seguridad. Esta situación ha impulsado mejoras incrementales en la seguridad de las aplicaciones en los últimos años.

La reestructuración para migrar a la nube comienza en las personas y los procesos, y la seguridad ha pasado a ocupar un lugar central en DevOps —a menudo, se habla de "DevSecOps". DevSecOps automatiza los procesos de ciberseguridad, a la vez que controla la cadena de herramientas de integración y entrega continuas (CI/CD) que estructura el ciclo de vida de las aplicaciones. La seguridad debe integrarse con la automatización de la integración y entrega continuas; de lo contrario, queda fuera del desarrollo, la integración y la entrega de la producción. Teniendo esto en cuenta, el 40 % de las organizaciones señala que DevSecOps ha fomentado un alto nivel de colaboración entre sus partes implicadas en el desarrollo y la gestión de la infraestructura, los propietarios de aplicaciones y los encargados de la ciberseguridad. Además, el 40 % también señaló que DevSecOps les permite incrementar su eficiencia operativa.

La utilización de DevSecOps no solo puede mejorar la eficiencia y la colaboración, sino que también puede transformar las prioridades de las organizaciones, desde la reacción ante incidentes de seguridad hasta el fortalecimiento proactivo de su postura de seguridad. Al incluir de forma continua controles de seguridad en el proceso DevOps, los líderes de TI pueden dedicar menos tiempo a gestionar los problemas cotidianos, y más a aportar valor al negocio.

El 46%

de las organizaciones desea que se utilicen controles de seguridad para la integración continua

El 40%

de las empresas señalan que DevSecOps ha permitido

un alto nivel de colaboración

mayor eficiencia operativa

Blog de Oracle Cloud Security

LA DIFERENCIA QUE MARCA ORACLE

Seguridad inteligente y automatizada

Automatiza la seguridad para reducir la complejidad, evitar errores humanos y reducir costes con la aplicación automatizada de parches en Autonomous Database y Autonomous Linux, y mitiga amenazas gracias a Cloud Guard y Oracle Identity Cloud Service.

Automatiza controles de seguridad básicos, como el cifrado de datos estáticos y en movimiento, junto con pruebas automatizadas a medida que se agregan nuevas funciones. Asimismo, la seguridad se ajusta y actualiza continuamente. Descubre cómo integrar Jenkins con los servicios de Oracle Cloud para realizar pruebas automatizadas.

Identifica decisiones de configuración que plantean un riesgo y alerta de desfases de configuración gracias a Data Safe.

Permite el proceso de entrega continua (CD) a través de la automatización en la nube: Oracle Cloud Infrastructure (OCI) expone todos nuestros servicios a operadores y desarrolladores. Nuestros servicios admiten de forma nativa herramientas de aprovisionamiento de código abierto para ayudar a los equipos de DevOps a construir infraestructuras inmutables mediante código.

Gestiona el estado de seguridad en la nube para detectar recursos mal configurados, a la vez que proporciona a los administradores visibilidad para evaluar la prioridad de los problemas y resolverlos.

Tendencia 4

Los CISO tienen más responsabilidades que nunca

Los responsables de seguridad de la información (CISO) deberán tener mayor conocimiento de la nube, ya que cada vez están más involucrados en la transformación digital y las iniciativas empresariales.

El último año ha puesto de manifiesto la necesidad de prepararse para la nube y modernizarse digitalmente. Las organizaciones se apoyan por ello más que nunca en sus responsables de seguridad de la información (CISO). Con el aumento de sus responsabilidades, los CISO se han convertido en impulsores del cambio en sus empresas, ya que son ellos quienes se encargan de respaldar la transformación digital (DX) y las iniciativas de computación en la nube. Los CISO están dedicando más tiempo a trabajar con los líderes de línea de negocio, alinear los procesos de negocio con la computación en la nube, anticipar los riesgos cibernéticos, actualizar los modelos de amenazas ligados a la computación en la nube e identificar las aplicaciones de TI ocultas. De hecho, el 73 % de las organizaciones han contratado o prevén contratar a un CISO con mayor experiencia en la nube, mientras que el 53 % emplea o espera contratar a un responsable de seguridad de la información empresarial (BISO) para integrar la ciberseguridad en sus procesos empresariales[4].

Al tiempo que los CISO se centran más en el negocio, Oracle está notando la aparición de CISO DX. Estos cargos tendrán que pulir los procesos de negocio mientras redefinen cómo se realiza el trabajo. Deben integrar la ciberseguridad en las iniciativas de DX e integrar una sólida seguridad cibernética en todos los aspectos de TI, en particular en los que atañen a la nube pública. Los CISO DX no solo deben racionalizar la cartera de tecnología, sino transformarla en un stack de seguridad totalmente integrado y escalable. Esto requiere un pipeline de datos de alto rendimiento para el procesamiento de datos por lotes y de flujos, la integración de las API entre herramientas, la ingestión de información sobre amenazas para el enriquecimiento de datos, y la automatización de procesos para dar respuesta inmediata a los incidentes y mitigar los riesgos.

Los CISO deberán incorporar la seguridad al desarrollo ágil de software, DevOps y los pipelines de integración y entrega continuas (CI/CD). Además, deben conseguir que sus equipos comprendan el modelo de responsabilidad de seguridad compartida en la nube y, a continuación, crear un modelo sinérgico de seguridad híbrida que abarque todos los aspectos de la infraestructura de TI. Por último, deben trabajar con el negocio para crear políticas de privilegios mínimos que puedan bloquear cuentas, gestionar usuarios con privilegios y proteger datos confidenciales.

EL 73%
de las organizaciones ha contratado o planea contratar un CISO

EL 53%
de las empresas tiene o planea contratar un BISO

Más información sobre la figura del CISO experto en la nube

[4] The Mission of the Cloud-centric CISO

LA DIFERENCIA QUE MARCA ORACLE

Oracle Cloud Infrastructure

Proporciona aislamiento y protecciones a los clientes, con residencia de datos, soberanía y seguridad en la nube.

Ofrece protección full-stack: con nuestro enfoque de seguridad con confianza cero, tú decides cómo la infraestructura, los usuarios, los dispositivos y las aplicaciones interactúan con los datos.

Permite la detección automatizada de errores de configuración de seguridad comunes para minimizar el riesgo gracias a herramientas como Oracle Cloud Guard.

Proporciona soluciones de seguridad para detectar amenazas, corregir errores y establecer protección contra ataques

Con seguridad de serie en la nube: todas las aplicaciones de SaaS de Oracle Fusion llevan integrado Oracle Identity Cloud Service (IDCS) para una seguridad sin fisuras basada en la identidad.

> El CISO DX no es solo un nuevo cargo, sino una evolución del papel del CISO, y de su relación con la transformación empresarial y digital. Para garantizar la prioridad, los CISO DX deben estar en contacto directo con el CEO.

KPMG

Tendencia 5

Una mejor gestión de la seguridad requiere mayores niveles de visibilidad

Las organizaciones están invirtiendo en nuevas herramientas para integrar el stack de seguridad en sus soluciones en la nube y permitir una visibilidad total del conjunto de aplicaciones e infraestructuras.

A raíz de la crisis global, las empresas buscan estabilidad y la nube se ha convertido en un elemento vital. La computación en la nube ha aumentado la velocidad con la que las organizaciones pueden abordar las dificultades y crear nuevas oportunidades, pero las complejidades crecientes plantean nuevos desafíos en materia de seguridad y visibilidad en todo el stack de tecnología. Las aplicaciones nativas de la nube introducen nuevas herramientas, procesos y roles, que a menudo, al ser de reciente creación, no gozan del mismo nivel de supervisión operativa que las aplicaciones tradicionales. El crecimiento de las opciones y aplicaciones de SaaS ha dado lugar a un uso no aprobado de la nube, con más de 1000 servicios no autorizados en uso actualmente en cada empresa. Además, al ser las cadenas de suministro más vulnerables al fraude, las organizaciones deben implementar un enfoque zero trust para lograr una visibilidad y una capacidad de auditoría amplias en todo el negocio.

A medida que crece nuestro ecosistema digital, las empresas tendrán que aprovechar las nuevas herramientas para hacer frente a las crecientes presiones sobre la privacidad y la regulación de los datos. El volumen y la variedad de datos dificultan su detección y clasificación, al tiempo que complican la aplicación de políticas de seguridad coherentes por parte de los equipos de seguridad. De hecho, el 30 % de las organizaciones han descubierto secretos en la nube, incluidas contraseñas, claves de cifrado y claves de API almacenadas en servidores basados en la nube. Con la evolución de las normativas del sector y en cuanto a conformidad, se requieren mecanismos más complejos para garantizar que la ejecución cumpla los reglamentos.

Al haberse disparado rápidamente la adopción de la nube con el teletrabajo, comprender el acceso a la nube y los privilegios es cada vez más difícil para los equipos de seguridad, que también controlan la actividad. Las empresas deben anticiparse y hacer frente a las complejidades de la protección de sus entornos en la nube. Muchas grandes organizaciones trabajan con varios proveedores de IaaS, PaaS y SaaS, cada uno con su propia versión del modelo de responsabilidad compartida, lo cual conlleva riesgos tales como configuraciones erróneas, vulnerabilidades de software, errores humanos y redundancia de procesos. Para reducir el riesgo e impulsar la protección continua, las empresas deben tener en cuenta tanto su infraestructura como la seguridad de las bases de datos y aplicaciones, la seguridad corporativa y la privacidad, así como la gestión de identidades y acceso.

Más de 1000

servicios no autorizados usados a diario

El 30 % de las empresas

han encontrado secretos en servidores basados en la nube

eBook sobre seguridad de datos y protección

LA DIFERENCIA QUE MARCA ORACLE

Supervisión, gestión y mitigación de seguridad con Oracle Cloud

Proporciona controles de seguridad SaaS completos a los propietarios de aplicaciones, los auditores y los equipos de operaciones de seguridad mediante Oracle Identity Cloud Service (IDCS) y Oracle Risk Management Cloud (RMC).

Ofrece respuestas y soluciones: Oracle Identity Cloud Service (IDCS) proporciona control del comportamiento y autenticación secundaria.

Brinda una base de datos autónoma con autoprotección: Gestión de la seguridad en el conjunto de la base de datos con Oracle Data Safe para analizar la actividad, gestionar las políticas de auditoría, detectar desfases de configuración y eliminar riesgos desde las fases de prueba y desarrollo.

Con gestión del estado de seguridad en la nube: Oracle Cloud Guard te ayuda a obtener una vista unificada del estado de seguridad en la nube de todos los inquilinos en Oracle Cloud.

Oracle Cloud Guard detecta recursos mal configurados y actividades no seguras en todos los inquilinos y proporciona a los administradores de seguridad visibilidad para evaluar la prioridad de los problemas de seguridad en la nube y resolverlos. Las inconsistencias de seguridad se pueden corregir automáticamente con opciones de seguridad listas para usar que permiten escalar de forma eficaz el centro de operaciones de seguridad.

Previsiones

Por ahora, queda claro que 2020 ha cambiado para siempre la forma de hacer negocios. Lo que también resulta evidente es que un enfoque centrado en la seguridad puede ser muy útil para reducir la complejidad e impulsar al mismo tiempo la innovación. Con las herramientas adecuadas, las organizaciones pueden automatizar la seguridad, evitar errores humanos y reducir costes. Además, dado que el teletrabajo y la computación en la nube se están convirtiendo en la nueva norma, los líderes sénior de TI asumirán un papel más importante a la hora de conformar un futuro más seguro para su negocio en los próximos años.

Prueba Oracle Cloud Free Tier

Más información sobre la seguridad siempre activa

Más información

Descubre historias de clientes que han realizado cambios significativos

Ver ahora

Más información sobre la seguridad de la infraestructura en la nube

Seguir leyendo

ORACLE