ORACLE

Las 5 principales tendencias de seguridad en la nube para 2021 y más allá

Liderar el cambio con confianza

Adaptarse a los cambios sin comprometerse

A medida que la tecnología cambia y las empresas cambian sus prioridades, la única constante es la necesidad de proteger la información crítica. La pandemia llevó a las industrias a adaptarse y remodelar sus operaciones, y casi un tercio de las organizaciones mencionaron la adopción de servicios en la nube como "significativamente más importante" que antes de la pandemia[1]. Y el 55% de las organizaciones afirma que la mayoría de los empleados continuarán trabajando de forma remota después de la pandemia al menos un día a la semana[2]. Teniendo esto en cuenta, las empresas deben invertir en una nube segura para mantenerse competitivas.

En 2020, los líderes de TI se enfrentaron a desafíos sin precedentes en cómo modernizar la infraestructura clave sin aumentar los costos ni sacrificar la seguridad. Asumieron nuevos niveles de responsabilidad, mantuvieron los sistemas seguros y aportaron un valor más estratégico.

Ya sea trasladando cargas de trabajo a una nube pública, permitiendo nuevos niveles de automatización o reduciendo la complejidad, es importante contar una postura de ciberseguridad sólida. Oracle cuenta con décadas de experiencia protegiendo datos y aplicaciones, y nos comprometemos a ofrecer una nube más segura con Oracle Cloud Infrastructure (OCI), creando confianza y protegiendo datos valiosos.

Mantenerse a la vanguardia es crucial, por lo que compartimos las tendencias de seguridad que se espera que tengan el mayor impacto en los próximos años, destacando cómo Oracle puede ayudar a abordar las necesidades de seguridad de una organización.

[1] Encuesta de Omdia sobre las TIC en las empresas 2020-2021

1

Tendencia 1

El trabajo remoto aumenta la necesidad de un enfoque de seguridad de confianza cero

2

Tendencia 2

Mayor inversión en seguridad inteligente

3

Tendencia 3

La automatización segura de DevOps

4

Tendencia 4

Los CISOs cumplen más funciones que nunca

5

Tendencia 5

Una mejor gestión de la seguridad requiere mayores niveles de visibilidad

Tendencia 1

El trabajo remoto está aumentando la necesidad de un enfoque de seguridad de confianza cero

Los ataques de ciberseguridad han aumentado un 47%[3], en parte debido al trabajo remoto.

La pandemia de COVID-19 ha acelerado un nivel ya vigoroso de adopción de la nube, al tiempo que ha creado nuevas oportunidades para los actores de amenazas. El rápido aumento de los colaboradores que trabajan desde casa, combinado con las reuniones virtuales y una mayor dependencia del comercio electrónico, ha expuesto a muchas organizaciones a ataques de ciberseguridad que explotan el uso ampliado de los servicios en la nube.

nada menos que el 70% de las empresas presentan desafíos con la higiene cibernética de endpoint, y están informando un aumento del 47% en los ataques de ciberseguridad, incluidos los intentos de phishing. La naturaleza descentralizada y la rápida adopción de los servicios en la nube exigen mayores precauciones. Sin embargo, las empresas utilizan un promedio de 573 aplicaciones de TI en la sombra, muchas de las cuales no han sido examinadas, lo que a menudo conduce a configuraciones inadecuadas y a un uso no supervisado. Dado que muchos colaboradores trabajan fuera de los muros corporativos físicos de una organización, es fácil pasar por alto las señales de advertencia exhibidas por los informantes maliciosos. Mientras tanto, las configuraciones erróneas en la nube se están convirtiendo en una de las principales fuentes de fraude, siendo la principal amenaza las cuentas sobreprivilegiadas (44%) en los últimos 24 meses.

Un enfoque de confianza cero para la seguridad en la nube desempeñará un papel fundamental en la gestión de las amenazas, ya que cada vez más datos de la organización fluyen fuera del perímetro típico de la red. De hecho, el 87% de las organizaciones desea implementar una arquitectura de confianza cero después de la pandemia. Con un enfoque de confianza cero, no hay un nivel de confianza predefinido asignado a un usuario, carga de trabajo, dispositivo o red. Este enfoque debe desarrollarse desde la arquitectura hasta la aplicación, con todas las solicitudes de acceso validadas en función de todos los puntos de datos disponibles, incluidos la identidad del usuario, el dispositivo y la ubicación. Este contexto adicional utiliza múltiples factores para impulsar un enfoque basado en políticas al activar una autenticación de dos factores. Esto se basa en el principio del menor privilegio, ya que los usuarios solo reciben los privilegios y los niveles de acceso necesarios para sus funciones específicas.

[3] Informe de Wipro sobre el estado de la ciberseguridad en 2020

Un aumento del 47% en ataques de ciberseguridad

El 87% desea una arquitectura de confianza cero después de la pandemia

El 70% presenta problemas con la ciberhigiene de los endpoints

Modelo de confianza cero con OCI (en ingles)

1

LA DIFERENCIA DE ORACLE

Seguridad de la infraestructura de Oracle Cloud

El riesgo de amenazas constantes se reduce utilizando el aislamiento de inquilinos incorporado y el acceso con menos privilegios en la arquitectura de seguridad en la nube

La seguridad de la virtualización de la red aislada ha sido diseñada para evitar el movimiento lateral de amenazas y malos actores

La gestión de identidades y acceso integrada controla fácilmente quién accede a los recursos de la nube

El acceso seguro se ofrece con la autenticación de usuario y el inicio de sesión único (SSO) desde una variedad de dispositivos y ubicaciones, así como la autenticación basada en riesgos y prevención proactiva de fraudes en tiempo real

La computación consciente del contexto recopila y aprovecha la identidad, el dispositivo y la ubicación

Tendencia 2

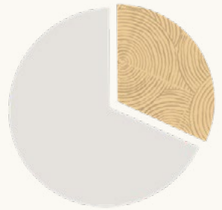
Mayor inversión en seguridad inteligente

La IA y el ML se han convertido en requisitos fundamentales para las tecnologías de ciberseguridad, más allá del malware.

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

Estas tecnologías se han utilizado en gran medida para detectar y prevenir amenazas (por ejemplo, nuevas variantes de malware, exploits o ataques de phishing). Sin embargo, la expansión de los servicios en la nube está impulsando aún más usos de IA y ML más allá de la detección de malware. Las funciones de seguridad automatizadas en las nubes de última generación reducen el tiempo y los recursos necesarios para gestionar manualmente el acceso de los usuarios, al tiempo que disminuyen los errores humanos. En consecuencia, entre el 40% y el 45% de los individuos creen que la IA puede superar a los analistas de seguridad en: identificación de acciones fraudulentas, mantenimiento de controles de configuración, identificación de actividad anómala de usuarios y evaluación y priorización de eventos de seguridad.

Se prevé que la escasez de personal en materia de ciberseguridad a nivel mundial alcance la asombrosa cifra de 1,8 millones de personas en 2022. Esta es una de las principales razones por las que el 88% de todas las cargas de trabajo se actualizarán de forma autónoma en los próximos tres años, aprovechando la automatización avanzada y la inteligencia. Dado que las organizaciones confían en mayor medida en la IA y el ML, los equipos de ciberseguridad obtendrán una herramienta crítica para prevenir brechas, al tiempo que tendrán más tiempo para centrarse en la innovación que impulsa el negocio.



El 32%
prioriza la ciberseguridad con IA

El 40% a 45%
creen que la IA puede superar a los analistas de seguridad

El 88%
de las cargas de trabajo tendrán actualizaciones autónomas

Leer el informe de IDC (en ingles)

LA DIFERENCIA DE ORACLE

Oracle Autonomous Database y Autonomous Linux

Autonomous Database

Autoprotección: automatiza la protección y la seguridad de los datos; parchea automáticamente la base de datos; y ayuda a evitar accesos/ataques no autorizados con un cifrado de extremo a extremo "siempre activo"

Autorreparación: protege contra tiempo de inactividad con una recuperación rápida y automática de dichas interrupciones, la autonomía basada en IA ejecuta diagnósticos y minimiza las interrupciones operativas

Reduce los costos de administración de seguridad en hasta un 55%

Autonomous Linux

Parcheo sin tiempo de inactividad del SO y de la bibliotecas clave del espacio de usuario sin reiniciar ni programar el tiempo de inactividad

> La IA/ML no es sólo una cuestión de colaboración; se trata de tecnologías que permiten el cambio perpetuo. La capacidad de adaptarse a velocidad y escala es una ventaja competitiva y, en el caso de la ciberseguridad, puede ser una cuestión de supervivencia.

accenture

Tendencia 3

La automatización segura de DevOps

A medida que DevOps se automatiza cada vez más, el 46% de las organizaciones desea que DevSecOps utilice controles de seguridad para la integración continua.

La evolución de las empresas en 2020 aumentó la demanda de nuevas aplicaciones. Esta demanda ha aumentado tan rápidamente que las empresas están produciendo aplicaciones más rápido de lo que pueden introducir nuevos controles de seguridad en los marcos y programas de cumplimiento existentes, creando así una "brecha de ritmo". Las empresas deben responder a esta brecha de ritmo incorporando la automatización de la seguridad en su ciclo de vida de producción para evitar ineficiencias y gastos generales, al tiempo que se protegen contra la posible exposición si los servicios se ponen en marcha antes de la implementación de la seguridad. Este escenario ha provocado mejoras graduales en la seguridad de las aplicaciones durante los últimos años.

El reequipamiento para la nube comienza con personas y procesos, y la seguridad ha surgido como un caso de uso principal de DevOps, a menudo denominado "DevSecOps". DevSecOps automatiza los procesos de ciberseguridad, mientras controla la cadena de herramientas de integración continua y entrega continua (CI/CD) que orquesta el ciclo de vida de las aplicaciones. La seguridad debe integrarse con la automatización de CI/CD, de lo contrario queda fuera del desarrollo, la integración y la entrega de la producción. En este sentido, el 40% de las organizaciones afirma que DevSecOps ha fomentado un alto nivel de colaboración entre su responsables de desarrollo, gestión de infraestructuras, propietarios de aplicaciones y ciberseguridad. Además, el 40% también señaló que DevSecOps les permite obtener una mayor eficiencia operativa a través de la automatización.

El empleo de DevSecOps no solo mejora la eficiencia y la colaboración, sino que también transforma el enfoque de una organización, que pasa de reaccionar ante los incidentes de seguridad a fortalecer su postura de seguridad de forma proativa. Al integrar continuamente los controles de seguridad en el proceso de DevOps, los responsables de TI dedican menos tiempo a gestionar problemas cotidianos y más tiempo a aportar valor a la empresa.

El 46%
desea que DevSecOps utilice controles de seguridad para la integración continua

El 40%
afirma que DevSecOps ha permitido

un alto nivel de colaboración

mayor eficiencia operativa

LA DIFERENCIA DE ORACLE

Seguridad inteligente y automatizada

Automatiza la seguridad para reducir la complejidad, evitar errores humanos y reducir los costos con parches automatizados para Autonomous Database y Autonomous Linux, y la mitigación de amenazas por parte de Cloud Guard y Oracle Identity Cloud Service

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

Identifica las opciones de configuración que plantean un riesgo y resalta la desviación de la configuración con Data Safe

Permite el proceso de entrega continua (CD) a través de la automatización de 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 desarrollar infraestructuras inmutables mediante el uso de códigos

Adopta la gestión de la postura de seguridad en la nube para detectar recursos mal configurados, al tiempo que proporciona a los administradores la visibilidad necesaria para clasificar y resolver problemas

Tendencia 4

Los CISOs cumplen más funciones que nunca

Las funciones de los CISOs exigirán una mayor experiencia centrada en la nube a medida que se comprometan más con la transformación digital y las iniciativas empresariales.

El pasado año se hizo hincapié en la necesidad de preparación para la nube y la modernización digital. Como resultado, las organizaciones recurren más que nunca a sus directores de seguridad de la información (CISO). A medida que estos profesionales cumplen más funciones, se han convertido en los agentes de cambio de sus organizaciones, con la tarea de apoyar la transformación digital (DX), así como las iniciativas de computación en la nube. Los CISO dedican más tiempo a trabajar con los líderes de la LOB, a alinear los procesos empresariales con la computación en la nube, a anticiparse a los riesgos cibernéticos, a actualizar los modelos de amenazas vinculados a la computación en la nube y a identificar las aplicaciones de TI en la sombra De hecho, el 73% de las organizaciones ha contratado o tiene previsto contratar a un CISO con mayores conocimientos de computación en la nube, mientras que el 53% emplea o planea emplear a un director de seguridad de la información empresarial (BISO) para integrar la ciberseguridad en sus procesos comerciales [4].

Con el CISO centrándose más en la empresa, Oracle también observa la aparición de la transformación digital. Estos ejecutivosdeberán perfeccionar los procesos de negocio y redefinir cómo se realiza el trabajo. Deben integrar la ciberseguridad en las iniciativas de transformación digital e incorporar una sólida ciberseguridad en todos los aspectos de la TI, especialmente la computación en la nube pública. Los CISOs de DX no solo deben racionalizar el portafolio de tecnología, sino transformarlo en una pila de seguridad estrechamente integrada y adaptable. Esto requiere una canalización de datos de alto rendimiento para el procesamiento de datos en flujo y por lotes, la integración de API entre herramientas, la ingesta de inteligencia sobre amenazas para el enriquecimiento de datos y la automatización de procesos para la respuesta inmediata a incidentes y la mitigación de riesgos.

Tendrán que integrar la seguridad con el desarrollo ágil, DevOps y la integración continua automatizada y los canales de entrega continua (CI/CD). Además, deben hacer que sus equipos comprendan el modelo de responsabilidad de seguridad compartida en la nube y, a continuación, construir un modelo de seguridad híbrido sinérgico que cubra todos los aspectos de la infraestructura de TI. Por último, deben trabajar con la empresa para crear políticas con mínimos privilegios que puedan bloquear cuentas, gestionar usuarios con privilegios y proteger datos confidenciales.

[4] La misión del CISO centrado en la nube

El 73%

contrató o tiene previsto contratar a un CISO

El 53%

emplea o planea emplear a un BISO

Lee sobre el CISO centrado en la nube (en ingles)

LA DIFERENCIA DE ORACLE

Oracle Cloud Infrastructure

Ofrece aislamiento y protección al cliente con residencia de datos, soberanía y seguridad en la nube

Ofrece protección de pila completa: con nuestro enfoque de seguridad de confianza cero, es posible decidir cómo la infraestructura, los usuarios, los dispositivos y las aplicaciones interactúan con los datos

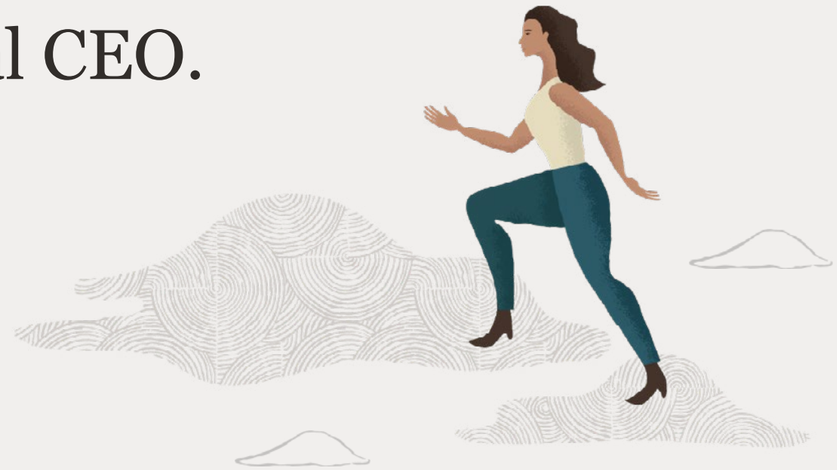
Proporciona detección automatizada de los errores de seguridad más comunes para minimizar el riesgo a través de herramientas como Oracle Cloud Guard

Ofrece soluciones de seguridad para detectar amenazas, corregir errores y proteger contra ataques

Ofrece una serie de seguridad en la nube integrada: cada aplicación Oracle Fusion incluye Oracle Identity Cloud Service (IDCS) para una seguridad consistente y basada en la identidad

> El CISO de DX no es solo un nuevo cargo, sino más bien una evolución del cargo de CISO y su relación con la empresa y la transformación digital. Para garantizar la prioridad, estos profesionales deben reportarse directamente al CEO.

KPMG



Tendencia 5

Una mejor gestión de la seguridad requiere mayores niveles de visibilidad

Las organizaciones están invirtiendo en nuevas herramientas para integrar la pila de seguridad en sus soluciones en la nube y permitir una visibilidad completa en todas las aplicaciones e infraestructuras.

A medida que las empresas buscan estabilidad tras una crisis global, la nube se ha convertido en un salvavidas. La computación en la nube ha aumentado la velocidad con la que las organizaciones pueden abordar las dificultades y crear nuevas oportunidades, pero las crecientes complejidades plantean nuevos desafíos para la seguridad y la visibilidad en toda la pila de tecnología. Las aplicaciones nativas de la nube introducen nuevas herramientas, procesos y personas que a menudo son inmaduras, y carecen 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 de la nube no autorizado, con más de 1.000 de estos servicios no autorizados en uso en cada empresa en la actualidad. Y con las cadenas de suministro más vulnerables al fraude, las organizaciones deben implementar un enfoque de confianza cero para una amplia visibilidad y auditoría en toda la empresa.

A medida que nuestro ecosistema digital crece, las empresas necesitarán aprovechar 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 el descubrimiento y la clasificación de los mismos, a la vez que dificultan a los equipos de seguridad la aplicación de políticas de seguridad coherentes. De hecho, el 30% de las empresas han descubierto "secretos en la nube", incluyendo contraseñas, claves de cifrado y claves de API almacenadas en servidores basados en la nube. Con la evolución de las normativas de cumplimiento y de la industria, éstas exigen mayores mecanismos para garantizar la ejecución conforme.

Con el trabajo remoto que provoca la rápida adopción de la nube, comprender el acceso y los privilegios en la nube es cada vez más difícil para los equipos de seguridad que también están monitoreando la actividad. Las empresas deben anticiparse y analizar las complejidades de seguridad de sus entornos de nube. Debido a que grandes organizaciones trabajan con múltiples proveedores de IaaS, PaaS y SaaS, cada uno con su propia versión del modelo de responsabilidad compartida, las empresas se vuelven susceptibles a 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 su infraestructura, junto con la seguridad de las bases de datos y las aplicaciones, la seguridad y la privacidad corporativas, así como la gestión de identidad y acceso.

Más de 1000

servicios no autorizados utilizados diariamente

El 30%

encontró secretos almacenados en servidores basados en la nube

Ebook sobre seguridad y protección de datos

LA DIFERENCIA DE ORACLE

Supervisión, gestión y mitigación de la seguridad de Oracle Cloud

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

Ofrece respuesta y remediación: Oracle Identity Cloud Service (IDCS) ofrece supervisión del comportamiento y autenticación secundaria

Ofrece una base de datos autónoma autoprotegida: Gestiona la seguridad en la base de datos, utilizando Oracle Data Safe para: analizar la actividad; gestionar las políticas de auditoría; detectar la desviación de configuración y eliminar el riesgo del proceso de prueba y desarrollo

Utiliza Cloud Security Posture Management: Oracle Cloud Guard ayuda a obtener una visión unificada de la postura de seguridad en la nube de todos los inquilinos de Oracle Cloud Infrastructure

Oracle Cloud Guard detecta recursos mal configurados y actividades no seguras entre los inquilinos y proporciona a los administradores de seguridad la visibilidad para clasificar y resolver los problemas de seguridad en la nube. Las inconsistencias de seguridad se pueden remediar automáticamente con recetas de seguridad listas para usar a fin de adaptar eficazmente el centro de operaciones de seguridad

Lo que viene

A estas alturas, está claro que 2020 ha cambiado permanentemente la forma de hacer negocios. Lo que también es evidente es que un enfoque que dé prioridad a la seguridad puede contribuir en gran medida a reducir la complejidad y, al mismo tiempo, impulsar la innovación. Con las herramientas adecuadas, las organizaciones pueden automatizar la seguridad, evitar errores humanos y reducir los costos. Y con el trabajo remoto y la computación en la nube convirtiéndose en la nueva normalidad, los líderes de TI asumirán un papel más importante en la conformación de un futuro más seguro para su empresa en los próximos años.

Prueba el Modo Gratuito de Oracle Cloud

Descubra cómo adaptarse a los cambios con Oracle Cloud

Más información

Conoce historias de clientes que realizaron cambios significativos

Mirar ahora

Más información sobre la seguridad de la infraestructura de la nube

Leer más

ORACLE