ORACLE

# As 5 principais tendências de segurança na nuvem para 2021 e além

## Conduzindo a mudança com confiança

# Adaptando-se à mudança com menos riscos

À medida que a tecnologia muda e as empresas alteram suas prioridades, a única constante é a necessidade de proteger as informações críticas. A pandemia levou as indústrias a adaptar e remodelar as operações, com quase um terço das organizações citando a adoção de serviços em nuvem como "significativamente mais importante" do que antes da pandemia[1]. E 55% das organizações dizem que a maioria dos funcionários continuará trabalhando remotamente após a pandemia pelo menos um dia por semana[2]. Com isto em mente, as empresas devem investir em uma nuvem segura para se manterem competitivas.

Em 2020, os líderes de TI enfrentaram desafios sem precedentes sobre como modernizar as principais infraestruturas sem aumentar os custos ou sacrificar a segurança. Eles assumiram novos níveis de responsabilidade, mantiveram os sistemas seguros e contribuíram com um valor mais estratégico.

Seja movendo cargas de trabalho para uma nuvem pública, permitindo novos níveis de automação, ou reduzindo a complexidade, uma postura robusta de segurança cibernética é importante. A Oracle tem décadas de experiência na proteção de dados e aplicativos, e nos comprometemos a oferecer uma nuvem mais segura com a Oracle Cloud Infrastructure (OCI) - gerando confiança e protegendo dados valiosos.

Ficar à frente é crucial, e é por isso que estamos compartilhando as tendências de segurança que devem ter o maior impacto nos próximos anos, destacando como a Oracle pode ajudar a atender às necessidades de segurança de uma organização.

[1] Omdia's 2020–2021 ICT Enterprise Insights Survey

1

## Tendência 1

**O trabalho remoto está aumentando a necessidade de uma abordagem de confiança zero para a segurança**

2

## Tendência 2

**Maior investimento em segurança inteligente**

3

## Tendência 3

**A automação segura do DevOps**

4

## Tendência 4

**Os CISOs estão tendo mais responsabilidades que nunca**

5

## Tendência 5

**Uma melhor gestão da segurança requer níveis mais elevados de visibilidade**

# Tendência 1

## O trabalho remoto está aumentando a necessidade de uma abordagem de confiança zero para a segurança

**Os ataques de segurança cibernética aumentaram em 47%[3], em parte devido ao trabalho remoto.**

A pandemia da COVID-19 acelerou um nível já elevado de adoção da nuvem, ao mesmo tempo em que criou novas oportunidades para os agentes de ameaças. O rápido aumento de funcionários trabalhando em casa, combinado a reuniões virtuais e uma maior dependência do *ecommerce*, expôs muitas organizações a ataques de segurança cibernética que exploram o uso expandido de serviços em nuvem.

Cerca de 70% das empresas estão tendo desafios com a higiene cibernética de pontos de extremidade, e estão relatando um aumento de 47% nos ataques de cibersegurança, incluindo tentativas de *phishing*. A natureza descentralizada e a rápida adoção de serviços em nuvem exigem maiores precauções. No entanto, as empresas usam uma média de 573 aplicativos de TI na sombra (shadow IT), muitos dos quais não foram verificados, o que muitas vezes leva a configurações inadequadas e uso não supervisionado. Com muitos funcionários agora trabalhando do lado de fora das paredes de uma organização, é fácil perder os sinais de alerta exibidos por pessoas com intenções maliciosas. Enquanto isso, as configurações incorretas na nuvem estão se tornando uma das principais fontes de fraude, com a maior ameaça vindo de contas superprivilegiadas (44%) nos últimos 24 meses.

Uma abordagem de confiança zero para a segurança em nuvem desempenhará um papel fundamental no gerenciamento de ameaças, à medida que mais dados organizacionais fluem para fora do perímetro típico da rede. De fato, 87% das organizações querem implementar uma arquitetura de confiança zero após a COVID-19. Com uma abordagem de confiança zero, não há um nível predefinido de confiança atribuído a um usuário, carga de trabalho, dispositivo ou rede. Esta abordagem deve ser construída da arquitetura para o aplicativo, com cada solicitação de acesso validada com base em todos os pontos de dados disponíveis - incluindo identidade, dispositivo e localização do usuário. Este contexto adicional usa vários fatores para orientar uma abordagem baseada em políticas, desencadeando uma autenticação de dois fatores. Isto se baseia no princípio do privilégio mínimo, com os usuários recebendo apenas os privilégios e níveis de acesso necessários para suas funções específicas.

[3] Wipro's State of Cybersecurity Report 2020

**Ataques de segurança cibernética aumentaram em**

**47%**

**87%**

**querem uma arquitetura de confiança zero após a COVID-19**

**70%**

**têm desafios com higiene cibernética de pontos de extremidade**

Modelo de confiança zero com a OCI (em inglês)

1

A DIFERENÇA DA ORACLE

# Oracle Cloud Infrastructure Security

**O risco de ameaças constantes é reduzido** utilizando o isolamento integrado do locatário e o acesso com menos privilégios na arquitetura de segurança da nuvem

**A segurança de virtualização de rede isolada** é projetada para evitar o movimento lateral de ameaças e maus agentes

**O gerenciamento integrado de identidades e acesso** controla facilmente quem acessa os recursos na nuvem

**O acesso seguro é oferecido** com autenticação de usuário e logon único (SSO) de uma variedade de dispositivos e locais, bem como autenticação baseada em risco e prevenção proativa de fraudes em tempo real

**A computação sensível ao contexto** coleta e usa a identidade, o dispositivo e a localização

# Tendência 2

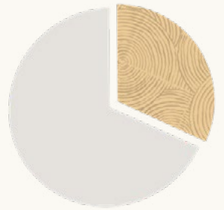
## Maior investimento em segurança inteligente

**IA e ML se tornaram requisitos fundamentais para tecnologias de segurança cibernética - além de apenas malware.**

Embora as organizações estejam apertando seus orçamentos como resultado da pandemia, elas ainda estão dispostas a investir em inteligência artificial (IA) e machine learning (ML) como elementos centrais de sua postura de segurança. Na verdade, 9 em cada 10 entrevistados apontam essas tecnologias como fundamentais para sua estratégia de segurança na nuvem, e 32% das organizações estão priorizando segurança cibernética com IA como o principal investimento nos próximos 12 a 18 meses.

IA e ML têm sido amplamente usados para detectar e prevenir ameaças (por exemplo, novas variantes de malware, explorações ou ataques de *phishing*). No entanto, a expansão dos serviços em nuvem está exigindo ainda mais usos de IA e ML além da detecção de malware. Os recursos de segurança automatizados em nuvens de última geração podem reduzir o tempo e os recursos necessários para gerenciar manualmente o acesso do usuário, além de diminuir o erro humano. Consequentemente, 40%-45% dos indivíduos acreditam que a IA pode superar os analistas de segurança em tarefas como identificação de ações fraudulentas, manutenção de controles de configuração, identificação de atividades anômalas do usuário e triagem e priorização de eventos de segurança.

Prevê-se que a escassez global de mão-de-obra em cibersegurança atinja a impressionante marca de 1,8 milhão até 2022. Esta é uma das principais razões pelas quais 88% de todas as cargas de trabalho serão atualizadas de forma autônoma nos próximos três anos, aproveitando a automação e a inteligência avançadas. Com as organizações dependendo mais da IA e do ML, as equipes de segurança cibernética ganharão uma ferramenta crítica na prevenção de violações, tendo mais tempo para se concentrar na inovação que impulsiona os negócios.



**32%**
**priorizam a segurança cibernética com IA**

**40%-45%**
**acreditam que a IA pode superar os analistas de segurança**





**88%**
**das cargas de trabalho terão atualizações autônomas**

Leia o relatório do IDC (em inglês)

A DIFERENÇA DA ORACLE

# Oracle Autonomous Database e Autonomous Linux

## Autonomous Database

**Autoproteção:** automatiza a proteção e a segurança de dados, corrige automaticamente o banco de dados, e ajuda a evitar acesso não autorizado/ataques com criptografia de ponta a ponta "sempre ativa"

**Autorreparo:** protege contra tempo de inatividade, com recuperação rápida e automática de interrupções - a autonomia baseada em IA executa diagnósticos e minimiza a interrupção operacional

**Reduz os custos administrativos de segurança** em até 55%

## Autonomous Linux

**Correção sem tempo de inatividade** do kernel do sistema operacional e bibliotecas de espaço do usuário sem reinício ou tempo de inatividade programado

> IA/ML não se trata apenas de colaboração; é sobre permitir a mudança perpétua. A capacidade de adaptação em velocidade e escala é uma vantagem competitiva e, no caso da segurança cibernética, pode ser uma questão de sobrevivência.

accenture

# Tendência 3

## A automação segura do DevOps

**À medida que o DevOps se torna cada vez mais automatizado, 46% das organizações querem DevSecOps para utilizar controles de segurança para integração contínua.**

A evolução dos negócios em 2020 aumentou a demanda por novos aplicativos. Esta demanda aumentou tão rapidamente que as organizações estão produzindo aplicativos mais rápido do que podem introduzir novos controles de segurança em estruturas e programas de conformidade existentes - criando assim uma "lacuna de ritmo". As empresas devem responder a esta lacuna de ritmo incorporando a automação de segurança ao seu ciclo de vida de produção para evitar ineficiências e despesas gerais, ao mesmo tempo em que se protegem contra a exposição potencial se os serviços entrarem em operação antes da implementação da segurança. Este cenário desencadeou melhorias incrementais na segurança de aplicativos nos últimos anos.

A adaptação para a nuvem começa com pessoas e processos, e a segurança surgiu como um dos principais casos de uso do DevOps - muitas vezes referido como "DevSecOps". O DevSecOps automatiza os processos de segurança cibernética, enquanto controla a cadeia de ferramentas de integração contínua e entrega contínua (CI/CD) que orquestra o ciclo de vida do aplicativo. A segurança deve ser integrada à automação de CI/CD, caso contrário é deixada de fora do desenvolvimento, integração e entrega da produção. Diante disso, 40% das organizações relatam que o DevSecOps promoveu um alto nível de colaboração entre seus *stakeholders* em desenvolvimento, gerenciamento de infraestrutura, proprietários de aplicativos e segurança cibernética. Além disso, 40% também observaram que o DevSecOps permite que eles ganhem maior eficiência operacional por meio da automação.

Empregar o DevSecOps pode não apenas melhorar a eficiência e a colaboração, mas também transformar o foco de uma organização, de reagir a incidentes de segurança a fortalecer proativamente sua postura de segurança. Ao incluir continuamente os controles de segurança no processo de DevOps, os líderes de TI podem passar menos tempo gerenciando problemas do dia a dia e mais tempo agregando valor aos negócios.

**46%**

**querem DevSecOps para utilizar os controles de segurança para integração contínua**

**40%**

**relatam que o DevSecOps permitiu**

- um nível mais alto de colaboração
- maior eficiência operacional

A DIFERENÇA DA ORACLE

# Segurança inteligente e automatizada

**Automatiza a segurança** para reduzir a complexidade, evitar erros humanos e reduzir custos com patches automatizados para o Autonomous Database e Autonomous Linux – e mitigação de ameaças pelo Cloud Guard e pelo Oracle Identity Cloud Service

**Automatiza controles básicos de segurança**, incluindo criptografia de dados em repouso e em movimento, juntamente com testes automatizados à medida que novos recursos são adicionados e a segurança é continuamente refinada e atualizada. Leia como integrar o Jenkins aos serviços da Oracle Cloud para testes automatizados

**Identifica as opções de configuração** que representam um risco e destaca o desvio de configuração com o Data Safe

**Permite o processo de entrega contínua (CD) através da automação em nuvem:** a Oracle Cloud Infrastructure (OCI) expõe todos os nossos serviços a operadores e desenvolvedores. Nossos serviços suportam de forma nativa ferramentas de provisionamento de código aberto para ajudar as equipes de DevOps a construir infraestruturas imutáveis usando código

**Adota o gerenciamento de postura de segurança na nuvem** para detectar recursos configurados incorretamente, ao mesmo tempo em que fornece aos administradores a visibilidade para triagem e resolução de problemas

# Tendência 4

## Os CISOs estão tendo mais responsabilidades que nunca

**As funções do CISO exigirão maior experiência centrada na nuvem conforme se tornam mais envolvidos com iniciativas de transformação digital e de negócios.**

O último ano enfatizou a necessidade de prontidão para a nuvem e modernização digital. Como resultado, as organizações estão dependendo mais do que nunca de seus diretores de segurança da informação (CISOs). À medida que os CISOs assumem mais responsabilidades, eles se tornam os agentes de mudança de suas organizações - sendo encarregados de apoiar a transformação digital (DX), assim como iniciativas de computação em nuvem. Os CISOs estão passando mais tempo trabalhando com líderes de LOB (linha de negócio), alinhando processos de negócios com computação em nuvem, antecipando riscos cibernéticos, atualizando modelos de ameaças vinculados à computação em nuvem e identificando aplicativos sombra de TI. Na verdade, 73% das organizações contrataram ou planejam contratar um CISO com maiores habilidades de computação em nuvem, enquanto 53% empregam ou planejam empregar um responsável de segurança da informação (BISO) para integrar a segurança cibernética em seus processos empresariais [4].

Com o CISO se concentrando mais nos negócios, a Oracle também está vendo o surgimento do CISO DX. Estes executivos serão chamados para refinar os processos de negócios enquanto redefinem como o trabalho é feito. Eles devem integrar a segurança cibernética em iniciativas de DX e incorporar uma forte segurança cibernética em todos os aspectos de TI, especialmente computação em nuvem pública. Os CISOs DX devem não apenas racionalizar o portfólio de tecnologia, mas transformá-lo em uma pilha de segurança firmemente integrada e escalável. Isto requer um pipeline de dados de alto desempenho para processamento de dados de fluxo e lote, integração de API entre ferramentas, captura de inteligência de ameaças para enriquecimento de dados e automação de processos para resposta imediata a incidentes e mitigação de riscos.

Os CISOs precisarão integrar a segurança ao desenvolvimento ágil, DevOps e pipelines automatizados de integração contínua e entrega contínua (CI/CD). Além disso, eles devem fazer com que suas equipes entendam o modelo de responsabilidade de segurança compartilhada na nuvem e, em seguida, criem um modelo de segurança híbrido sinérgico que cubra todos os aspectos da infraestrutura de TI. Por fim, eles devem trabalhar com a empresa para criar políticas de privilégio mínimo que possam bloquear contas, gerenciar usuários privilegiados e proteger dados confidenciais.

[4] The Mission of the Cloud-centric CISO

**73%**

**contrataram ou planejam contratar um CISO**

**53%**

**empregam ou planejam empregar um BISO**

Leia sobre o CISO centrado na nuvem (em inglês)

A DIFERENÇA DA ORACLE

# Oracle Cloud Infrastructure

**Oferece isolamento e proteções ao cliente** com residência de dados, soberania e segurança na nuvem

**Oferece proteção completa:** com a nossa abordagem de segurança de confiança zero. Você decide como a infraestrutura, os usuários, os dispositivos e os aplicativos interagem com os dados

**Fornece detecção automatizada de** configurações incorretas de segurança comuns para minimizar riscos por meio de ferramentas como o Oracle Cloud Guard

**Fornece soluções de segurança** para detectar ameaças, corrigir erros e proteger contra ataques

**Oferece séries de segurança em nuvem integradas:** todo aplicativo SaaS do Oracle Fusion inclui o Oracle Identity Cloud Service (IDCS) para uma segurança consistente e baseada em identidade

> O CISO DX não é apenas um novo título, mas sim uma evolução do papel do CISO e sua relação com os negócios e a transformação digital. Para assegurar a prioridade, os CISOs DX devem se reportar diretamente ao CEO.

KPMG

# Tendência 5

## Uma melhor gestão da segurança requer níveis mais elevados de visibilidade

**As organizações estão investindo em novas ferramentas para integrar a pilha de segurança em suas soluções de nuvem e permitir total visibilidade em todos os aplicativos e infraestrutura.**

À medida que as empresas buscam estabilidade após uma crise global, a nuvem se tornou uma tábua de salvação. A computação em nuvem aumentou a velocidade com que as organizações podem lidar com as dificuldades e criar novas oportunidades, mas as crescentes complexidades representam novos desafios para a segurança e a visibilidade em toda a pilha de tecnologia. Os aplicativos nativos em nuvem introduzem novas ferramentas, processos e personas que muitas vezes são imaturos, sem o mesmo nível de supervisão operacional que os aplicativos tradicionais. O crescimento nas opções e aplicativos SaaS deu origem ao uso não autorizado da nuvem, com mais de 1.000 desses serviços não autorizados em uso em cada empresa hoje. E, com as cadeias de suprimentos mais vulneráveis à fraude, as organizações devem implementar uma abordagem de confiança zero para ampla visibilidade e auditoria em toda a empresa.

À medida que nosso ecossistema digital cresce, as empresas precisarão utilizar novas ferramentas para lidar com pressões crescentes sobre a privacidade e os regulamentos de dados. O volume e a variedade de dados dificultam sua descoberta e classificação, ao mesmo tempo que tornam problemático para as equipes de segurança impor políticas de segurança consistentes. De fato, 30% das organizações descobriram "segredos de nuvem", incluindo senhas, chaves de criptografia e chaves de API armazenadas em servidores baseados em nuvem. Com a evolução dos regulamentos de conformidade e do setor, elas exigem mecanismos maiores para garantir a execução em conformidade.

Com o trabalho remoto desencadeando a rápida adoção da nuvem, entender o acesso e os privilégios nela é cada vez mais difícil para as equipes de segurança que também estão monitorando a atividade. As empresas devem se preparar e navegar pelas complexidades de proteger seus ambientes em nuvem. Como muitas grandes organizações trabalham com vários provedores de IaaS, PaaS e SaaS - cada uma com sua própria versão do modelo de responsabilidade compartilhada - as empresas se tornam suscetíveis a configurações incorretas, vulnerabilidades de software, erros humanos e redundância de processos. Para reduzir riscos e impulsionar a proteção contínua, as empresas precisam considerar sua infraestrutura, juntamente com a segurança de bancos de dados e aplicativos, segurança corporativa e privacidade, bem como o gerenciamento de identidades e acesso.



**+1000**

**serviços não autorizados utilizados diariamente**



**30%**

**encontraram segredos de nuvem armazenados em servidores em nuvem**

Ebook de segurança e proteção de dados

A DIFERENÇA DA ORACLE

# Monitoramento, gerenciamento e mitigação de segurança da Oracle Cloud

**Fornece controles de segurança SaaS completos** para proprietários de aplicativos, auditores e equipes de operações de segurança por meio de: Oracle Identity Cloud Service (IDCS) e Oracle Risk Management Cloud (RMC)

**Oferece resposta e remediação:** O Oracle Identity Cloud Service (IDCS) oferece monitoramento comportamental e autenticação secundária

**Fornece um banco de dados autônomo e com autoproteção:** Gerencia a segurança em todo o banco de dados, usando o Oracle Data Safe para: analisar a atividade, gerenciar as políticas de auditoria, detectar desvios de configuração e remover o risco do processo de teste e desenvolvimento

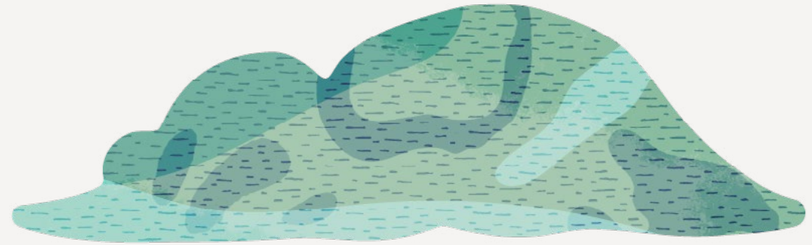
**Utiliza o Cloud Security Posture Management:** O Oracle Cloud Guard ajuda você a obter uma visão unificada de sua postura de segurança na nuvem em todos os locatários clientes na Oracle Cloud Infrastructure

**O Oracle Cloud Guard detecta recursos configurados incorretamente e atividades inseguras** em todos os locatários e fornece aos administradores de segurança a visibilidade para triagem e resolução de problemas de segurança na nuvem. As inconsistências de segurança podem ser corrigidas automaticamente com receitas de segurança prontas para uso para dimensionar efetivamente o centro de operações de segurança

# O que vem por aí

Até agora, está claro que 2020 mudou permanentemente a maneira como os negócios são feitos. O que também é aparente é que uma abordagem de segurança em primeiro lugar pode contribuir muito para reduzir a complexidade e, ao mesmo tempo, impulsionar a inovação. Com as ferramentas certas, as organizações podem automatizar a segurança, evitar erros humanos e reduzir custos. E com o trabalho remoto e a computação em nuvem se tornando o novo normal, os líderes sênior de TI assumirão um papel maior na formação de um futuro mais seguro para suas empresas nos próximos anos.

Experimente o Oracle Cloud - Modo Gratuito



**Descubra como navegar pela mudança com a Oracle Cloud**

Saiba mais

**Conheça histórias de clientes que fizeram mudanças significativas**

Assista agora

**Leia mais sobre segurança de infraestrutura em nuvem**

Leia mais

ORACLE