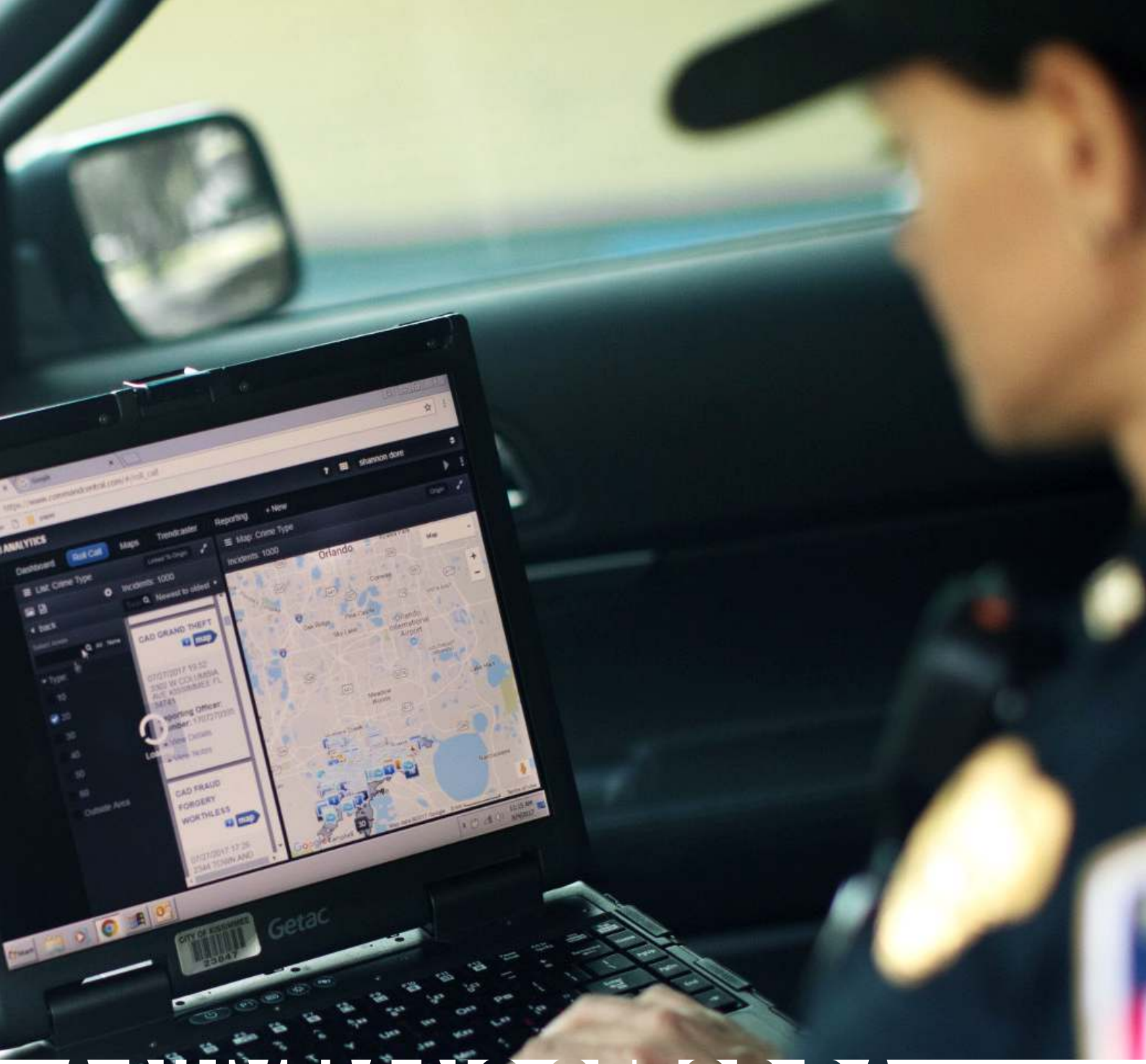


A NUVEM NO SETOR DA SEGURANÇA PUBLICA

O QUE VOCÊ PRECISA SABER AGORA

MOTOROLA SOLUTIONS

1

POR QUE COMPUTAÇÃO EM NUVEM E POR QUE AGORA?

A computação em nuvem (cloud computing) tem sido utilizada em torno de muitos anos na empresa e está ganhando muito mais interesse das agências governamentais por uma variedade de razões, incluindo: custos, agilidade e simplificação da rede. No entanto, existem necessidades e desafios de dados. Então como as soluções em nuvem podem auxiliar na aplicação da lei e por que você deve fazer a transição para a nuvem agora?

Enquanto o custo é um fator importante, o benefício mais importante para suas operações é a capacidade da nuvem para melhorar drasticamente a gestão e utilização de dados global, em última análise, ajudando a manter os componentes mais seguros.

A EXPLOSÃO DE DADOS

Todas as formas de dados estão explodindo. De acordo com a Cisco, o tráfego global anual de IP atingirá 3,3 zettabytes (ZB) por ano até 2021, ou 278 exabytes (EB) por mês. Para referência, apenas em 2016, a taxa anual de correr para o tráfego global de IP foi de 1,2 ZB por ano, ou 96 por mês (EB 1 Zetabyte equivale a 1 trilhão de Gigabytes). Nesta era digital, policiais estão sobrecarregados com dados estruturados e, cada vez mais, os dados não estruturados, tais como vídeo, mídias sociais, e-mail e dados do sensor. Esse tsunami de dados está dificultando a eficácia, por exemplo, um mandado de busca consome em redes aproximadamente 3 terabytes de dados em evidencias digitais, e sem as ferramentas adequadas pode levar quatro semanas para os pesquisadores chegarem a apenas 1 terabyte. Além disso, eles devem processar dados estruturados tradicionais, incluindo mandados de prisão, registros e arquivos criminais.

A expansão da Internet das Coisas (IoT) também está alimentando uma série de capacidades de segurança pública, melhorando e gerando mais dados. Assim também é mais e mais um vídeo. Isso se aplica na geração de vídeos de câmeras corporais, câmeras automotivas, câmaras de vigilância fixas, e agora até mesmo em drones.

Para isso tudo fazer sentido, ferramentas analíticas avançadas podem ajudar a extrair o máximo valor destes dados. Elas ajudam a agregar e correlacionar dados históricos e informações em tempo real dispersas em toda a sua operação de segurança pública. Esses pontos são fundamentais para aprimorar a segurança pública.

Existe um potencial para desenvolver sua estratégia de gerenciamento de dados e melhorar os sistemas antigos e processos ultrapassados. As soluções em nuvem podem e devem desempenhar um papel fundamental nessa evolução.

EM NÚMEROS

1 Zettabyte

=

1 trilhão de Gigabytes

1 Zettabyte = 1000 Exabytes

1 Exabyte = 1000 Petabytes

1 Petabyte = 1000 Terabytes

1 Terabyte = 1000 Gigabytes

EVOLUÇÃO DOS SISTEMAS DE GESTÃO DE DADOS

Atualemente a maioria das agências de aplicação da lei ainda dependem de diferentes sistemas desatualizados, que guardam informações em sigilos, reduzindo a capacidade efetiva de obter e entregar inteligência onde e quando necessário. É claro que essa agência deseja tornar melhor o acesso tempo real aos relatórios e informações detalhadas para ajudar a concentrar recursos na luta contra a criminalidade de forma mais inteligente e eficiente.

Hoje, as cidades começam a abraçar novos sistemas e tecnologias e já veem algumas vitórias importantes, por exemplo, o Departamento de Polícia de Chicago (CPD) que está implantando amplamente ferramentas preditivas e analíticas depois de ver resultados iniciais positivos. O Prefeito de Chicago Rahm Emanuel e a polícia acreditam que utilizando o que há de mais recente em TI, incluindo vigilância por vídeo e policiamento controlado por dados, estão reduzindo os crimes violentos na cidade.

Mudanças demográficas nas forças policiais também irão afetar a disseminação das tecnologias orientadas por dados. Por volta de 2020, millennials (a geração do milênio, composta por jovens nascidos após os anos 2000) irão compor 50% da mão-de-obra. Esta geração nascida na era digital é alfabetizada no ambiente da tecnologia e hábil em multitarefas. As agências já estão experimentando a influência destes fatores, pois cada vez mais se utilizam smatphones para auxiliar em atividades diárias. Manter-se alinhado à tecnologias também pode auxiliar no processo de recrutamento e melhorar a retenção de pessoal qualificado.

O volume e a velocidade de dados tende a aumentar continuamente. A nuvem não apenas ajudará a gerenciar essa explosão de dados e fornecerá ferramentas analíticas poderosas, mas também como os serviços em nuvem são uma tecnologia "aditiva", e não "substitutiva", os departamentos podem continuar a obter valor dos investimentos existentes enquanto amplificam suas capacidades.

Da gestão de grandes quantidades de dados ao recrutamento de millennials que esperam as mais recentes ferramentas tecnológicas, a nuvem é fundamental para as necessidades da comunidade de segurança pública, à medida que continua a evoluir.

> **Mudanças demográficas nas forças policiais irão afetar a disseminação da tecnologia orientada a dados. Por volta de 2020, millennials irão compor 50% da mão-de-obra.**

2

O QUE É A NUVEM?

A nuvem utiliza uma abordagem para o processo de compra, gerenciamento, e implantação de infra-estrutura e solições software de TI. Com as soluções locais, os aplicativos são implantados pelo cliente, nos equipamentos de propriedade do cliente, e posteriormente geridos pelo cliente. Os clientes são responsáveis por todos os processos, incluindo a disponibilidade de serviço, durabilidade de dados, segurança de dados, geo-redundância, escalabilidade, e muito mais.

Por outro lado, as soluções hospedadas em nuvem são oferecidas como serviço, implantadas em uma nuvem privada, publica, ou comunitária de um data center do provedor de serviços em nuvem. Neste caso, a infra-estrutura é gerida pelo provedor de serviço em nuvem e pode ser operada apenas para uma organização ou grupo de organizações (privadas ou nuvem comunitária), ou posto à disposição do público em geral, normalmente orientado para o setor público (núvem pública).

Por último, soluções híbridas podem ser uma combinação de nuvem hospedada privada, e soluções no local.

MODELOS DE IMPLEMENTAÇÃO DE TECNOLOGIA

NUVEM
Provedor de serviço em nuvem
Hospedado e Totalmente gerenciado

NO LOCAL
Cliente Totalmente gerenciado
Data Center

HÍBRIDA
Combinação de
"nuvem" e "no local"

MODELOS DE IMPLANTAÇÃO DE NUVEM

PRIVADO	A infra-estrutura de nuvem é operada exclusivamente para uma organização por um provedor de serviço em nuvem, geralmente como infra-estrutura isolada em seu data center.
COMUNIDADE	A infra-estrutura de nuvem é compartilhada por várias organizações e oferece suporte a uma comunidade específica que tem preocupações comuns. (Por exemplo, missão, requisitos de segurança, política e considerações sobre conformidade).
PÚBLICO	A computação em nuvem é uma infra-estrutura disponibilizada para o público em geral ou de um grande grupo industrial.

CONTRIBUIÇÃO DA NUVEM

Quando se trata soluções hospedadas em nuvem (seja em um ambiente de nuvem privada, pública ou comunitária), existem diferentes modelos para interagir e consumir recursos da nuvem. De um modo geral, estes são classificados como: Infraestrutura Como Serviço (IaaS), Plataforma Como Serviço (PaaS) e Software Como Serviço (SaaS).

IaaS fornece a menor quantidade de recursos de um provedor de serviços em nuvem. Os clientes compram e consomem a infra-estrutura, incluindo a computação, rede e recursos de armazenamento. Este é o modelo mais flexível, mas também requer mais trabalho por parte do consumidor, conforme os clientes estão comprando capacidades básicas, e implementando sua própria solução para recursos de IaaS. Esses clientes são plenamente responsáveis pelo desempenho de tais implementações.

O PaaS permite que os consumidores de nuvem também comprem serviços de um provedor de serviços em nuvem, em vez de apenas comprar recursos básicos como em IaaS. Os serviços variam de acordo com o provedor, mas podem incluir bancos de dados, ferramentas de gerenciamento de contêineres, mensagens, entradas API e balanceamento de carga. Com PaaS, os componentes básicos de sua solução são fornecidos. Dito isto, uma vez que os serviços e interfaces variam entre provedores de serviços em nuvem, aplicativos construídos usando recursos de PaaS são muito menos portateis entre fornecedores de serviços em nuvem. Mesmo com o desenvolvimento simplificado de aplicativos fornecidos pela PaaS, uma quantidade significativa de trabalho ainda é exigido pelo consumidor de nuvem para criar soluções completas.

SaaS apresenta aos consumidores de nuvem soluções de software completas na nuvem. Os clientes de soluções de SaaS compram ou locam recursos de aplicativos diretamente para resolver um problema. Um exemplo familiar é Netflix, um fornecedor de soluções de SaaS que fornece aos seus clientes uma solução completa de streaming de vídeo, construídos em torno de aplicações para streaming, faturamento, gerenciamento de contas, etc. Para colocar isso em perspectiva, a Netflix é um consumidor de IaaS e PaaS da Amazon Web Services (AWS), utilizando estes recursos e serviços para construir aplicativos e implantar uma solução de SaaS, que seus clientes de locarão, pagando uma taxa mensal para acesso.

Para a maioria das agências de segurança pública estaduais e municipais, as soluções SaaS oferecerão as respostas mais abrangentes às suas necessidades de policiamento.

MODELOS DE CONSUMO EM NUVEM

= Você gerencia

= Outros gerenciam

NO LOCAL	INFRAESTRUTURA COMO UM SERVIÇO	PLATAFORMA COMO UM SERVIÇO	SOFTWARE COMO UM SERVIÇO
Aplicativo	Aplicativo	Aplicativo	Aplicativo
Dados	Dados	Dados	Dados
Tempo de execução	Tempo de execução	Tempo de execução	Tempo de execução
Middleware (Software que conecta duas aplicações diferentes e separadas)	Middleware (Software que conecta duas aplicações diferentes e separadas)	Middleware (Software que conecta duas aplicações diferentes e separadas)	Middleware (Software que conecta duas aplicações diferentes e separadas)
O/S	O/S	O/S	O/S
Virtualização	Virtualização	Virtualização	Virtualização
Servidores	Servidores	Servidores	Servidores
Armazenamento	Armazenamento	Armazenamento	Armazenamento
Rede de Comunicação	Rede de Comunicação	Rede de Comunicação	Rede de Comunicação

3

SEGURANÇA DE DADOS NA NUVEM

Ao considerar a segurança de diferentes tecnologias, é importante entender que as ameaças mais graves para os sistemas de uma organização tem menos a ver com o local onde se encontram, e mais como eles são acessados, como os dados são protegidos em repouso e em trânsito, e como os aplicativos são protegidos.

A maioria dos ataques não tem como alvo a infra-estrutura, mas a camada de aplicação através de ataques por injecção, quebra de autenticação, controle de acesso e segurança insuficiente de uma configuração errada, todos combinados com um nível inadequado de registo e monitoramento. Essas são todas as áreas em que os provedores de serviços em nuvem, em conjunto com os provedores de soluções SaaS que entregam os aplicativos, sobressaem. Embora as soluções locais possam, teoricamente, fazer o mesmo, o orçamento de segurança de TI dos provedores de serviços de nuvem superam até mesmo o maior orçamento de segurança de TI do departamento. Ainda assim, a segurança é sobre a redução de riscos e a análise de custo-benefício e há considerações de segurança positivas e negativas para diferentes modelos de implantação.

As maiores ameaças aos sistemas de uma organização possuem menos relação com o local onde estão localizadas, e mais com como são acessadas, como os dados são protegidos em repouso e em trânsito e como os aplicativos são protegidos.

NO LOCAL

Há três áreas principais onde a segurança se destaca:

1. Quando há uma necessidade de ser isolada, ou não conectada à Internet pública.
2. Quando há um regulamento de privacidade de dados ou outra necessidade de conformidade para que os dados residam em uma área não suportada pela nuvem.
3. Quando o controle absoluto sobre a segurança é desejado.

No entanto, controle não se traduz necessariamente em segurança. A proteção adequada dos aplicativos, dados, serviços e infraestrutura que você possui tem um custo considerável, tanto em termos de despesas de capital quanto recursos de segurança de TI para configurar e manter as ferramentas de segurança e a postura de segurança. Isso pode ser tempo e dinheiro que poderiam ser mais bem gastos com foco na missão principal de sua organização

NUVEM

Com uma implantação de SaaS na nuvem, a maior parte da segurança é gerenciada por um provedor de serviços em nuvem (por exemplo, AWS) e um provedor de soluções SaaS (por exemplo, Netflix). Isso libera recursos preciosos de segurança de TI para se concentrar em quem deve ter acesso aos dados. O conjunto de ferramentas fornecido por esses provedores permite que a administração de segurança simples aponte e clique para controlar o acesso a dados e serviços e também fornece interfaces simples para auditoria e notificação aos administradores quando as configurações de segurança são modificadas. Essas ferramentas administrativas tornam a configuração incorreta da segurança praticamente uma situação do passado.

A nuvem também é particularmente valiosa por sua resiliência cibernética e pela capacidade de se defender de ataques direcionados e sustentados de negação de serviço distribuída (DDoS), como os lançados pelos Botnets.

Embora os críticos da nuvem sugerissem que a concentração de informações na nuvem a torna um alvo tentador para mal-intencionados, apenas o tamanho e a escala da nuvem têm os recursos necessários para lidar adequadamente com ataques em larga escala. Os provedores de nuvem fazem grandes esforços para se proteger contra ataques. Seria quase impossível igualar esse nível de defesa no local.

Informações de ameaças (Threat Intelligence) é outra área onde a nuvem se destaca. Os provedores de serviços em nuvem têm ferramentas de monitoramento extremamente sofisticadas e podem muito bem ser os primeiros a perceber uma tentativa de ataque ou violação, alertando imediatamente o provedor da solução ou até você mesmo.

Em um mundo onde mal-intencionados colaboram e coordenam, é extremamente benéfico ter um provedor de serviços em nuvem trabalhando a seu favor.

Além disso, como estes provedores veem tantos ataques contra muitos de seus locatários, eles são os primeiros a aplicar as práticas recomendadas de segurança com base no tipo de padrões de ataque que percebem. Ao fazer isso, uma organização se beneficia das lições aprendidas em uma ampla amostra de outras organizações.

Provedores de serviços em nuvem e provedores de soluções SaaS também eliminam grande parte do ônus caro e demorado de buscar certificações de conformidade de segurança, como certificações do DoD, certificações FIPS, certificações ISO e outros requisitos específicos do país. Tais certificações e atestados não apenas dão ao seu departamento de TI a confiança de que a solução é segura, mas também economizam tempo e recursos do departamento de TI, liberando orçamento para ser gasto em outro lugar.

HÍBRIDO

Para aqueles que querem aproveitar muitos dos benefícios de segurança da nuvem, mas ainda querem manter um controle mais rigoroso sobre seus dados, uma abordagem híbrida pode fazer sentido. As implantações de nuvem híbrida oferecem ao cliente vários graus de controle, como permitir que o cliente controle as chaves de criptografia de dados que ainda existem na nuvem, todo o caminho para manter as chaves de criptografia no local e criptografar os dados no local antes de enviá-los para a nuvem. No último exemplo todos os dados na nuvem são criptografados em trânsito e em repouso usando chaves de criptografia que nunca saem do local do cliente.

A segurança híbrida também pode assumir outras formas. Por exemplo, os clientes podem continuar provisionando e credenciando seus funcionários no local, depois usam essas mesmas identidades e credenciais para acessar uma solução SaaS. Isso permite a reutilização de soluções existentes de Gerenciamento de Identidades e Acesso e permite um único local para usuários integrados e externos, independentemente de eles acessarem uma solução no local ou na nuvem. Este é apenas um exemplo de combinações de nuvens híbridas. Muitos tipos são possíveis, com o cliente mantendo controle total sobre o que existe no local e um alto grau de controle sobre as partes que existem na nuvem.

4

CONSIDERAÇÕES SOBRE A SOLUÇÃO SAAS

Ao escolher uma solução SaaS baseada em nuvem, há várias questões para ponderar. Segurança, tanto física quanto cibernética. Dados privados. Serviço disponível. Escalabilidade Redundância. Onde começar? Abaixo, discutimos alguns dos fatores mais importantes ao decidir sobre uma nova solução SaaS.

SEGURANÇA E PRIVACIDADE

Embora as soluções SaaS geralmente incorporem fortes recursos de segurança, é importante verificá-las e garantir que você se sinta confortável com suas competências. Para esse fim, ao fazer uma avaliação, tanto a segurança do provedor de serviços de nuvem subjacente quanto a segurança do provedor de soluções SaaS precisam ser levadas em consideração.

Para o provedor de serviços de nuvem, a segurança física de seu data center é um vetor de ataque crítico e precisa ser considerada. É importante entender como as salas de servidores estão seguras, quem tem acesso e como os visitantes são controlados. O acesso físico às salas de servidores é registrado, monitorado e auditado? No caso das operações do governo, o pessoal autorizado é vetado pelos cidadãos do país? As verificações em segundo plano são realizadas em administradores e outras pessoas com acesso a recursos? Também é importante entender onde os servidores em nuvem estão localizados fisicamente e se você precisa que os dados residam fisicamente em um país ou área física específica. E quais requisitos de redundância geográfica existem?

A segurança na nuvem, assim como no local, é toda sobre como os dados são manipulados, incluindo sua confidencialidade em trânsito e em repouso, sua integridade e sua disponibilidade. Você deve entender e se sentir confortável com quem tem acesso aos dados, quando eles têm acesso a eles e de onde eles têm esse acesso. Todo acesso a dados, seja para ler dados, gravar dados, criar dados ou excluir dados, deve ser registrado. Padrões também são obrigatórios aqui. Uma das regras de ouro em segurança é "não invente o seu próprio." Um provedor de soluções SaaS deve ser capaz de explicar o uso de padrões abertos controlados e baseados no setor para segurança.

> **UMA DAS REGRAS DE OURO EM SEGURANÇA É "NÃO INVENTE O SEU PRÓPRIO."**

Estas perguntas adicionais também devem ser considerados:

Criptografia
Os dados são criptografados em trânsito e em repouso usando criptografia de padrões abertos?

O gerenciamento de Patch
As vulnerabilidades conhecidas são ativamente corrigidas de maneira oportuna?

Informações de Ameaças
O provedor da solução o alerta se seus dados foram comprometidos ou tentaram um acesso não autorizado?

Segurança de aplicativos
O código é continuamente verificado quanto às vulnerabilidades conhecidas?

Conformidade
Quais critérios o fornecedor de soluções está em conformidade?

Traga Sua Própria Credencial
O provedor de soluções permite que você aproveite sua infra-estrutura existente de gerenciamento de identidades e acesso?

Autenticação de múltiplos fatores (AMF)
O provedor de soluções oferece tecnologias de AMF seguras e utilizáveis que são resistentes a ataques de phishing?

Aplicação de Políticas
O provedor de soluções permite que você aplique políticas de segurança de TI?

Ataques DDoS
A combinação de o provedor de serviço em nuvem/provedor de soluções SaaS defende ativamente os ataques de negação de serviço distribuída (DDoS), garantindo que o acesso a seus dados e serviços permaneça disponível mesmo em face de um ataque contínuo e direcionado?

Análise
A segurança do provedor de soluções foi avaliada por um terceiro independente?

Saber que seus dados estão protegidos contra maus agentes é um bom começo, mas também deve ser protegido contra uso indevido pelo provedor de soluções. Como proprietário dos dados, você deve ter direito de propriedade sobre os dados e como eles são usados. É importante garantir que existam políticas implementadas pelo provedor de serviços em nuvem e pelo provedor de soluções SaaS que impeçam o acesso inadequado de dados. Os provedores também devem contratar funcionários e administradores que tenham passado por extensas verificações de antecedentes e sejam recomendados com referências múltiplas e confiáveis. Além disso, se for tomada a decisão de deixar o provedor de soluções SaaS, você deverá manter seus dados. A soberania de dados deve ser um requisito obrigatório.

DISPONIBILIDADE E ESCALABILIDADE

DISPONIBILIDADE

A disponibilidade descreve a capacidade de um sistema ou serviço de continuar a operação na presença de falhas de hardware e software. É uma função dos parâmetros de confiabilidade de tempo médio entre falhas (MTBF) e tempo médio de reparo (MTTR). É geralmente representado como uma porcentagem ou uma fração, por exemplo 9995, que indica a porcentagem de tempo que o serviço deve estar disponível. A alta disponibilidade é desejável para serviços devido à importância que eles desempenham em suas operações, estejam eles operando em um ambiente de nuvem pública ou privada ou em hardware dedicado no local.

Outro aspecto da disponibilidade são as garantias de desempenho, que podem ser consideradas um tipo de falha gradual ou flexível. Um serviço que não atende às garantias de desempenho não pode ser considerado altamente disponível. Por esse motivo, considere como você pode gerenciar a disponibilidade na presença de falhas e na presença de cargas de trabalho aumentadas.

> **A ALTA DISPONIBILIDADE É DESEJÁVEL PARA SERVIÇOS DEVIDO À IMPORTÂNCIA QUE ELES DESEMPENHAM EM SUAS OPERAÇÕES**

Manter a alta disponibilidade de um serviço implica abordar as seguintes questões:

1. Garantir que o serviço continuará a operar na presença de falhas limitadas de hardware.

2. Assegurar que o serviço continuará a operar na presença de falhas limitadas de software do sistema.

3. Garantir que o sistema continue a funcionar como esperado na presença de crescente carga de trabalho.

Os dois primeiros requerem algum nível de redundância para endereçar e o terceiro requer um grau de escalabilidade do sistema.

Um recurso de sistema necessário para soluções locais e na nuvem é a presença de infraestrutura de rede. Para soluções SaaS, essa rede é uma combinação de infraestrutura de rede do provedor de serviços em nuvem, conectividade de provedor de telecomunicação e a Internet. Para soluções no local, essa rede consiste em infraestrutura de rede de propriedade do cliente. A melhor prática para obter uma rede altamente disponível com uma solução SaaS é usar provedores de hardware e telecomunicações redundantes nos dois lados da conexão de rede com o provedor de serviços em nuvem. Para obter conectividade de alta disponibilidade, o hardware de conexão deve ser redundante, mesmo ao se conectar do mesmo local. Provedores de serviços em nuvem mantêm esse tipo de redundância em seus sistemas. A mesma abordagem é verdadeira para conectividade no local, embora toda a redundância deva ser mantida pelo proprietário da solução nas instalações da empresa.

A própria Internet é outro ponto de falha, mas a Internet foi projetada redundantemente com falhas. Como a Internet é simplesmente a interconexão de várias redes públicas e privadas, como Comcast e Verizon, e como essas conexões são redundantes e geograficamente diversas, há pouca preocupação de que a Internet não esteja disponível. As redes constituintes que compõem a Internet também são implantadas com redundância embutida, mas, mesmo assim, elas podem falhar, e é por isso que é recomendável se conectar de forma redundante por meio de vários provedores de telecomunicações. Cada vez mais, as soluções locais exigem conectividade com a Internet para interagir com dispositivos móveis. Portanto, em muitos casos, o fato de estar no local protege apenas parcialmente contra falhas na conectividade com a Internet. Ainda assim, fazer uso da Internet utilizando níveis apropriados de redundância é quase certamente mais confiável do que uma rede privada mantida por uma única entidade.

Fazer uso da Internet utilizando níveis apropriados de redundância é quase certamente mais confiável do que uma rede privada mantida por uma única entidade.

A fim de garantir a disponibilidade, os seguintes princípios devem ser seguidos:

1. Todas as soluções implantadas na nuvem precisam usar regras de exclusão ou disponibilidade específicas para a nuvem, de modo que falhas únicas no hardware subjacente não tornem a solução indisponível.

2. Todas as soluções precisam ser implantadas utilizando software de gerenciamento e orquestração que as implanta em máquinas virtuais (VM), de modo que falhas únicas de VM não tornem a solução indisponível.

3. Todas as falhas de VM devem ser detectadas e novas VMs serão colocadas on-line automaticamente.

4. Todas as soluções precisam ser implantadas usando software de gerenciamento e orquestração, de modo que interrupções sejam detectadas e os serviços afetados sejam reiniciados automaticamente.

5. Todas as soluções precisam ser monitoradas para degradação e falha de desempenho, assim instâncias adicionais da solução poderão ser colocadas on-line para aumentar o desempenho do serviço ou substituir os serviços com falha. Isso inclui soluções implantadas de maneira redundante para alta disponibilidade

ESCALABILIDADE

A escalabilidade pode ser classificada como horizontal ou vertical. A escalabilidade horizontal de um serviço permite que cópias adicionais de seus componentes sejam adicionadas ou removidas para levar em conta diferentes cargas de trabalho. A escala vertical é a técnica de adicionar poder de processamento, largura de banda e armazenamento ao hardware subjacente de um serviço existente sem adicionar cópias adicionais dos componentes de serviço.

Para que a escalabilidade horizontal seja alcançável, os serviços devem ser explicitamente projetados para escalabilidade. Essa escalabilidade pode ser aplicada em dois níveis diferentes da hierarquia do sistema - dimensionamento em uma zona de disponibilidade (AZ) e dimensionamento em vários AZs. Os AZs são recursos de processamento separados fisicamente e podem ser locais de implantação distintos "geograficamente" dentro de um único sistema do provedor de serviços de nuvem, ou provedores de serviços de nuvem separados.

O dimensionamento em toda a zona de disponibilidade tem a vantagem de aumentar a disponibilidade. O escalonamento dentro de um AZ também aumenta a disponibilidade, na medida em que o serviço se degradará com falhas de componentes individuais, em vez de falhar todos juntos.

Um passo adicional pode ser dado. Embora não recomendado, está implantando uma solução para vários provedores de nuvem, como AWS e Google. O custo adicional de desenvolvimento, implantação e manutenção de duas instâncias diferentes de cada serviço oferece pequenos benefícios além dos já acumulados por meio da redundância de provedores de nuvem e AZs individuais. O custo adicional de desenvolvimento, implantação e manutenção de duas instâncias diferentes de cada serviço oferece pouco benefício além dos benefícios já acumulados por meio da redundância de provedores de nuvem e AZs individuais.

Para garantir a escalabilidade, os seguintes princípios devem ser seguidos:

1. As soluções precisam ser projetadas para oferecer suporte à escalabilidade AZ única, de modo que instâncias adicionais dos componentes que compõem a solução possam ser adicionadas ou removidas sem afetar a funcionalidade, como componentes sem estado, balanceamento de carga, armazenamento de dados e particionamento.

2. As soluções precisam ser projetadas para oferecer suporte a várias escalabilidades do AZ, de forma que instâncias adicionais da solução, cada uma em um AZ separado, possam ser adicionadas ou removidas, como o balanceamento de carga e a sincronização de dados inter-AZ.

3. A infraestrutura de nuvem na qual as soluções estão em execução precisa utilizar o software de monitoramento para que situações de sobrecarga possam ser detectadas e recursos adicionais de computação e armazenamento possam ser implantados para lidar com o aumento da carga.

4. As próprias soluções também precisam ser monitoradas para que recursos adicionais possam ser colocados on-line na presença aumento de cargas de trabalho.maneira redundante para alta disponibilidade.

MONITORAMENTO

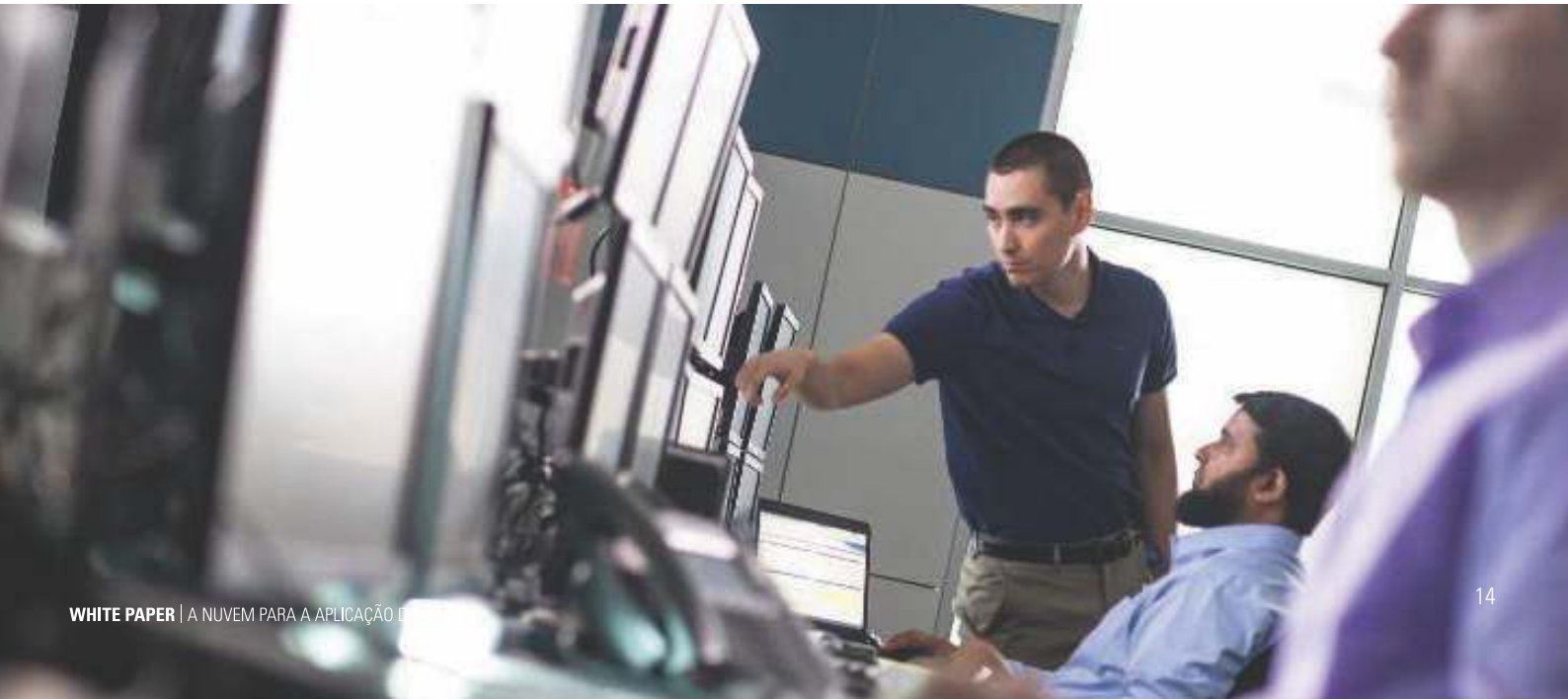
O monitoramento é outro aspecto crítico das soluções operacionais na nuvem. Em implantações que podem consistir em centenas ou milhares de recursos, incluindo servidores, bancos de dados e aplicativos baseados em nuvem, o monitoramento eficaz permite que você tenha insights sobre o status, a integridade e as tendências gerais existentes nesses recursos.

O monitoramento apresenta três desafios principais: determinar quais recursos e métricas devem ser monitorados, decidir como esses dados serão coletados em uma ferramenta de monitoramento e como os alertas de erros são manipulados. Os provedores de serviços em nuvem normalmente fornecem ferramentas básicas de monitoramento que podem ser usadas para coletar e visualizar dados gerados por seus serviços. As APIs publicadas por esses fornecedores permitem que os provedores de soluções SaaS exportem seus próprios dados internos para a plataforma de monitoramento de nuvem. No entanto, esses serviços de monitoramento de nuvem pública geralmente são básicos e devem ser aumentados com alguma combinação de ferramentas comerciais ou de código aberto.

Depois que os registros e métricas tiverem sido identificados e as ferramentas estiverem prontas para coletar os dados, é importante entender quanto desses dados você coletará e em que intervalo a coleta ocorrerá. Coletar uma imagem instantânea da utilização da CPU a cada 30 segundos, por exemplo, resulta em quase nenhum impacto em um sistema em execução, mas resultará em uma visão menos precisa do desempenho "quase em tempo real" do que se fosse uma imagem a cada 100 milissegundos. Os dados de log, em particular, podem resultar em conjuntos de dados extremamente grandes, especialmente quando mensagens de depuração (debug) são armazenadas, ou no caso de um grande número de de erros. As soluções em nuvem são naturalmente mais bem equipadas para lidar com essa enorme quantidade de dados, mas o impacto na execução de sistemas, o custo de armazenamento e a granularidade das métricas coletadas sempre devem ser ponderados para garantir que os benefícios superem esses custos.

O aspecto final, e talvez o mais desafiador, de qualquer implementação de monitoramento bem-sucedida é o processo de alertar o pessoal de operações ou os clientes sobre as condições de erro. A configuração de alerta ideal filtra os falsos positivos e as mensagens duplicadas ao mesmo tempo em que notifica os destinatários sobre todas as condições de erro válidas para que eles possam responder de maneira eficaz e em tempo hábil. Essa deve ser uma área de foco fundamental de qualquer organização que esteja lançando produtos ou serviços na nuvem.

Registros, eventos e métricas podem ser agregados para fornecer uma imagem do estado atual dos recursos físicos e de software. No entanto, a medida final de entrega e disponibilidade bem-sucedida é a capacidade real do usuário final de usar um aplicativo. Os provedores de soluções SaaS normalmente oferecem garantias de disponibilidade aos clientes na forma de Acordos de Nível de Serviço (SLAs). Os SLAs geralmente especificam a disponibilidade esperada de soluções geralmente expressas na forma de uma porcentagem, conforme explicado acima, com créditos garantidos ou mesmo reembolsos, caso o fornecedor não atenda ao SLA em um determinado período de tempo. O monitoramento eficaz ajuda a suportar os relatórios de SLA ao fornecer uma trilha de auditoria de operações bem-sucedidas.



VANTAGENS POR MODELO

	NO LOCAL	NUVEM	HÍBRIDO
CUSTO	• As implantações no local são normalmente estruturadas como um gasto de capital único, eliminando a necessidade de custos mensais recorrentes. • O hardware (servidores) de propriedade pode ser virtualizado e compartilhado para outras necessidades internas a critério do proprietário.	• Os custos da solução SaaS são classificados como OPEX, reduzindo a necessidade de aprovação de grandes investimentos durante um determinado ano. • Os custos de armazenamento na nuvem continuam diminuindo. Armazenamento extra pode ser disponibilizado sem hardware para aquisição. • Os custos de suporte / manutenção estão inclusos nos custos mensais e não como uma taxa adicional, facilitando o orçamento.	As soluções híbridas, dependendo de sua configuração, geralmente incluem muitos dos benefícios de soluções locais e na nuvem, além do seguinte: • O híbrido permite uma maneira mais barata de adicionar recursos a um sistema existente no local.
SEGURANÇA	• A segurança pode ser altamente personalizada para os processos, requisitos e requisitos regulamentares de uma organização individual. • O conhecimento do sistema e dos dados reside apenas internamente. Pode ser preferível para agências com necessidades de segurança em que não desejam dados "embaralhados" pela Internet ou que desejam restringir totalmente o acesso à Internet a seus sistemas, bancos de dados ou aplicativos.	• Segurança física, segurança de infraestrutura e segurança de aplicativos são gerenciados pelo comprador. • Um grau mais alto de resiliência cibernética ajuda a evitar ataques direcionados e sustentados de negação Negação Distribuída de Serviço (DDoS), mantendo os serviços disponíveis quando o comprador mais precisa deles. • Certificações mais avançadas significam que o comprador não precisa se preocupar com conformidades, como DoD, FIPS, ISO e outras específicas do país. • Provedores de serviços em nuvem monitoram ativamente e com êxito ameaças contra o comprador, e os alertam sobre possíveis preocupações.	• Vários controles de segurança podem ser implementados no local para atender necessidades específicas que a nuvem não prevê.
IMPLANTAÇÃO E ESCABILIDADE		• Normalmente, as soluções em nuvem podem ser implantadas em questão de dias (semanas / meses para mais personalização), porque o hardware e o software não precisam ser instalados no local. • Soluções em nuvem são altamente escalonáveis. As organizações podem simplesmente solicitar mais lugares ou armazenamento e recebe-lo rapidamente. • Atualizações de software e correções de "bugs" podem ser feitas com mais frequência, com a capacidade de reverter com mais facilidade quaisquer alterações. • As soluções em nuvem normalmente exigem menos envolvimento de TI e menos habilidade técnica interna para implantação, atualizações e alterações.	• A infraestrutura local pode suportar cargas de trabalho médias com a capacidade de aproveitar a nuvem para circunstâncias de failover nas quais a carga de trabalho excede o poder dos recursos no local. • Dados críticos de uma solução local podem ser replicados para um ambiente de nuvem em um local diferente dos sistemas primários para garantir a continuidade dos negócios em caso de falha crítica.
A ACESSIBILIDADE DO USUÁRIO	• Os sistemas locais podem ser executados sem acesso à Internet. Isso é útil para manter os aplicativos essenciais em execução, principalmente em áreas onde a conectividade com a Internet não é confiável.execução de aplicativos de missão crítica - especialmente em áreas onde a conectividade com a Internet não é confiável.	• Soluções em nuvem exigem conectividade com a Internet. Com a banda larga com e sem fio ficando mais barata e disponível em praticamente qualquer lugar, ela oferece fácil acesso para funcionários remotos por meio de múltiplos dispositivos.	

5

MANTENDO COMUNIDADES SEGURAS

Os departamentos de polícia enfrentam muitos desafios, desde uma explosão de dados, mobilidade e IoT, até o recrutamento, retenção e treinamento de oficiais. A tecnologia deve ajudar a aliviar os desafios e tornar os funcionários mais eficazes sem adicionar novos encargos, mas sistemas desatualizados e que mantêm as informações incomunicáveis podem reduzir a capacidade de derivar e fornecer inteligência de maneira eficaz da maneira necessária.

Para ter certeza de que as soluções SaaS baseadas em nuvem são adequadas para o comprador e seu departamento, é importante entender como essa tecnologia se adequa e melhora seus sistemas existentes e como selecionar com responsabilidade o fornecedor certo. Seguindo uma estrutura que ajuda a avaliar corretamente a segurança, a disponibilidade, a escalabilidade e o monitoramento do sistema, o comprador pode confiar na escolha da solução de nuvem correta.

De fato, as agências voltadas para o futuro estão percebendo que as soluções SaaS baseadas em nuvem, devidamente avaliadas e selecionadas de maneira inteligente, podem melhorar drasticamente o gerenciamento e utilização de dados. Com essas soluções em funcionamento, os dados se transformam de um fardo para um motor que alimenta as estratégias de policiamento controladas por dados que mantêm nossas comunidades e oficiais mais seguros.

Referências

1. "Era Digital um ponto de viragem para o policiamento, afirma o comissário Leppard", ComputerWeekly, Maio 14, 2015, notícias Http://www.computerweekly.com//4500246279/Idade Digital-a-ponto de viragem-para-policiamento-diz-comissário-Leppard
2. "Millennials: PwC no trabalho Https://www.pwc.com/gx/en/managing-tomorrows-people/future-of-work/assets/reshaping-the-workplace.pdf"
Motorola Soluções

MOTOROLA SOLUTIONS