Technology Solutions | Security

Microssegmentação

Entenda como fortalecer a sua rede utilizando métodos especializados para identificar e proteger segmentos críticos, garantindo maior segurança e eficiência.

Fernando Pierobon

Segmentação? Ok! Mas e a Microssegmentação?

A segmentação de rede é uma prática antiga, difundida e bem compreendida no modelo tradicional de infraestrutura. Há alguns anos, tínhamos um data center físico (possivelmente redundante, configurado em alta disponibilidade) com diversas VLANs e um NGFW como gateway.

As regras eram baseadas em protocolos e portas ou aplicações específicas, e criadas no firewall, que segmentava o ambiente por servidores (físico ou virtual) e subnets.

Esse modelo, como o conhecíamos, em um espaço físico, único e seguro, ficou para trás!

A(s) cloud(s) são uma realidade para a maioria das empresas - incluindo as públicas. A adoção de IaaS, por exemplo, busca agilizar os serviços, novos desenvolvimentos e expansões.

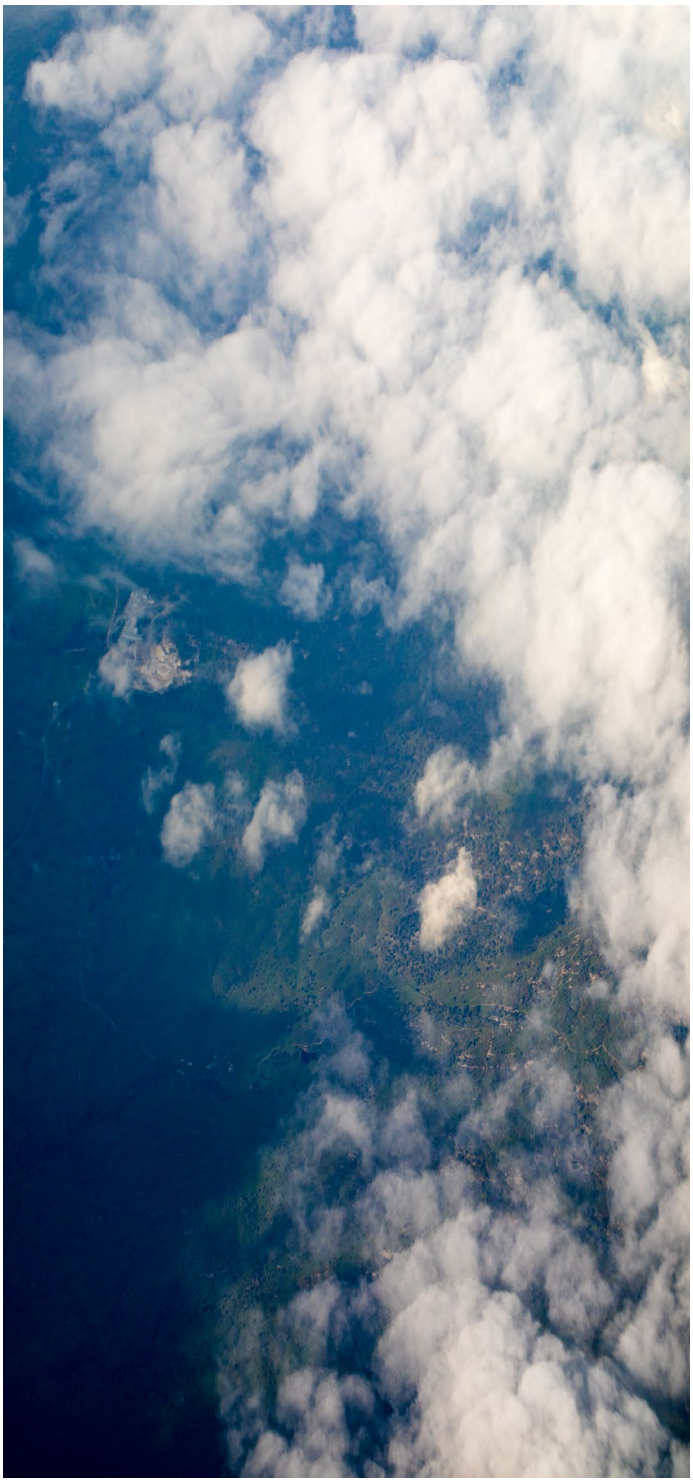
O data center moderno é cada vez mais heterogêneo, com ambientes e tecnologias diferentes, combinando servidores físicos, máquinas virtuais e contêineres, em instalações locais, nuvens privadas e públicas. Essas instalações são dinâmicas, com as empresas transferindo e migrando dados e cargas de trabalho conforme as demandas surgem.

Essa agilidade é um dos vários benefícios das clouds - além de elasticidade e escalabilidade. Mas, por outro lado, a complexidade é muito maior com a descentralização da infraestrutura, já que agora temos que administrar vários ambientes diferentes. Isso ocasiona uma perda de visibilidade e consequentemente compromete a segurança.

No caso de empresas que adotam multicloud (mais de um provedor), a equipe de TI tem que lidar com padrões variados, e as ferramentas tradicionais de segurança, projetadas para servidores e endpoints, não conseguem lidar com esse cenário misto e complexo.

Os vazamentos de informação e ataques recentes mostram que os invasores estão conseguindo tirar proveito dessa situação, e eles investem tempo se movendo lateralmente dentro do ambiente.

Não podemos esquecer ainda que qualquer um pode ser um insider! Um colaborador, motivado por ideologias, vingança ou apenas para ganhos financeiros, pode facilitar a entrada de um malware no ambiente da empresa!



Indiscutivelmente, esse cenário atual é o maior desafio das equipes de TI na última década.

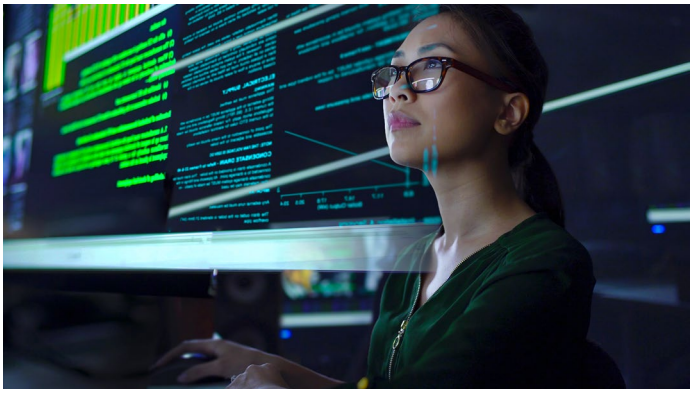
O Gartner define a microssegmentação como “o processo de implementação de isolamento e segmentação para fins de segurança dentro do data center virtual.” A microssegmentação ainda “reduz o risco de propagação lateral de ataques avançados e permite que as empresas apliquem políticas de segmentação baseadas em cargas de trabalho on-premises e na nuvem.”

Com a microssegmentação, é possível criar regras que protegem o tráfego de aplicativos com contexto adicional - como atribuição a nível de processo - independentemente do local onde essas aplicações residem (on-premises ou clouds).

Essas regras determinarão qual processo, dentro de qual servidor poderá se comunicar com qual outro processo, em um outro servidor.

De forma prática, estamos construindo uma regra que irá liberar a comunicação de um servidor a outro, na porta ‘x’ para um processo específico. Qualquer outra aplicação, nesses mesmos servidores, não terá esse tráfego liberado nessa porta.

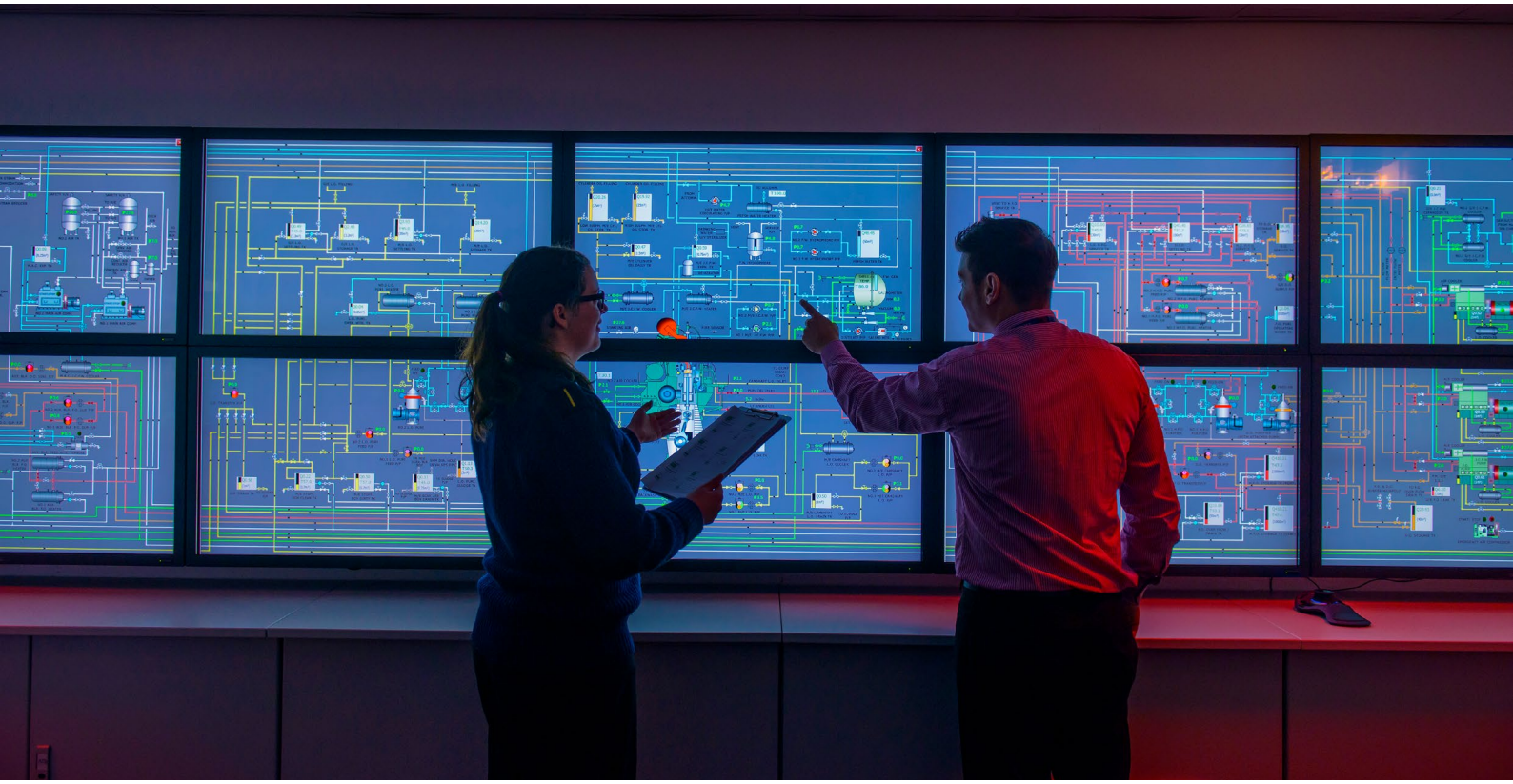
Estamos assim, microssegmentando nosso ambiente.



Uma solução completa deve ser independente de infraestrutura (firewalls e roteadores) e atuar fim a fim, a partir do endpoint. Ela precisa proteger os aplicativos à medida que se movem de um ambiente para outro (entre clouds ou on-premises).

As políticas criadas no nosso exemplo anterior vão possibilitar que um servidor se movimente de forma livre entre clouds e data center, mantendo suas regras e segurança. Isso vale para máquinas físicas, virtuais ou contêineres.

No conceito de Zero Trust, a microssegmentação permite que verifiquemos o acesso, autorizando o menor nível de privilégio possível e nunca assumindo confiança (em um servidor, aplicação ou protocolo de rede).



Outro ponto importante é:

Você sabe o que suas aplicações estão fazendo?

Os benefícios de uma solução de microssegmentação vão muito além de aumentar a segurança do seu ambiente. Os times de redes, servidores e desenvolvimento também ganham um suporte para descobrir os apps instalados, mapeando a comunicação de cada carga de trabalho, integrando com ferramentas de identidade e CMDB, em uma plataforma única e centralizada para todo o ambiente on-premises e multi-cloud.

Dessa forma, a microssegmentação permite entregar visibilidade completa de todo o ambiente a nível de processo!

Em uma primeira fase, a solução irá mapear e monitorar todas as comunicações de cada servidor sem afetar os usuários. Já em um segundo momento, poderemos bloquear protocolos e portas que estão abertas para processos não utilizados ou desnecessários, e ajustar as políticas para as necessidades específicas do nosso negócio.

Diferente de um firewall, onde temos que bloquear todo o tráfego e ir liberando individualmente as comunicações, uma solução de microssegmentação mapeia toda a comunicação de um servidor de forma automática. O resultado é apresentado para o administrador, em forma de gráfico ou tabela, que monitora o ambiente e depois aplica a política, efetivando as regras.

Por fim, uma solução líder de mercado deve permitir ainda monitoração e alerta para compliance, notificação de vulnerabilidades e tempo de resposta acelerada para qualquer ameaça que possa estar no ambiente.

**Fernando Mantovani Pierobon é Sr. Security Technical Architect da NTT DATA.*


NTT DATA