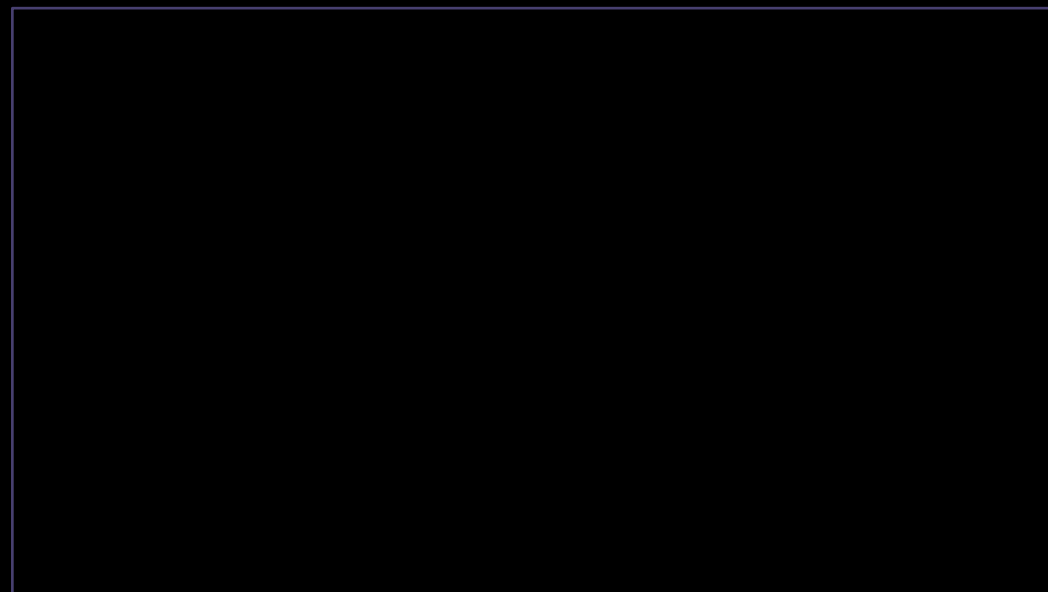




Prime

CCSF

Virtualização e
Segurança da Nuvem



Provedores de Serviços em Nuvem

- ▶ Em vários tamanhos e formas.
- ▶ Provedores de mega-nuvem:

 Amazon;

 Google;

 Microsoft;

 Oracle.

- ▶ É preciso levar em conta preços e termos contratuais.
- ▶ Se algo não estiver no contrato, não será feito.

Provedor de Serviços Gerenciados (MSP)/ Provedor de Serviços de Segurança Gerenciada (MSSP)



MSP – Controla remotamente a infraestrutura de TI.



MSSP - Terceiro que gerencia serviços de segurança.

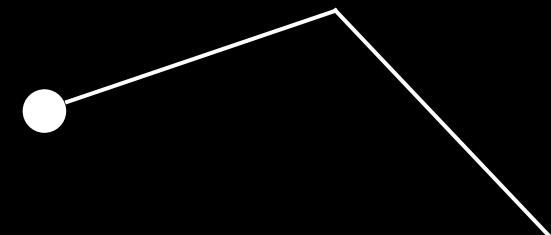
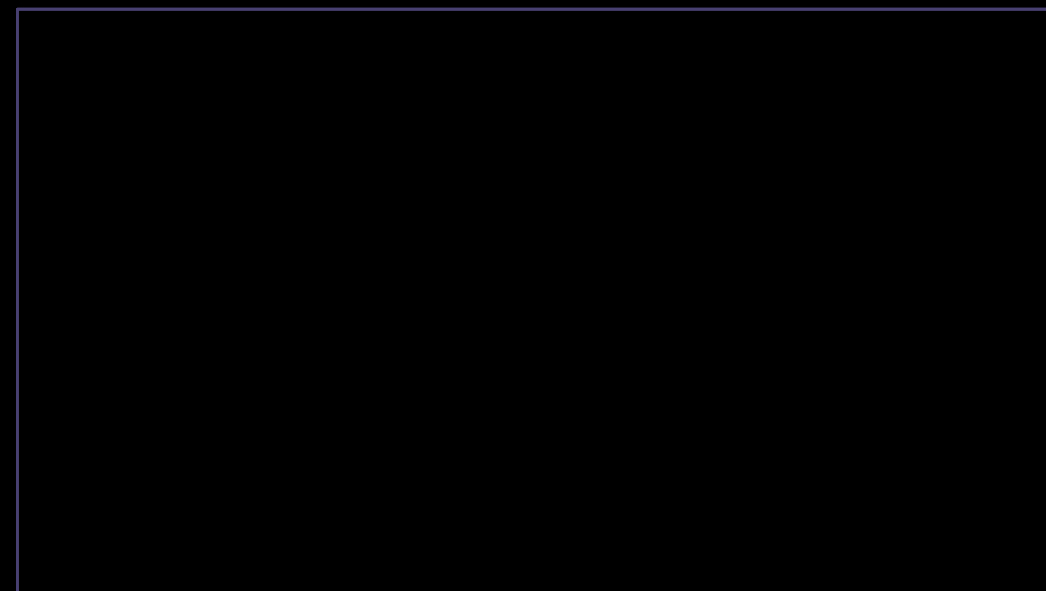


Fornecem força a uma empresa.



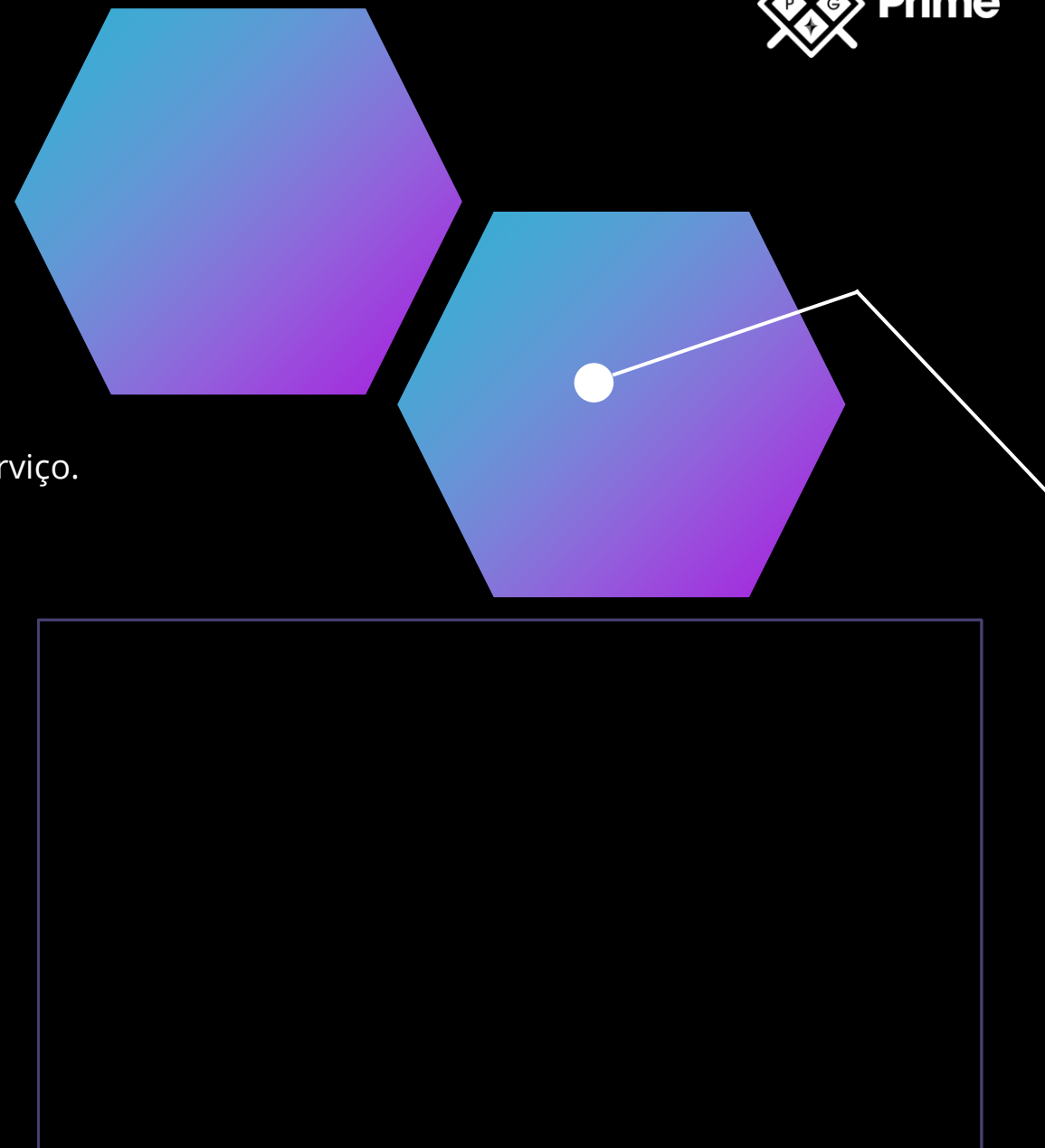
Desvantagens:

- ▶ Falta de flexibilidade;
- ▶ Falta de espaço para qualquer mudança.



On-Premises vs. Off-Premises

- ▶ On-premises = Sistema reside localmente.
- ▶ Pode ser uma máquina virtual (VM), armazenamento ou serviço.
- ▶ A organização tem controle do sistema.
- ▶ Desvantagens:
 -  Requer recursos locais;
 -  Não é fácil de escalar.
- ▶ "Na nuvem": Sistema distribuído em uma infraestrutura de forma remota e acessível por uma rede.



Fog Computing



Uso de computador de outra pessoa.



Desenvolvida pela Cisco.



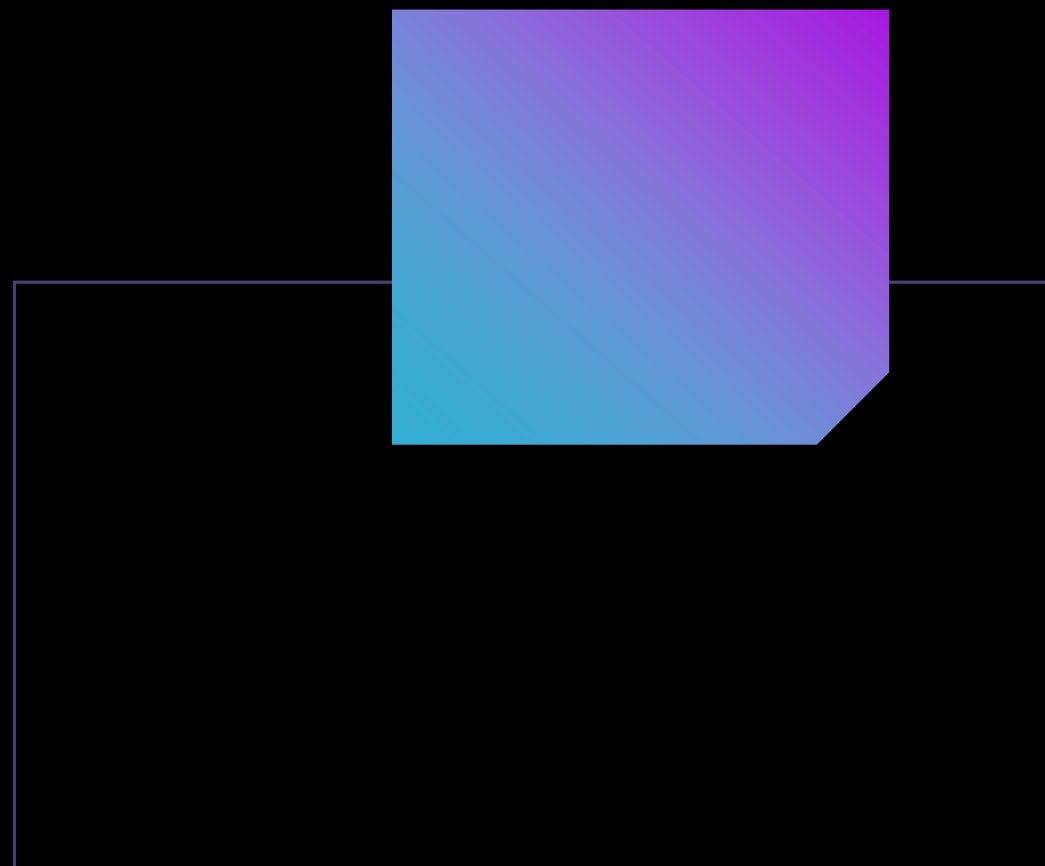
Move parte do trabalho para o espaço local.



Media o processamento entre o hardware local e os servidores remotos.



Complemento da nuvem, e não um substituto.



Computação de Borda



Computação realizada na borda de uma rede.



Impulsionada por quem pode processar na rede e quer novos mercados.



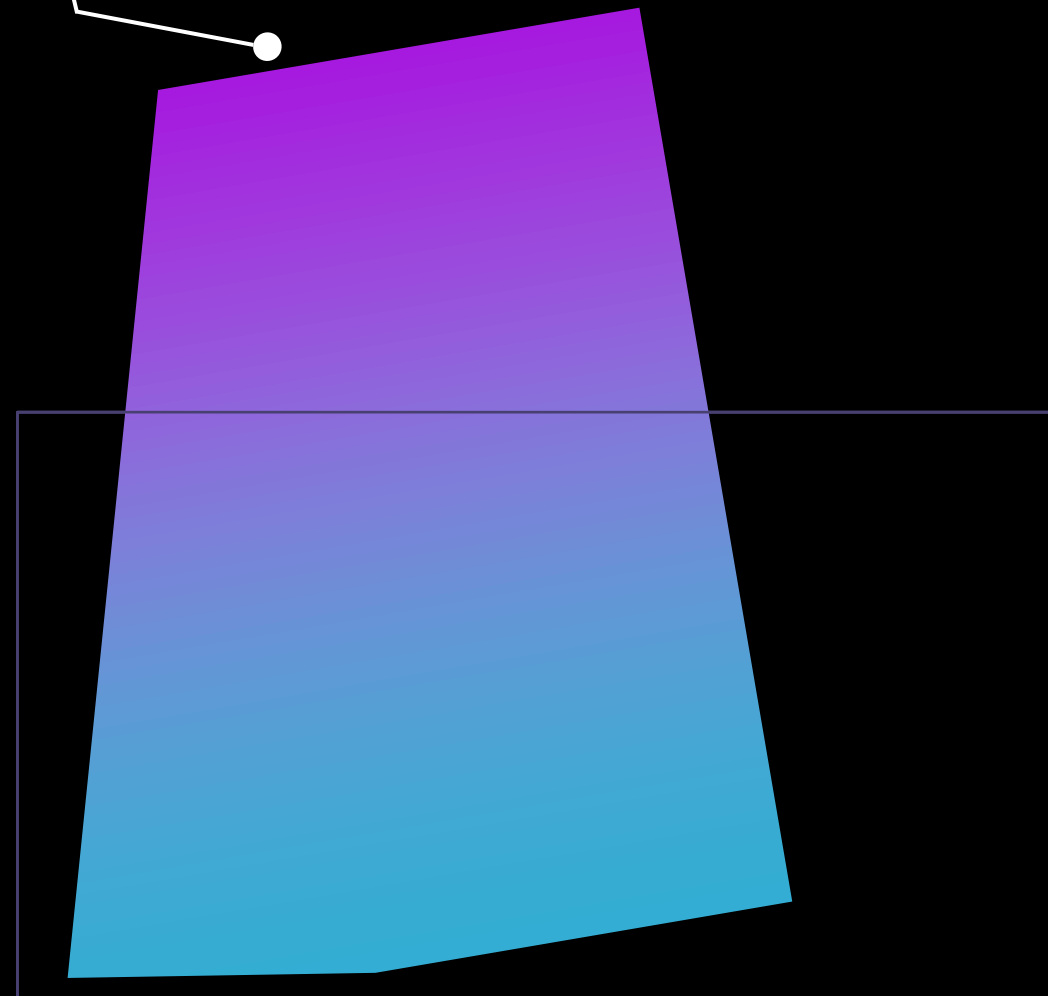
Impulsionada com a Internet das Coisas (IoT).



Depende da "borda" e de um processamento em nível suficiente.



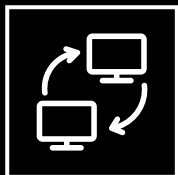
Pode gerenciar o fluxo de dados e fazer a computação no caminho.



Thin Client



Recursos limitados.



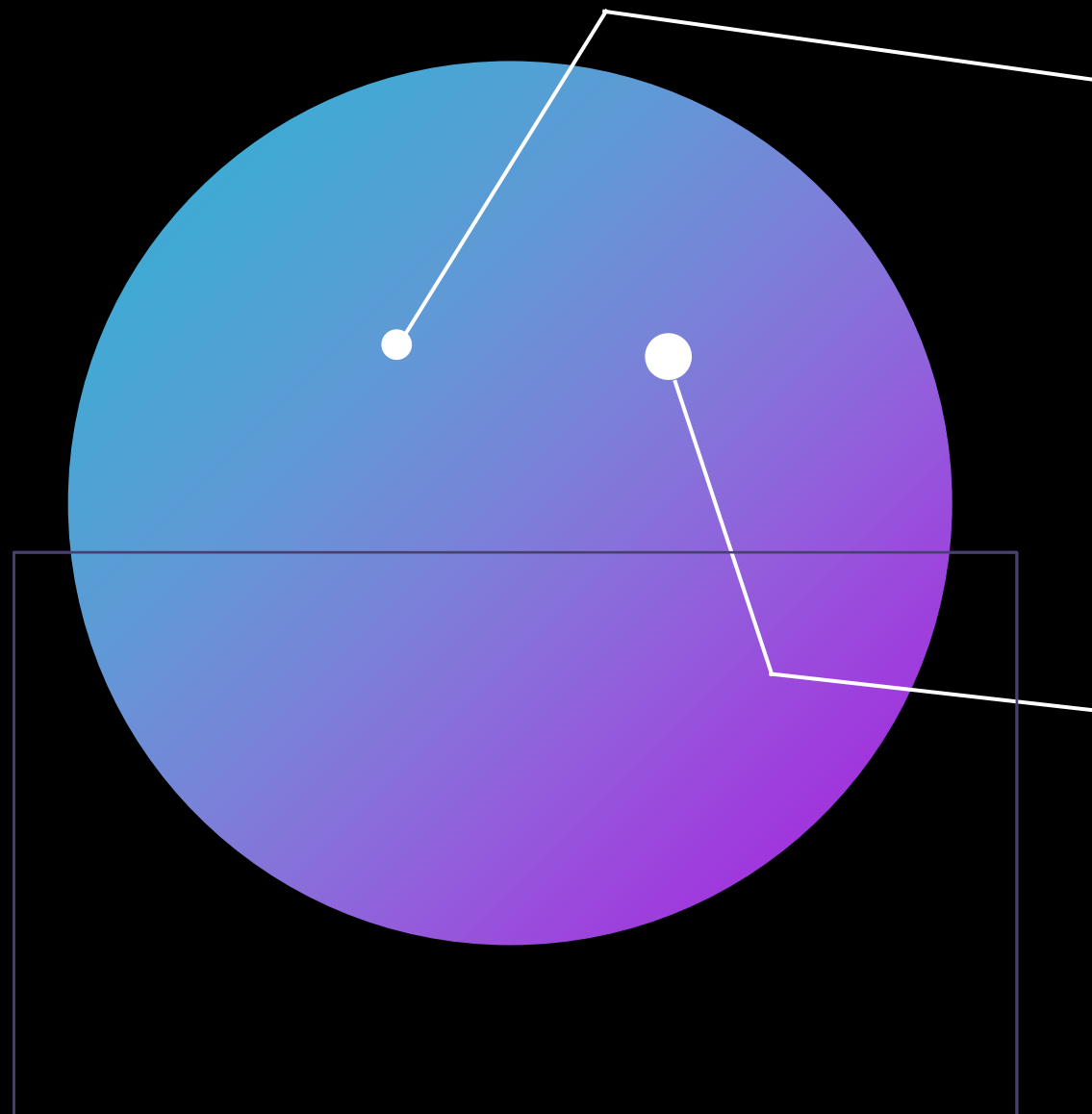
Comunica-se com outra máquina.



Permite o acesso a um servidor com recursos apropriados.



Utiliza computação em nuvem e virtualização.



Contêineres

- ▶ Contém as partes de um sistema operacional separadas do kernel.

- ▶ Permite ter, de forma separada:



Thread de memória;



CPU;



Armazenamento.

- ▶ Evolução do conceito de VM.

- ▶ Agrupado em um pacote:



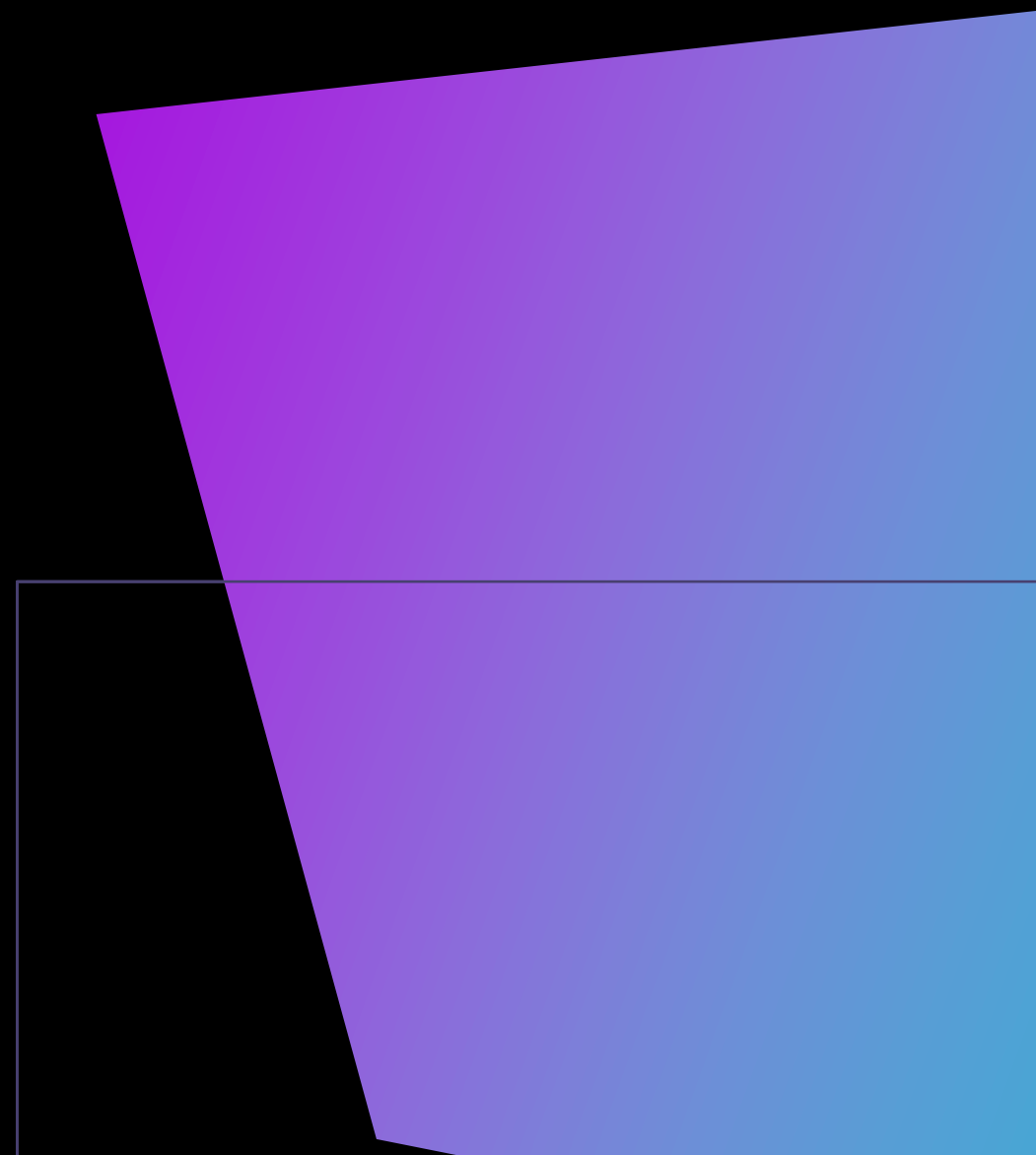
Aplicativo;



Bibliotecas;



Arquivos de configuração.



Microserviços/API

- ▶ API - Meio para especificar como alguém interage com um software.
- ▶ Se ele usa a API de REST, a interface definida é um conjunto de quatro ações em HTTP:



GET;



POST;



PUT;



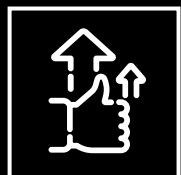
DELETE.

- ▶ Microserviços - Dividem o sistema em pequenos módulos.

Infraestrutura Como Código



Uso de arquivos de definição legíveis por máquina.

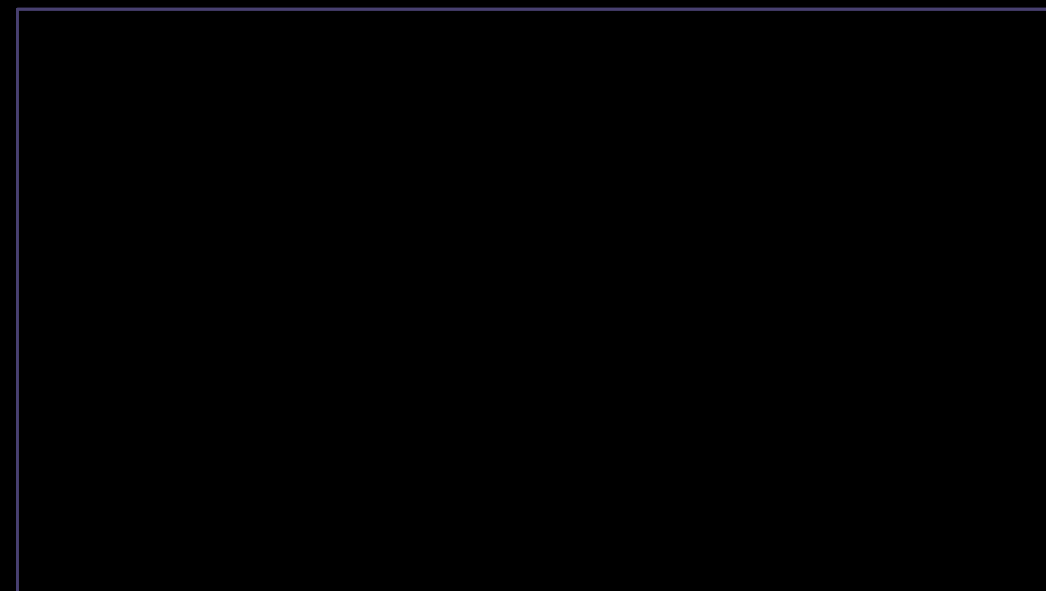


Vantagens:

- ▶ Flexibilidade;
- ▶ Escalabilidade.

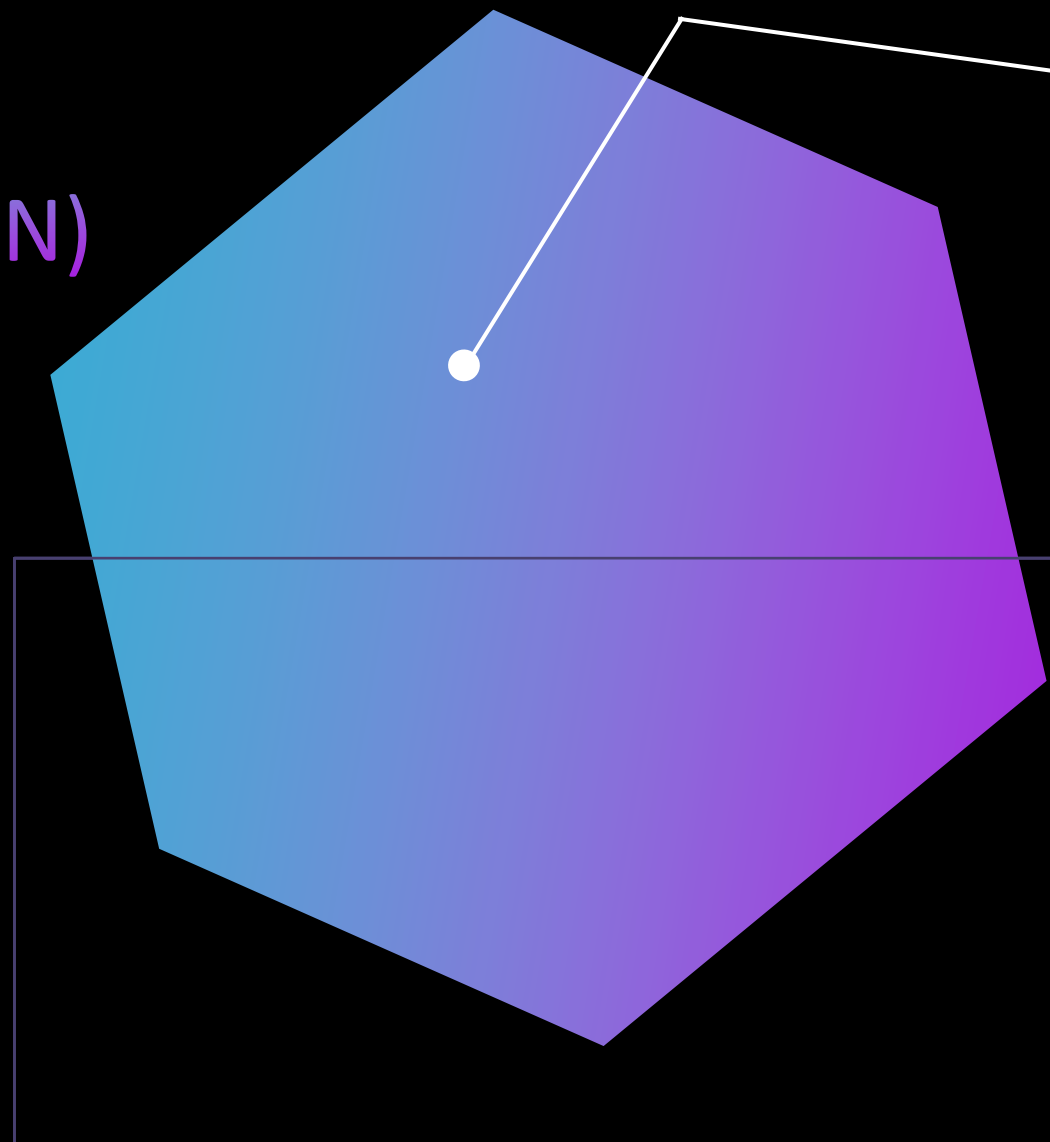


Permite gerenciar hardware físico de forma programática.



Rede Definida por Software (SDN)

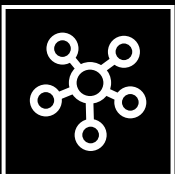
- ▶ Arquitetura na rede na qual o plano de controle e o de dados são separados.
 - ▶ Controle programático.
- ▶ Pilha de programação de rede completa.
 - ▶ Flexibilidade;
 - ▶ Programabilidade.
- ▶ Depende da função de rede (NFV).



Visibilidade Definida por Código (SDV)



Extensão da infraestrutura como ideia de código para o problema de visibilidade da rede.



Feito via código por malha SDN.



Vantagens:

- ▶ Flexibilidade no projeto;
- ▶ Capacidade de reconfiguração.

Arquitetura Sem Servidor

- ▶ A nuvem é um recurso compartilhado.
- ▶ Simplifica e adiciona recursos significativos.
- ▶ Capacidade de pico.

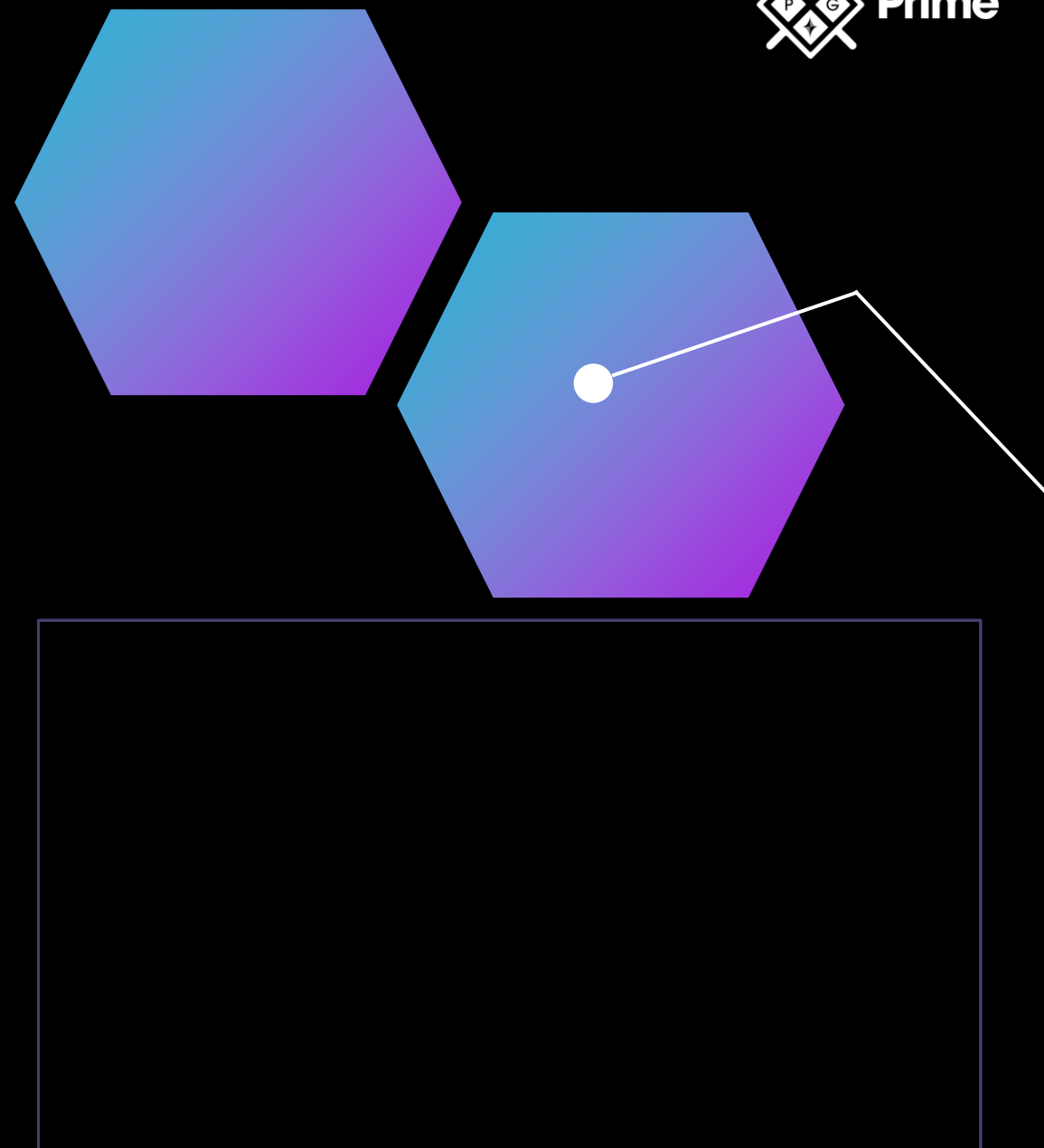
- ▶ Vantagens:



Provedores de nuvem podem fazer alterações por scripts automatizados;



Oferece suporte à integração de serviços.



Integração de Serviços

- ▶ Conexão de elementos de infraestrutura e software.
- ▶ A infraestrutura em nuvem consegue integrar serviços.



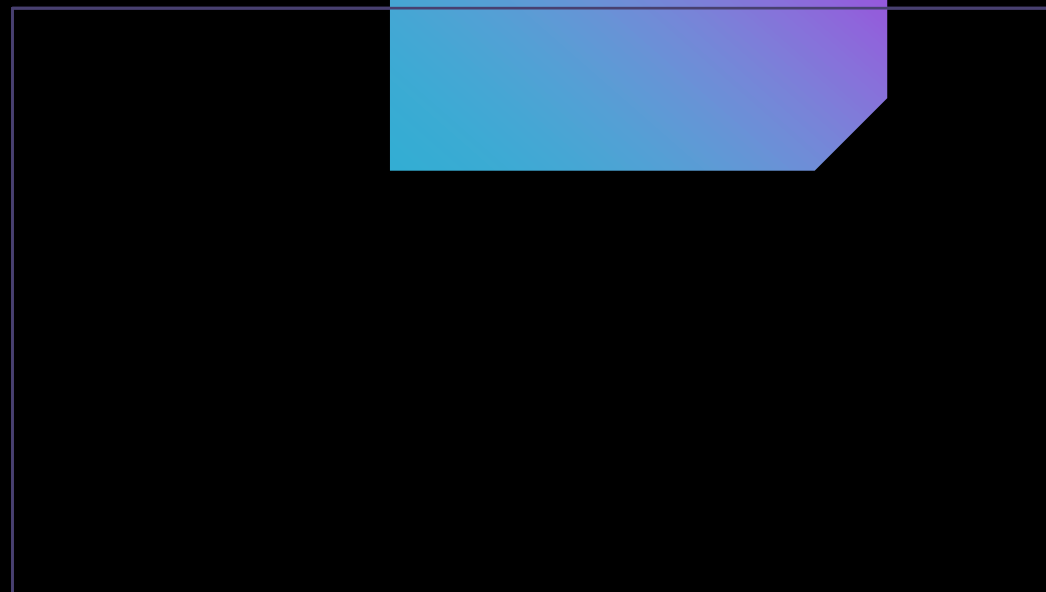
Scripts pré-projetados.



Economia de custos;



Confiabilidade.

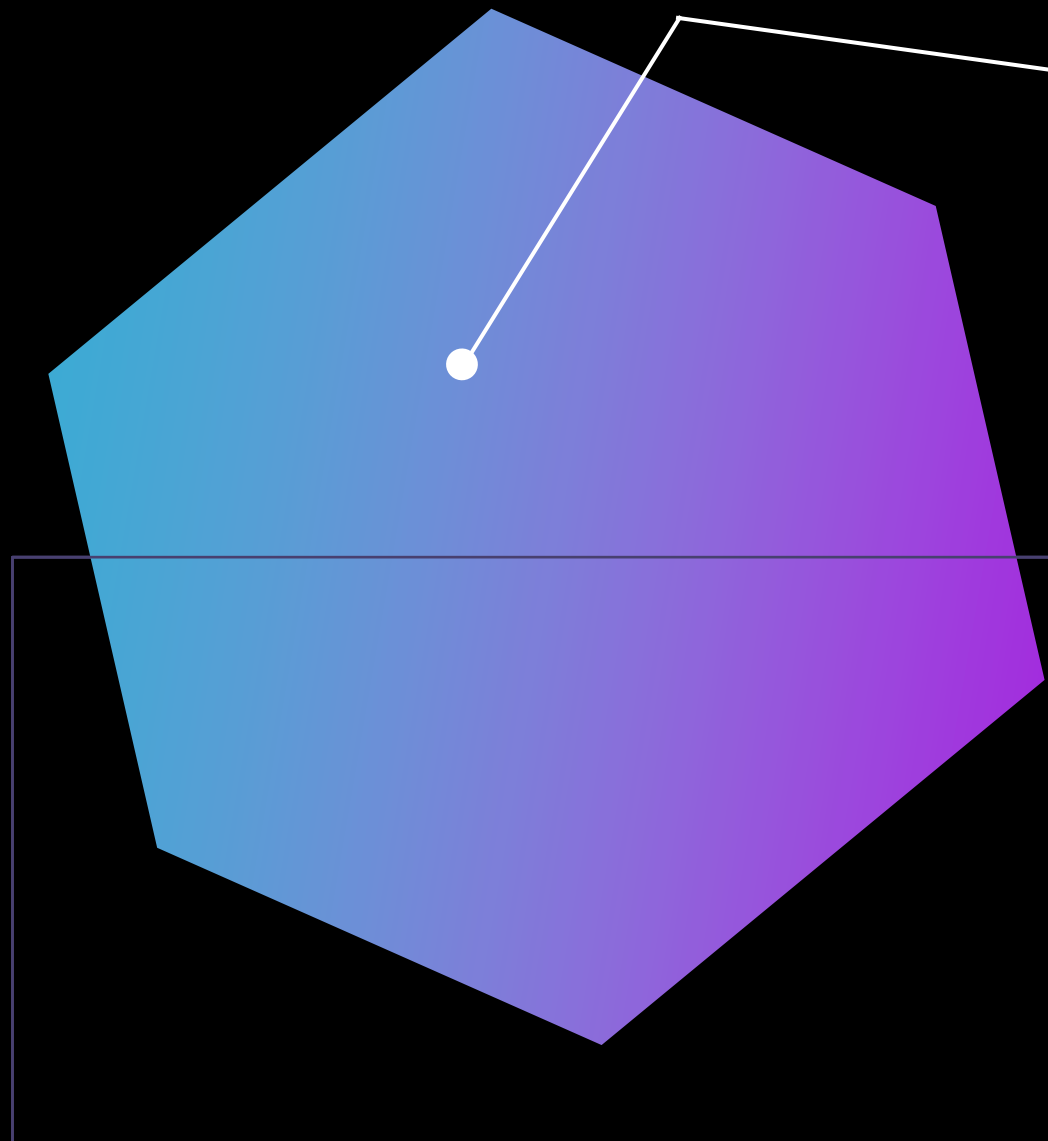


Políticas de Recursos

- ▶ Gerenciamento de recursos é feito através da política de recursos.
- ▶ Cada provedor tem uma maneira de interação com um menu de serviços.
- ▶ Com essa política, você pode:
 -  Definir o que, onde e como os recursos são provisionados;
 -  Definir restrições;
 -  Gerenciar recursos;
 -  Gerenciar custos.

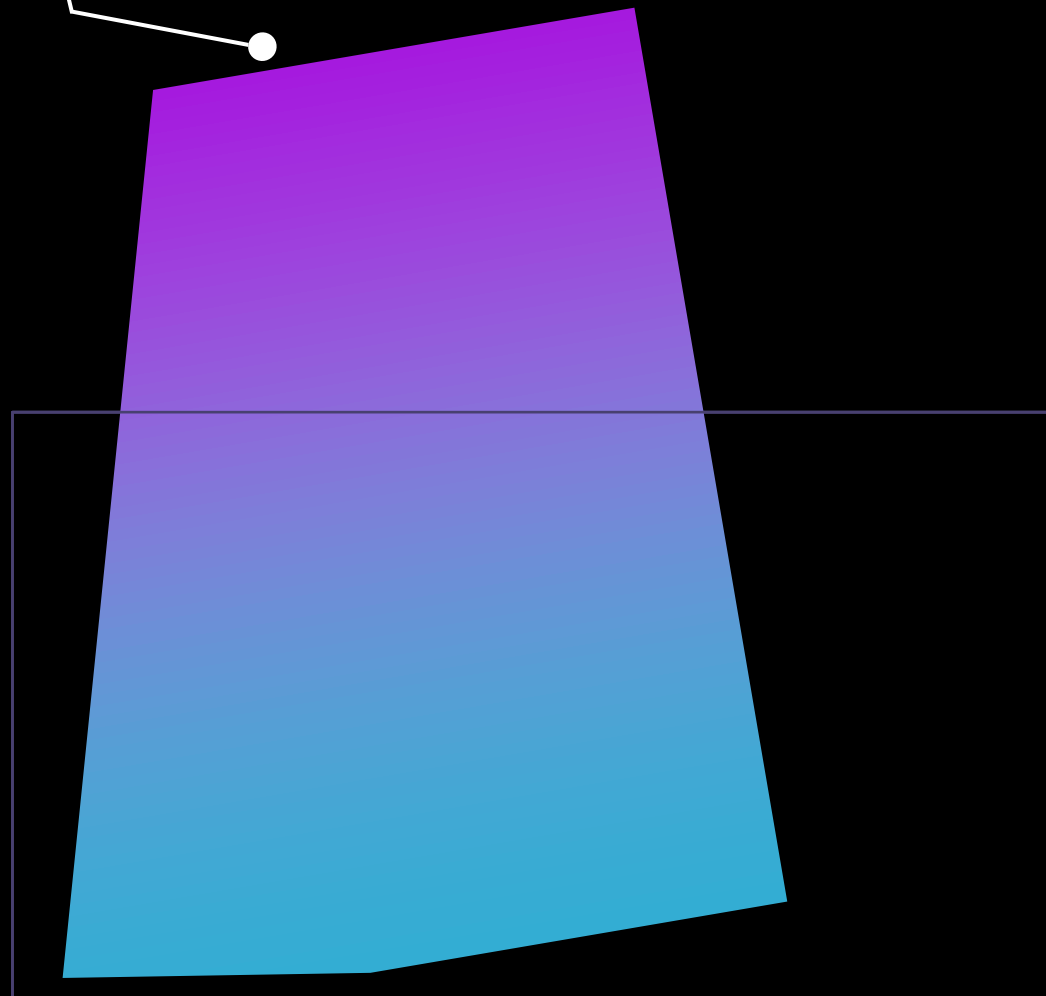
Gateway de Trânsito

- ▶ Conexão para interconectar nuvens privadas virtuais (VPCs) e redes locais.
- ▶ Vantagens:
 -  Definir e controlar a comunicação entre recursos na rede;
 -  Definir e controlar a comunicação entre recursos da própria infraestrutura.
- ▶ Implementados para dar suporte ao ambiente de nuvem.



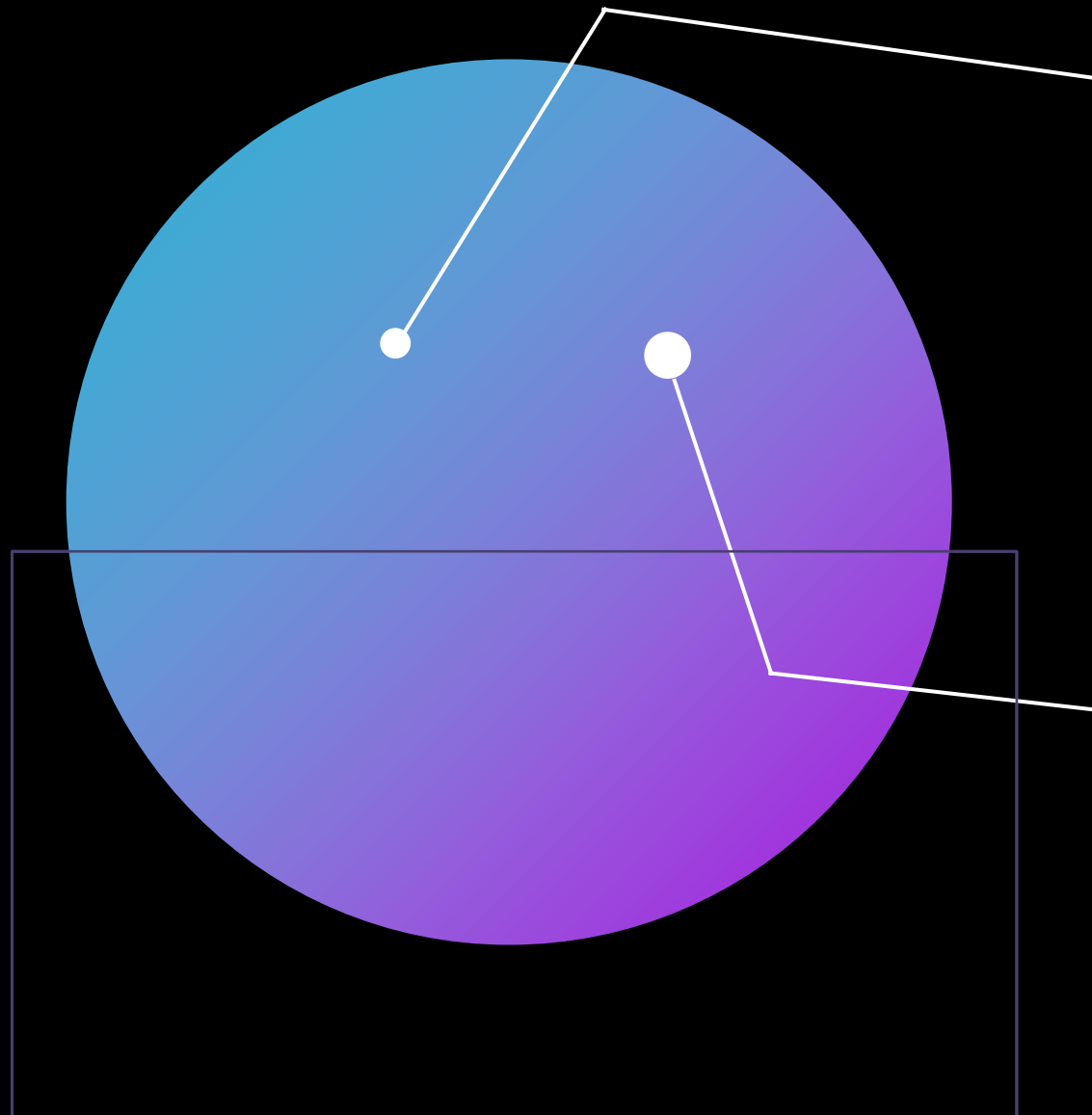
Virtualização

- ▶ Permite que um computador tenha mais de um sistema operacional.
- ▶ Abstração da camada do Sistema Operacional.
- ▶ É preciso empregar um hypervisor.
- ▶ Programa de baixo nível onde vários SOs são executados em um host.
- ▶ Vantagens:
 -  | Separação do software e hardware;
 -  | Melhoria de muitas funções do sistema.
- ▶ Máquinas virtuais = SOs convidados.



Hypervisor Tipo I

- ▶ Executados no hardware do sistema.
- ▶ Velocidade e eficiência.
- ▶ Exemplos:
 - ▶ KVM;
 - ▶ Xen;
 - ▶ Microsoft Windows Server Hyper-V;
 - ▶ Plataformas VMWare vSphere/ESXi.



Hypervisor Tipo II

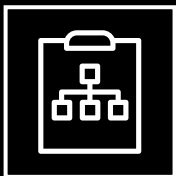
- ▶ Executados em cima de um sistema operacional host.
- ▶ Exemplos:
 -  VirtualBox (Oracle);
 -  VMware Player.
- ▶ Projetados para um número limitado de VMs.



Prevenção de Expansão de Máquinas Virtuais (VM) Sprawl



Disseminação e desorganização por falta de uma estrutura organizacional.



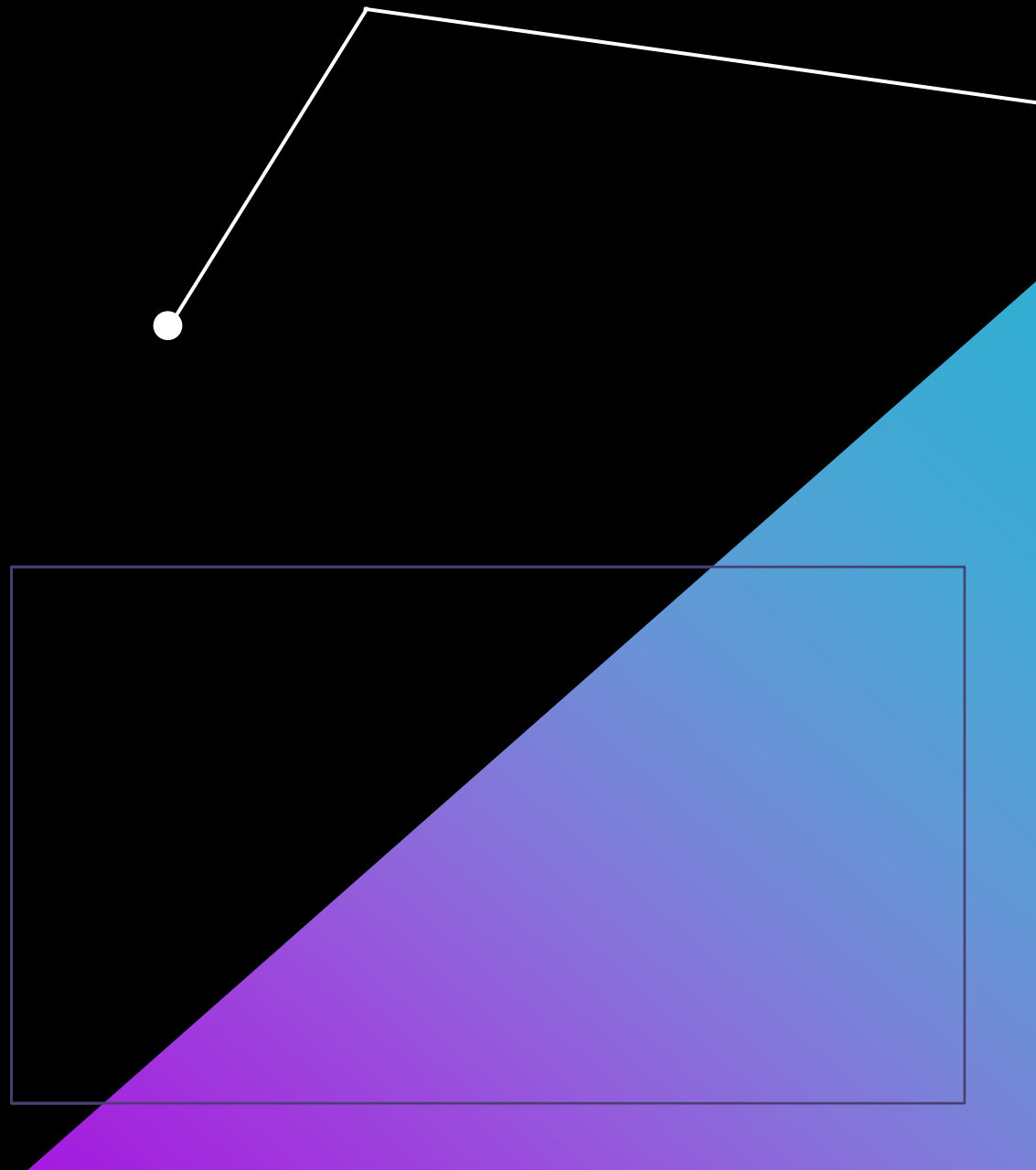
VMs são arquivos com uma cópia das estruturas de disco e memória.



Expansão da VM = Estrutura desorganizada.

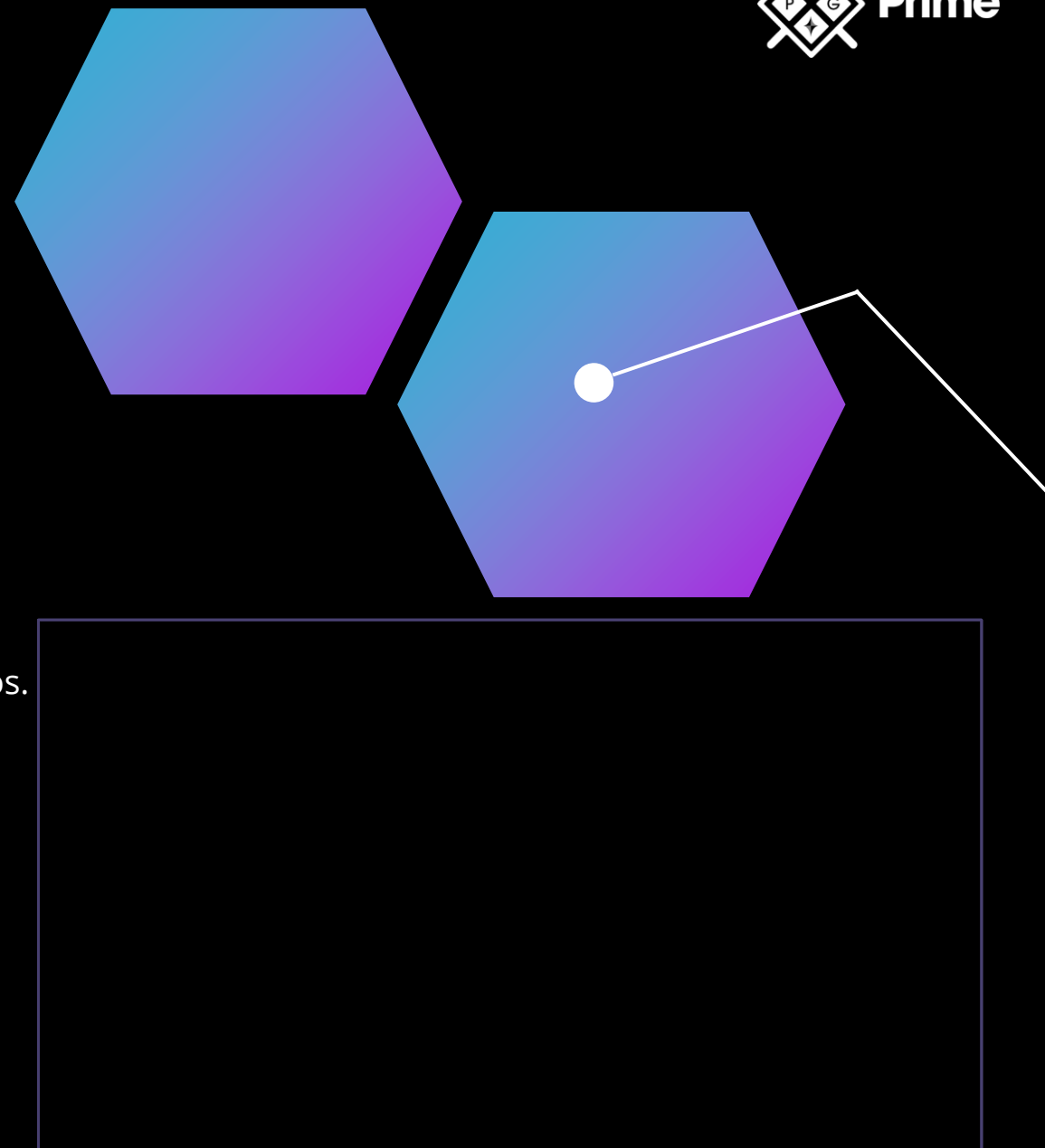


Uma ferramenta de gerenciamento permite que os administradores gerenciem VMs e evitem a expansão.



Proteção Contra Fuga de VM

- ▶ Software, malware ou invasor podem escapar de um VM.
- ▶ Uma fuga pode proporcionar ataques.
- ▶ Ambientes de VM de grande escala têm módulos específicos.
 - ▶ Conseguem detectar fuga;
 - ▶ Fornecem proteção para outros módulos.



OBRIGADO!

VIRTUALIZAÇÃO E
SEGURANÇA DA NUVEM