splunk>

Instituto Infnet

Integrantes:
Nicolas Marcos, Fabio Machado e Allan Andrade

Conhecendo o Splunk

O Splunk é uma das mais famosas plataformas de análise e monitoramento de ambientes em tempo real, permitindo pesquisas, análises, dashboards e reports.

O Splunk é o mecanismo de coleta, indexação e reconhecimento automático de padrões de informação considerada como dado de máquina.

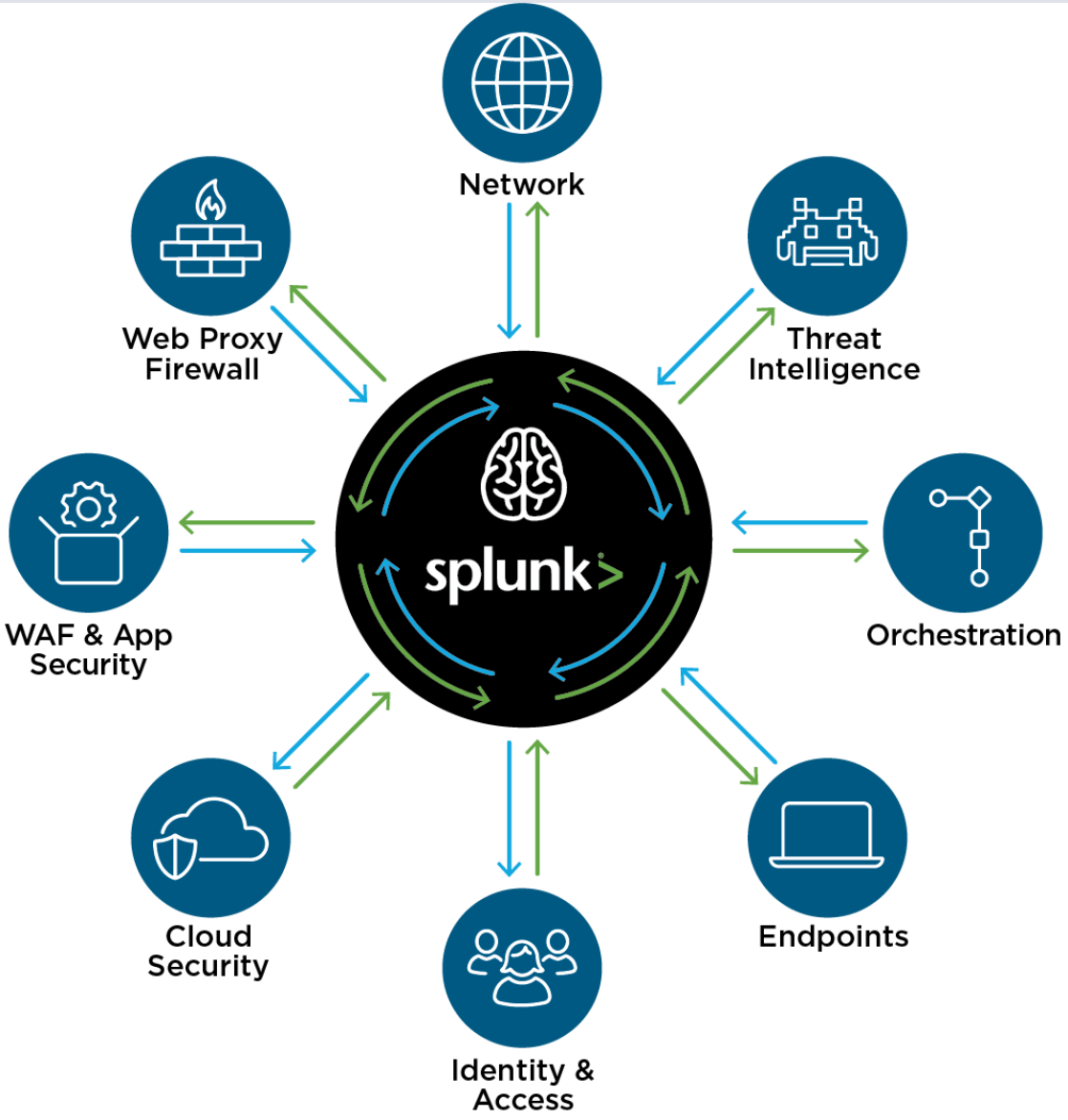
O Splunk não utiliza conectores, não utiliza qualquer tipo de bancos de dados por trás e nem impõe limite em relação ao volume de coleta e indexação de informação, já que estamos falando de uma ferramenta de Big Data.

Conhecendo o Splunk

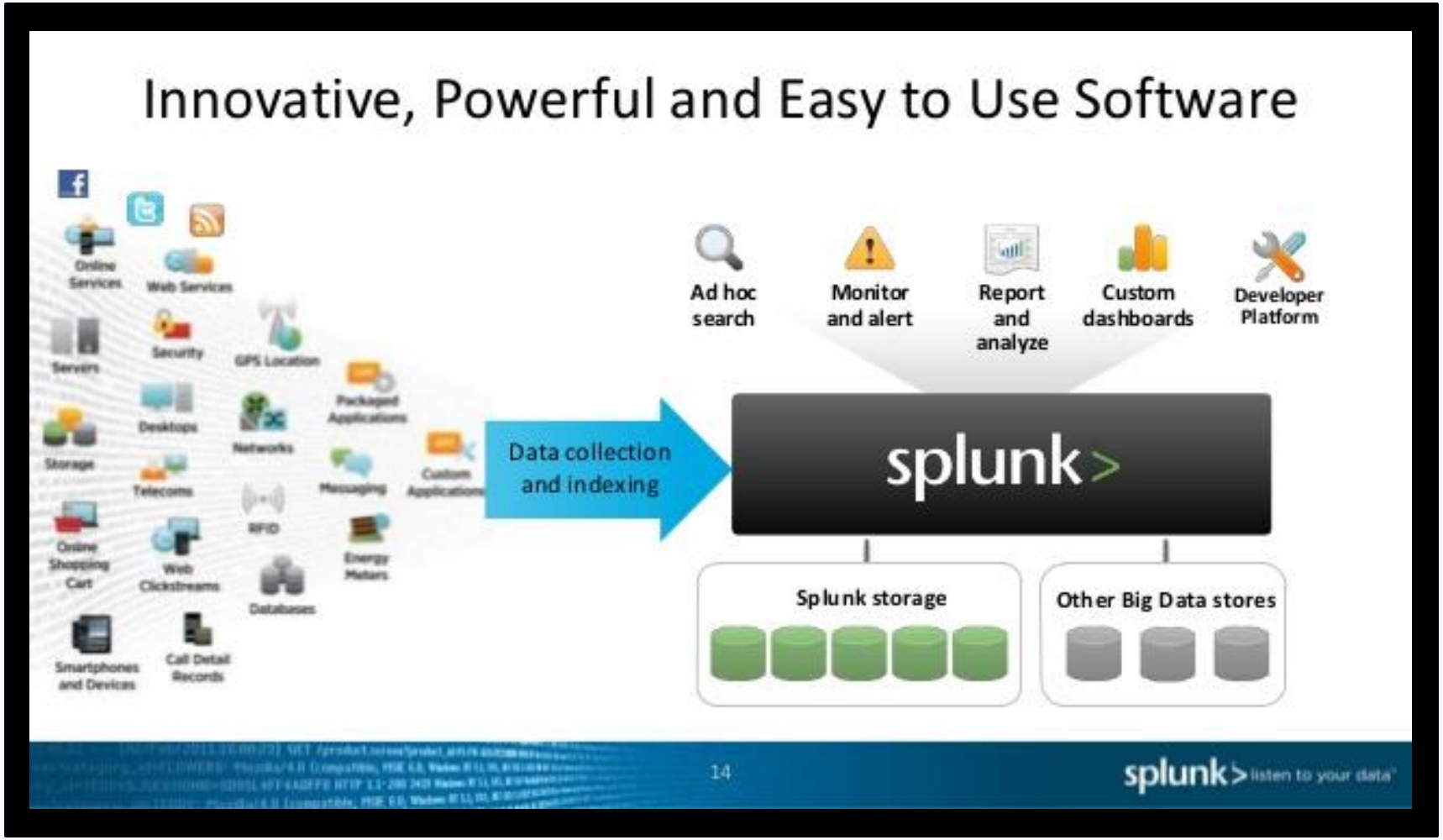
O Splunk realiza a captura, indexação e correlação dos dados em tempo real em um contêiner pesquisável.

Splunk é uma tecnologia usada para gerenciamento, segurança e conformidade de aplicativos, além de análises de negócios e da web.

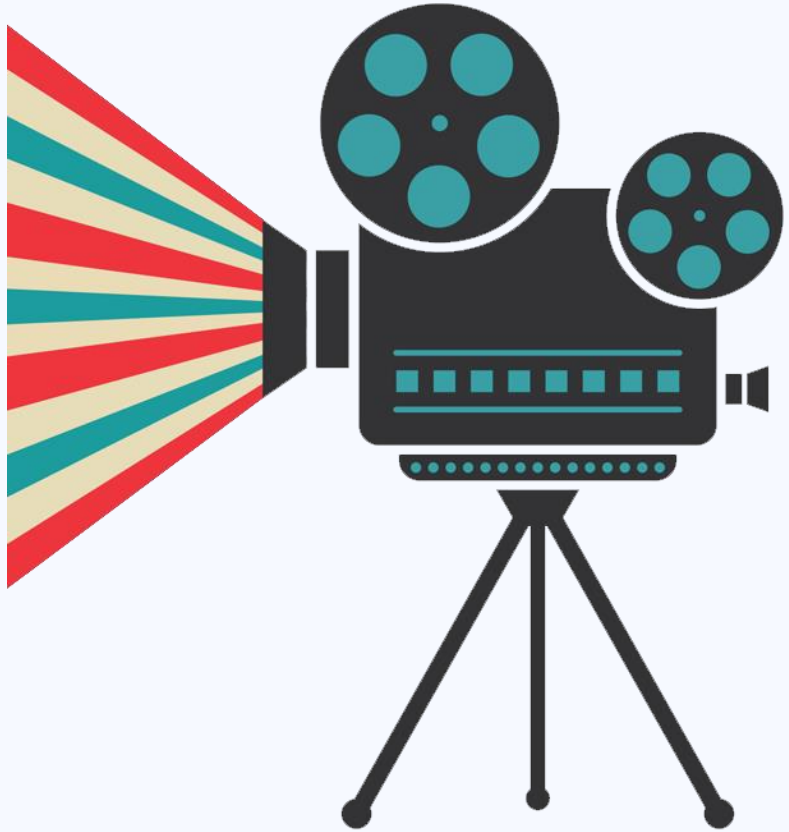
Splunk analisa os dados gerados pela máquina para fornecer inteligência operacional.



Como Splunk funciona?



Como Splunk funciona?



Armazenamento – “Buckets”

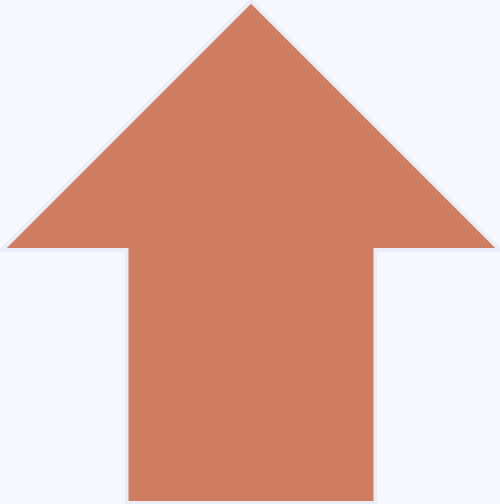
- Eventos mais recentes
- Se Hot bucket não atinja 1/10GB, em 90 dias migrará para Warm

- Buckets maiores que 1/10GB. Splunk poderá contar com até 300 Warm buckets. Criado o Warm bucket número 301, o mais antigo será migrado para Cold;

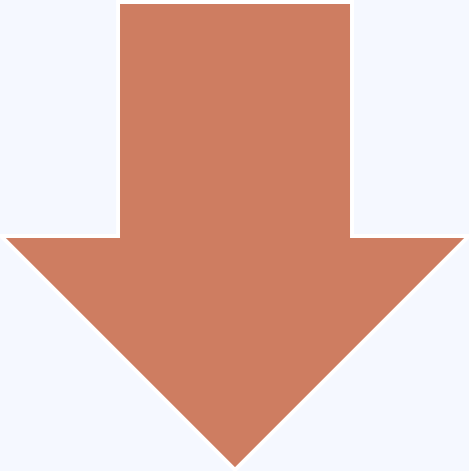
- Migrados de Warm podendo chegar até 500 GB antes de migrar para Frozen
- Atingindo seis anos serão migrados para Frozen;

- Splunk exclui permanentemente todos migrados de Cold para Frozen. É possível editar o arquivo para que essa remoção não ocorra.

Thawed



Estágio do descongelamento dos dados ou buckets. Estavam em um formato de Frozen antes do arquivamento e agora serão posicionados no diretório de Thawed buckets



Após colocar os Frozen buckets como “descongelados” no diretório citado, eles podem ficar o tempo que for necessário, e quando não os quiser mais, basta excluí-los

Empresas que utilizam o Splunk

AIRBUS HYATT Carnival PORSCHE

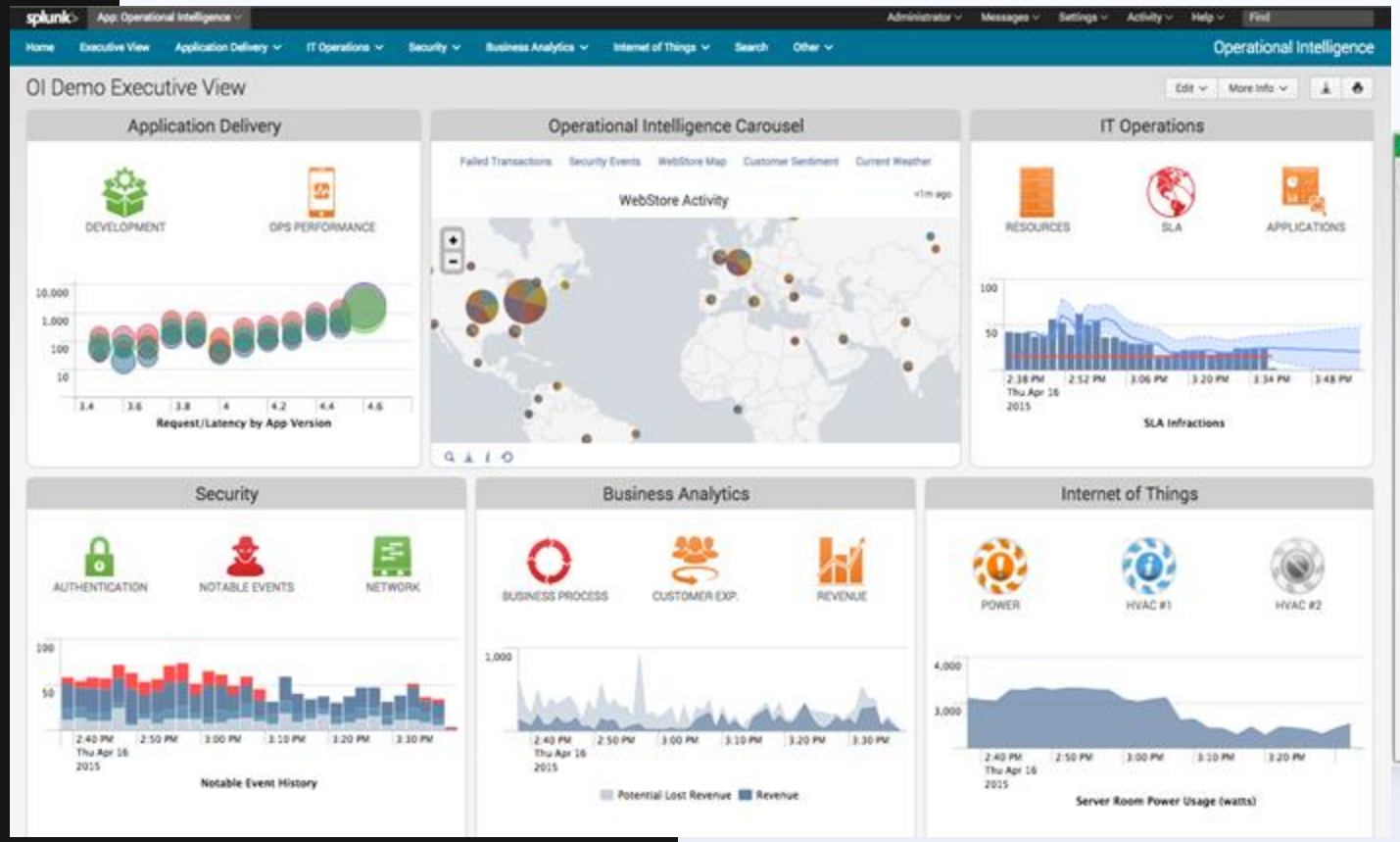
Empresas que utilizam o Splunk

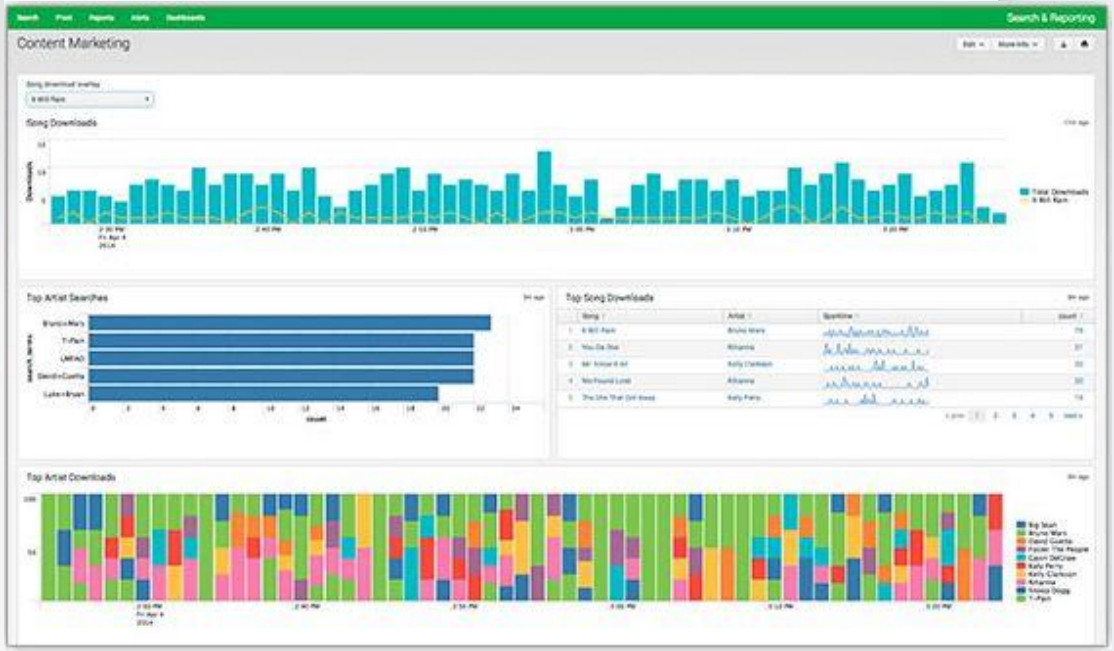
Licenciamento

- Standard Splunk Enterprise License -On Premise
- Standard Splunk Enterprise License – Cloud
- Enterprise Trial License e Sales Trial License
- Dev/Test License
- Free License

Relatórios

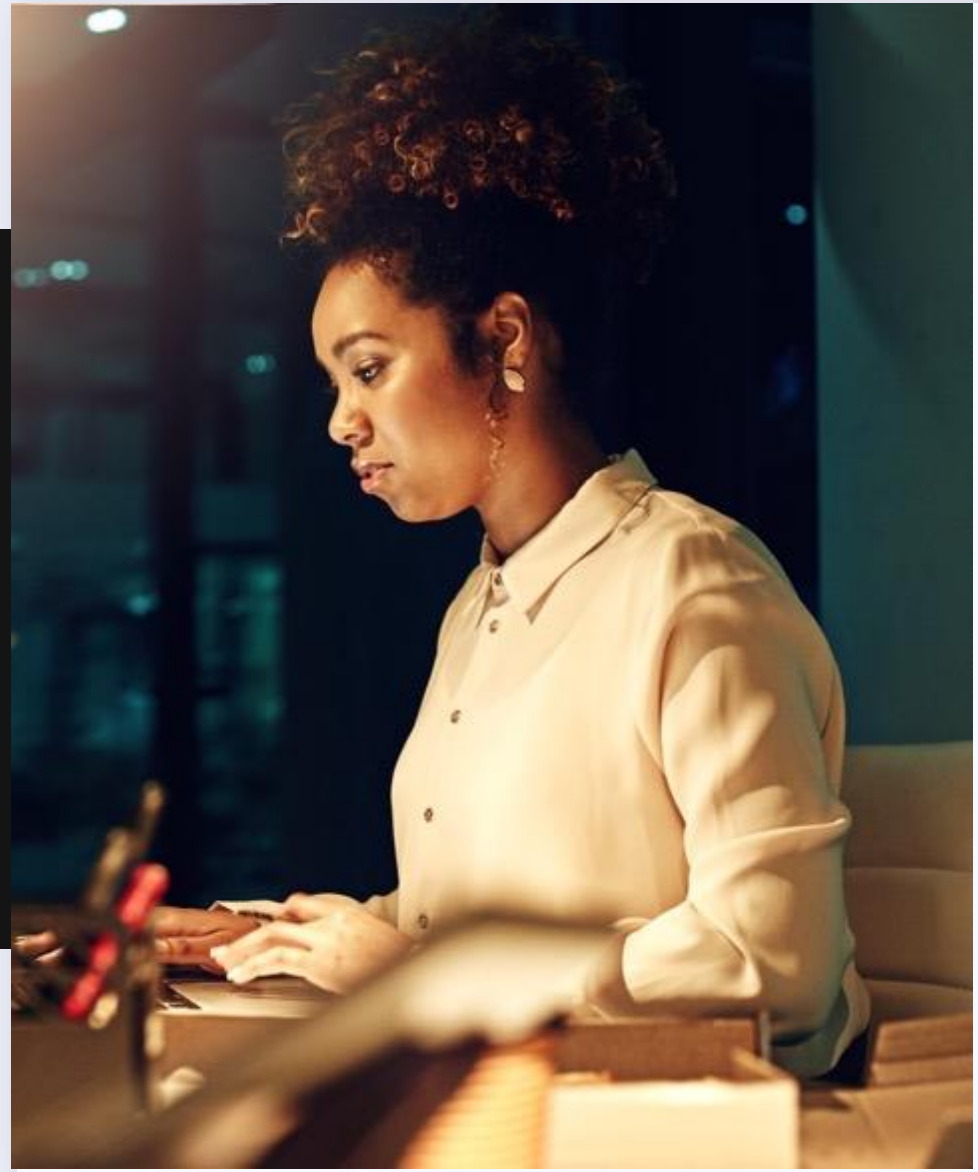
Splunk possibilita que o usuário crie os seus próprios relatórios baseados em vários tipos de gráficos





Escalabilidade

Splunk poderá iniciar os testes em laptops e depois migrar para máquinas maiores já que o produto tem escalabilidade horizontal ou linear, ou seja, pode operar bem com várias máquinas pequenas (hardware commodity) e não possui back-end o que torna o Splunk disponível em várias plataformas.



Conclusão

Splunk é uma ferramenta poderosa para monitorar diferentes desempenhos de infraestrutura, criar soluções, painéis, relatórios e alertas com facilidade além de gerenciar qualquer sistema com todos os logs armazenados dinamicamente..

Obrigado!

Perguntas?