

2025

# CSPM-Ready

Serviço de governança contínua

# Nós entregamos transformação digital...

Nossa equipe ajuda os clientes a identificar as capacidades e recursos certos para entregar transformação digital de ponta a ponta – onde quer que o cliente esteja em sua jornada.

A transformação digital catalisa o crescimento e otimiza os custos em três horizontes



## Abordagem

## Resultados focados

### Primeiro Horizonte: Migrar

Evoluir a TI existente, ampliando sua presença na nuvem e criando as bases para expansão de serviços e clientes em um modelo “Powered by”.



### Habilitar o negócio

Ganhe força  
Implante recursos e serviços em escala para fornecedores e clientes, com o apoio da Cloud Target, da Microsoft e de todo ecossistema.

10-20%  
Crescimento

### Segundo Horizonte: Modernizar

Mudar para um modelo operacional ágil e centrado no produto. Migrar e adotar sistemas nativos da nuvem.



### Reduzir Custo

Perder peso  
Otimizar despesas existentes, aproveitando a plataforma digital para acelerar os ganhos planejados.

10-30%  
Economia

### Terceiro Horizonte: Crescer & Inovar

Inovar, aprimorar e oferecer a capacidade de ampliar as parcerias para além do ecossistema atual de fornecedores, clientes e parceiros



### Reinventar o Negócio

Mudanças metabólicas  
Crie e lance novos negócios para gerar valor extra e crescimento da receita, aproveitando os serviços digitalmente nativos mais maduros

Novos  
negócios

# Dificuldades reais

## Falta de especialistas disponíveis

*“Temos bons profissionais, mas eles estão em suas tarefas. As análises ficam em segundo plano e acabamos atuando apenas de forma reativa, apagando incêndios...”*

*CIO – Indústria de Manufatura*

## Respostas lentas e insatisfatórias

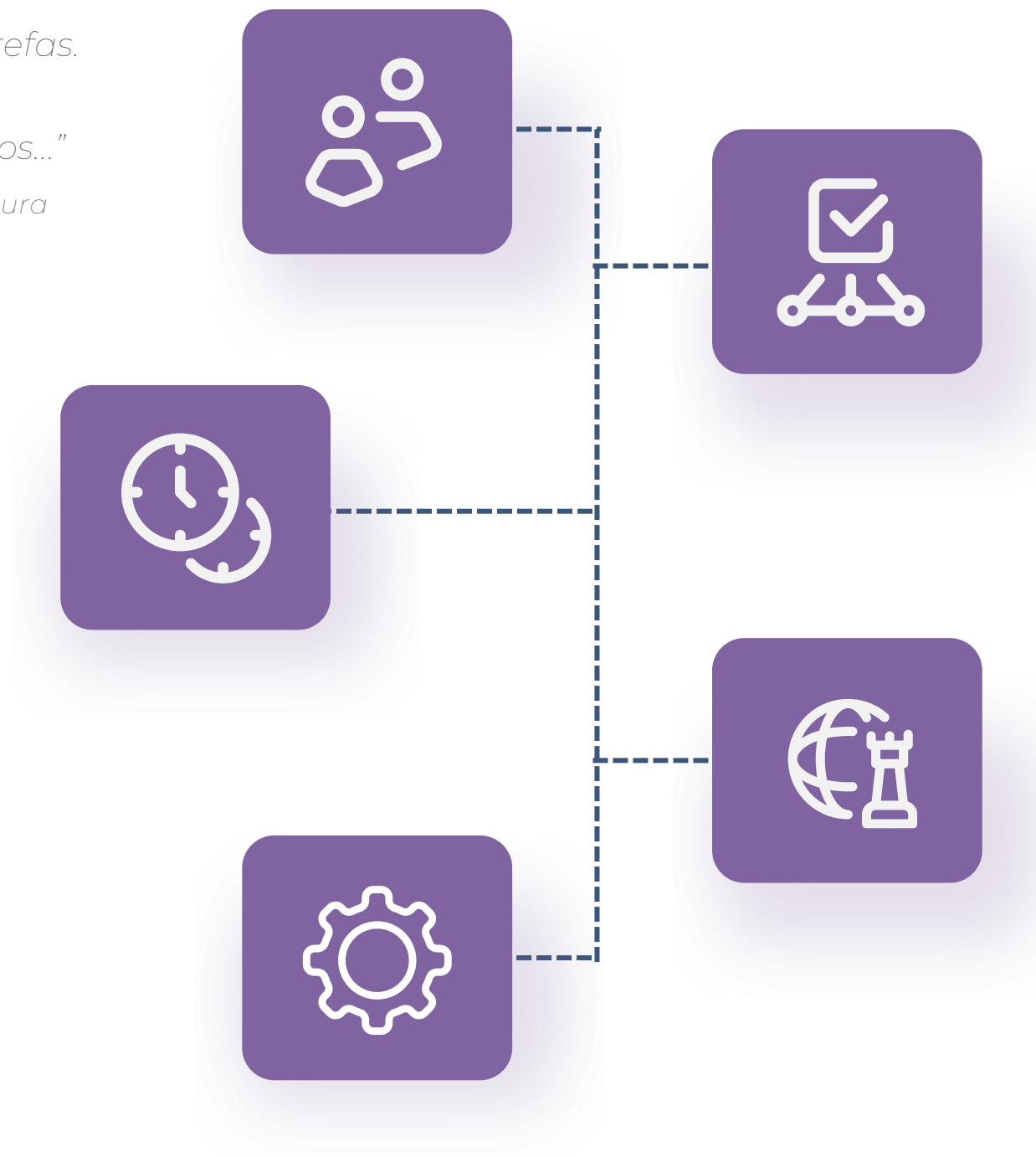
*“Em casos críticos, o retorno demora além do aceitável. Até conseguirmos uma solução, o impacto já gerou prejuízos e desgastes...”*

*Gerente de TI – Segmento de Saúde*

## Baixa automação

*“Grande parte das tarefas ainda é manual, ou centrada em pessoas, não em processos, aumentando consideravelmente o risco de falhas...”*

*Coordenador de Infraestrutura – Serviços Financeiros*



## Ambiente sem validações periódicas

*“Nosso ambiente roda, mas sem checagens regulares. Só descobrimos problemas quando algo para de funcionar, o que gera insegurança e falta de previsibilidade...”*

*CTO – Logística*

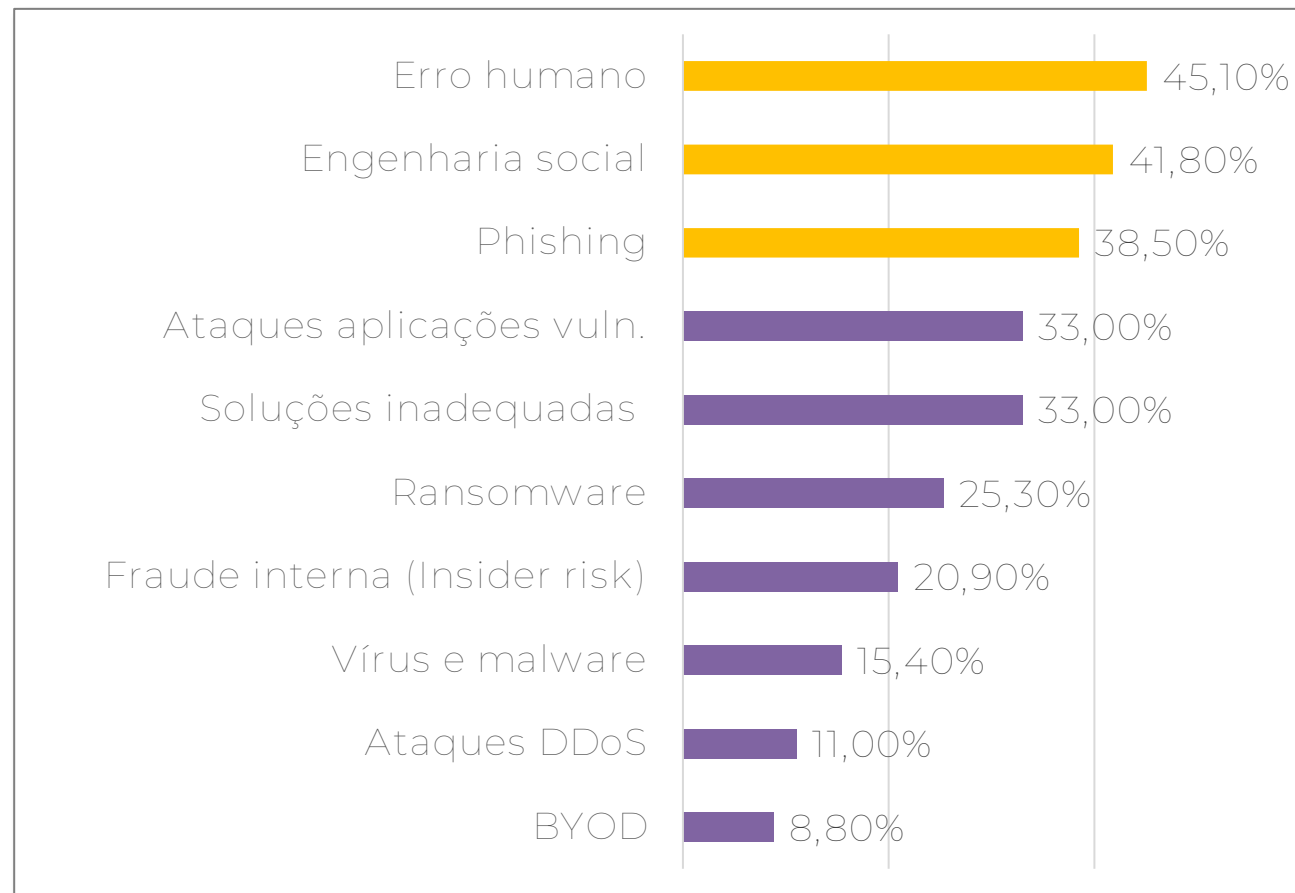
## Dificuldade para obter benchmark e insights de mercado

*“Não sabemos se estamos investindo certo ou se poderíamos reduzir custos. Falta referência para entender se nossa operação está no caminho certo...”*

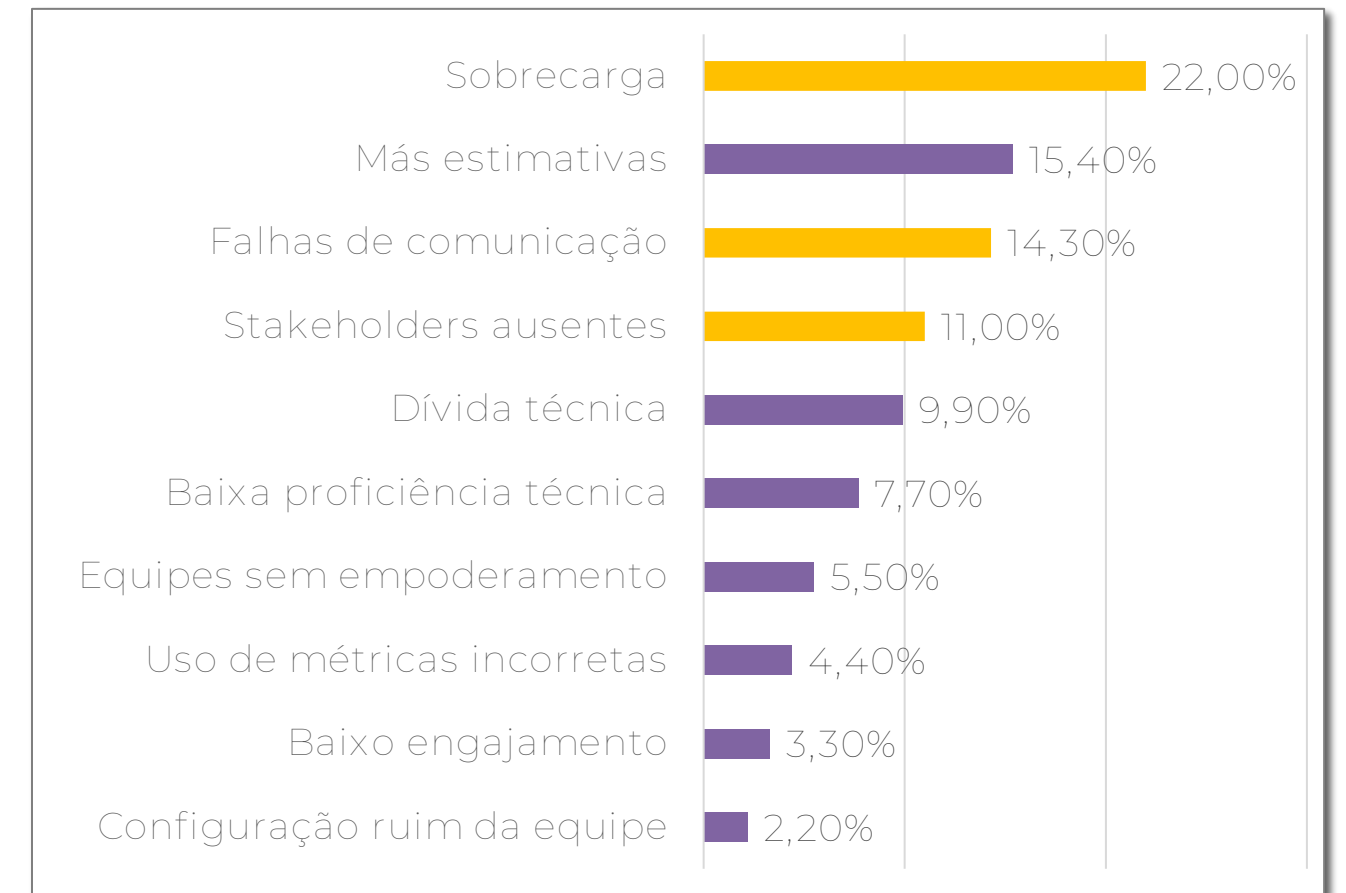
*Diretor de Operações – Educação*

# CTO's respondem...

...a sobrecarga é o principal fator de falhas durante entregas



...erro humano é apontado como principal risco cibernético



Equipes sobrecarregadas não apenas entregam menos, mas também expõem a empresa a riscos!

# SERVIÇOS GERENCIADOS

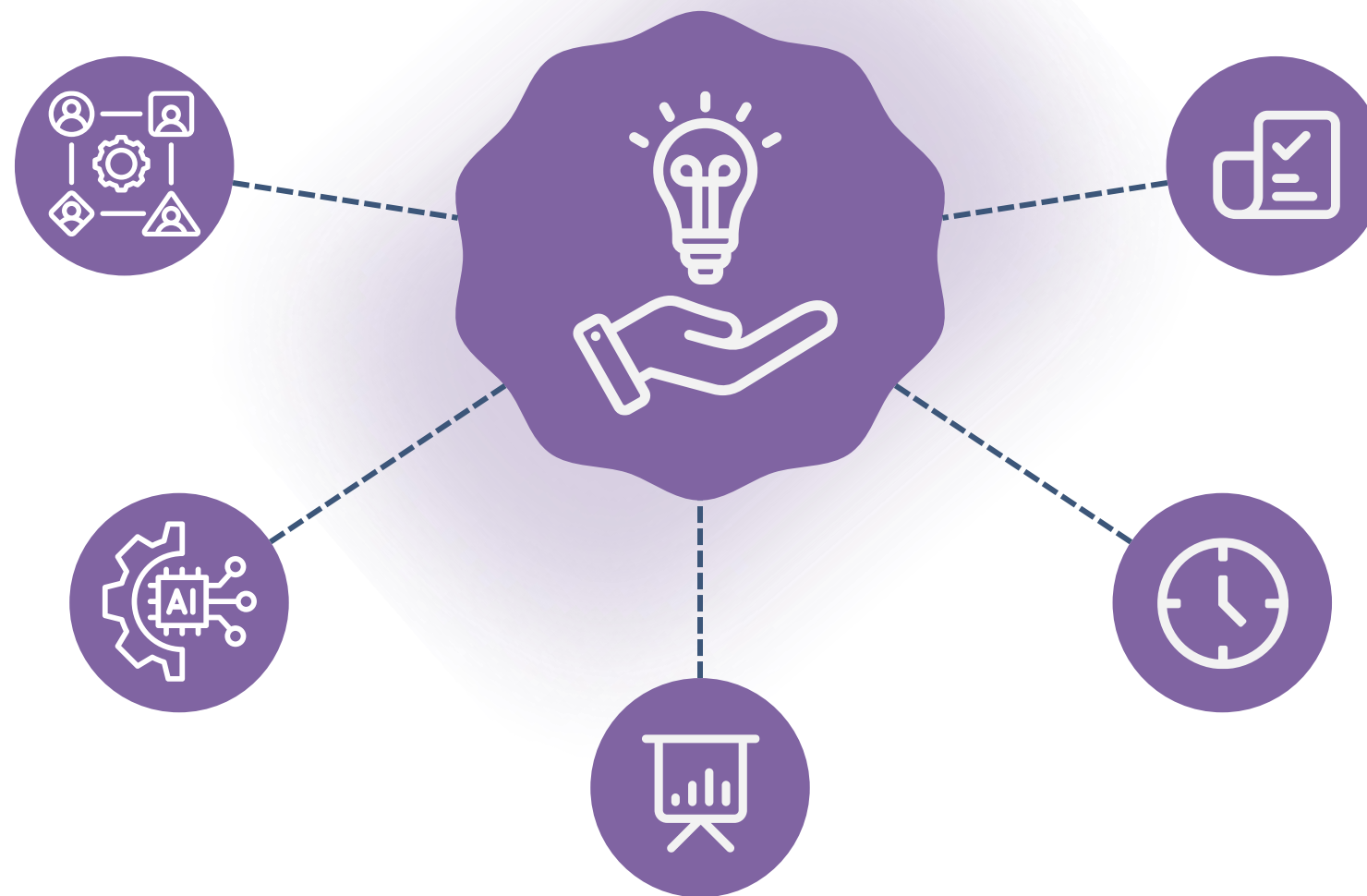
Soluções para garantir eficiência, segurança e continuidade.

## Equipe multidisciplinar

Cobertura completa em IaaS, PaaS e SaaS, seja infraestrutura, bancos de dados, segurança ou produtividade, especialistas sempre disponíveis para apoiar em cada camada do ambiente.

## Sistemas autônomos

Monitoramento 24x7 com uso de IA e alertas inteligentes. Soluções de ponta e desenvolvimento próprio para maior eficiência.



## Validações periódicas

Testes de backup & DR, campanhas de phishing e realização de protocolos de validação padronizadas e personalizados para garantir que tudo esteja operacional.

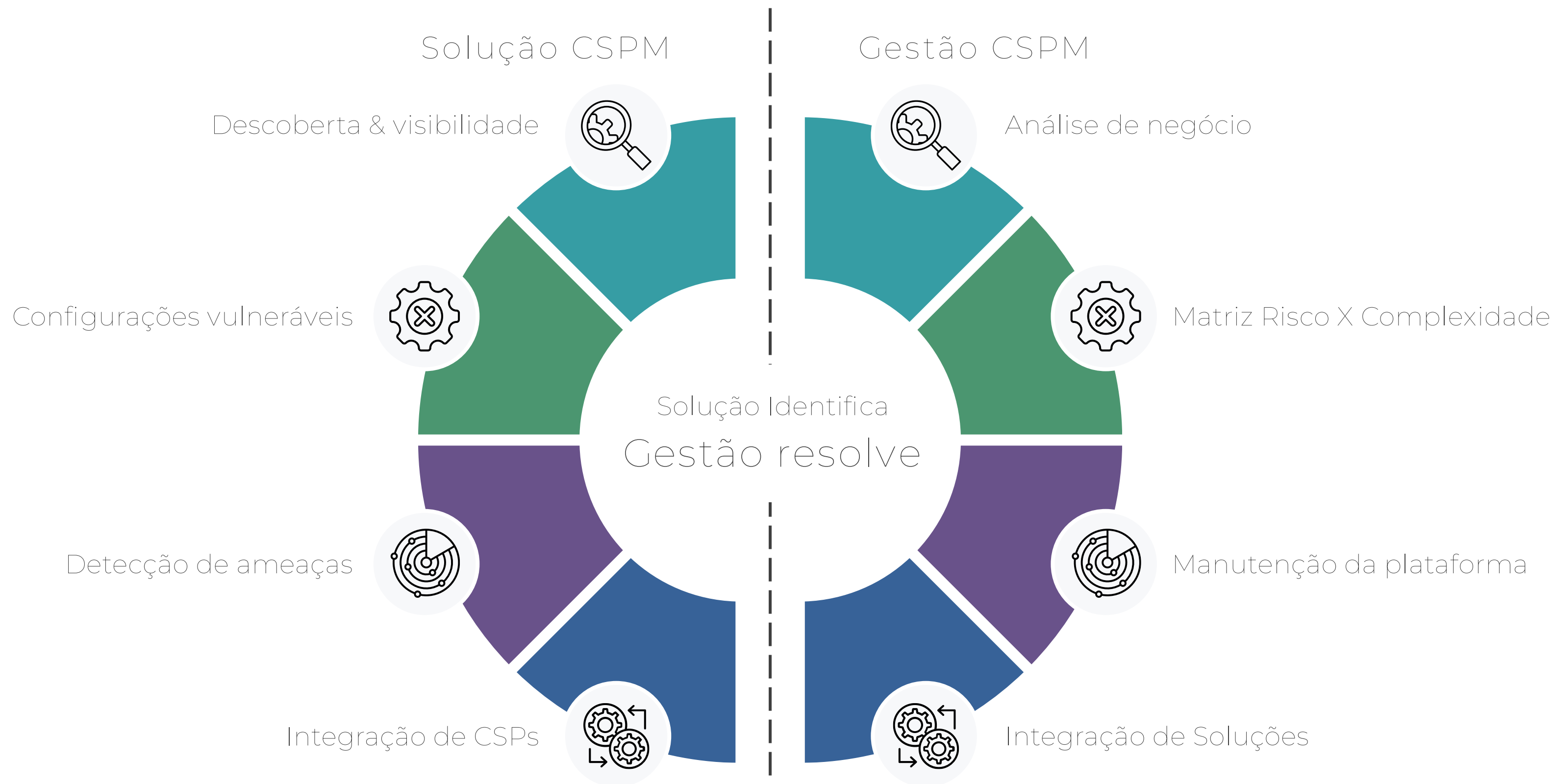
## Respostas rápidas

Suporte contínuo 24x7 com SLAs claros, assegurando respostas rápidas e eficazes a qualquer incidente

## Insights & relatórios executivos

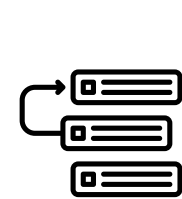
Relatórios técnicos e executivos com insights precisos e recomendações fundamentadas no mercado, oferecendo suporte direto à tomada de decisão

# Serviços Gerenciados CSPM-Ready



# Serviços Gerenciados

## CSPM-Ready – Fluxo de trabalho



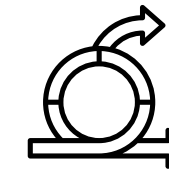
### Coleta & Análise

- Consolidação de alertas
- Classificação por risco X complexidade
- Análise técnica e de negócio



### Acompanhamento

- Monitoramento das ações aprovadas



### Comitê CSPM

- Apresentação de recomendações
- Discussão e esclarecimentos
- Decisão sobre execução ou exceção



### Refinamento da plataforma


- Registro de exceções e riscos aceitos
- Ajustes na ferramenta CSPM
- Preparação para próximo ciclo

*Transformando alertas em decisões estratégicas,  
acompanhadas por governança contínua*

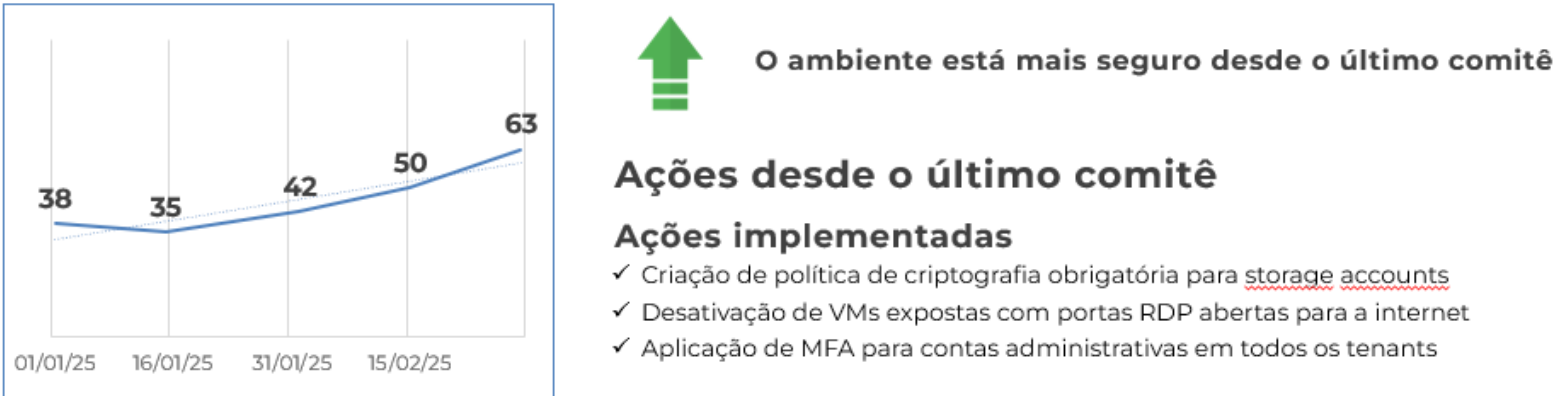
# Serviços Gerenciados

## CSPM-Ready – Dashboard modelo

### Comitê CSPM-Ready



#### Status do ambiente



#### Ações desde o último comitê

##### Ações implementadas

- ✓ Criação de política de criptografia obrigatória para [storage accounts](#)
- ✓ Desativação de VMs expostas com portas RDP abertas para a internet
- ✓ Aplicação de MFA para contas administrativas em todos os tenants

##### Ações justificadas

- ✓ Justificativa formalizada e registrada para exceção de logs em ambiente legado
- ✓ Registro de risco aceito para ambiente com dependência de sistema legado sem correção imediata

##### Ações em andamento

- Integração de alertas CSPM com o SIEM corporativo (Microsoft Sentinel)
- Revisão e correção de permissões excessivas em grupos de identidade

| Total de riscos         | 166 |
|-------------------------|-----|
| Riscos de nível crítico | 7   |
| Riscos de alto nível    | 17  |
| Riscos de médio nível   | 12  |
| Riscos de baixo nível   | 66  |


### Relatório executivo

Consolida métricas e insights para dar visão evolutiva do comitê

### Plano de ação

Extração & análise traduzida em ações prioritizadas e acompanhadas até sua resolução

### Comitê CSPM-Ready



#### Alerta (Solução CSPM)

**O acesso público da conta de armazenamento não deve ser permitido**

| Nível do risco                 | Alto                                     |
|--------------------------------|--|
| Data do alerta                 | 15/01/2025                               |
| Recurso(s) exposto(s)          | Bucket-temp1232                          |
| Fator de risco (Mitre)         | <a href="#">Exposure to the Internet</a> |
| Técnicas de exploração (Mitre) | <a href="#">Initial Access [T1190]</a>   |
| Caminhos de exploração         | 0  |

**Descrição**

O acesso de leitura público anônimo a contêineres e blobs no armazenamento do Azure é uma forma conveniente de compartilhar dados, mas pode apresentar riscos de segurança. Para evitar violações de dados causadas por acesso anônimo indesejado, a Microsoft recomenda a prevenção de acesso público a uma conta de armazenamento, a menos que o cenário o exija.

#### Ação (Análise técnica)

**O acesso público da conta de armazenamento não deve ser permitido**

| Complexidade de resolução       | Baixa      |
|---------------------------------|------------|
| Primeira apresentação ao comitê | 01/02/2025 |

**Plano de ação**

1. Identificar workloads que fazem que fazem uso deste Storage Account
2. Ajustar workloads para que realizem acesso autenticado / não anônimo
3. Bloquear o acesso anônimo ao Storage Account

**Análises já conduzidas**

Verificamos que o [bucket](#) não possui acesso acesso/tráfego nos últimos 30 dias (período máximo dos logs disponíveis). Como opção, ao plano de ação, o [bucket](#) possa ser removido.

**Ações alinhadas em comitê**

|             |                                   |
|-------------|-----------------------------------|
| Responsável | Kevin M.                          |
| Ação        | Seguir com plano de ação sugerido |
| Prazo       | 15 dias (próximo comitê)          |
| Status      | Em andamento                      |

# Empresa de logística



*“Com a padronização, o NOC deixou de ser apenas um ponto de reação e passou a atuar de maneira estratégica, apoiando na confiabilidade das operações e na tomada de decisões”*

*Diretor de TI*

## Desafio

- A gestão do NOC era realizada de forma fragmentada, utilizando diferentes ferramentas para monitorar cada camada da infraestrutura.
- Rede, VMware, Azure e servidores físicos eram acompanhados em soluções distintas.
- A ausência de visibilidade centralizada dificultava a priorização de incidentes e comprometia a eficiência operacional do time.

## Solução

- Implementamos um padrão único de monitoramento, capaz de abranger todos os ambientes de forma integrada.
- Alertas foram unificados, criando um fluxo mais claro e ágil para identificação e resposta.
- Foram definidas métricas personalizadas para acompanhar o desempenho de forma padronizada em toda a infraestrutura.

## Impacto

- Mais agilidade na detecção e resposta a incidentes, reduzindo riscos e tempo de indisponibilidade.
- Redução de custos ao eliminar redundâncias de ferramentas e otimização de processos internos do NOC.
- Maior precisão na geração de eventos, diminuindo os falsos-positivos e garantindo que a equipe atuasse apenas em ocorrências relevantes.

# Escritório de advocacia



“Com a migração para Azure e o suporte da Cloud contínuo da Cloud Target, conseguimos liberar nossa equipe para focar no que é estratégico para a cia, direcionando recursos em inovação.

CTO

## Desafio

- A infraestrutura estava totalmente on-premises, exigindo alto investimento em manutenção e sem a flexibilidade necessária para o crescimento do escritório.
- A equipe interna dedicava tempo excessivo à administração de servidores e sistemas, desviando esforços de atividades mais estratégicas.
- A falta de monitoramento centralizado e suporte especializado comprometia a disponibilidade e a segurança do ambiente de TI.

## Solução

- Realizamos a migração completa do ambiente por meio da estratégia de Lift & Shift, garantindo continuidade dos serviços e mínima interrupção.
- Implantamos o NOC da Cloud Target para monitoramento 24x7, padronizando alertas e garantindo maior confiabilidade operacional.
- Adotamos o modelo de Managed Services, com suporte contínuo e aplicação de insights que antecipam riscos e aumentam a performance do ambiente.

## Impacto

- O escritório passou a contar com um ambiente em nuvem mais moderno, escalável e preparado para evoluir conforme as necessidades do escritório.
- O NOC reduziu o tempo de resposta a incidentes e trouxe maior segurança, confiabilidade e tranquilidade à equipe de TI.
- Com o Managed Services, a equipe interna dedica seus recursos a iniciativas estratégicas, enquanto a Cloud Target cuida da manutenção e otimização do ambiente.

# Hospital



Elasticidade, segurança e eficiência: como o NOC da Cloud Target potencializa o ambiente Azure.

## Desafio

- O cliente precisava de uma infraestrutura moderna em nuvem, capaz de suportar aplicações críticas com alta disponibilidade e governança.
- Era necessário administrar o ambiente Azure de forma contínua, garantindo eficiência no consumo e segurança operacional.
- O projeto demandava a construção de uma base tecnológica robusta para suportar aplicações em Kubernetes, com foco em escalabilidade automatizada.

## Solução

- A Cloud Target implementou todo o ambiente no Azure, estruturando recursos e boas práticas para assegurar desempenho e confiabilidade.
- Adotamos o modelo de NOC e Managed Services, garantindo administração completa, monitoramento e suporte especializado 24x7.
- Construimos a arquitetura necessária para o Azure Kubernetes Services, habilitando escalabilidade automática e otimização de custos em tempo real.

## Impacto

- O hospital passou a contar com uma infraestrutura em nuvem moderna, flexível e preparada para sustentar novas demandas de negócio.
- A operação tornou-se mais eficiente com gestão proativa, redução de riscos e alta disponibilidade assegurada pelo NOC.
- O uso de AKS proporcionou escalabilidade automática para as aplicações, reduzindo custos de infraestrutura e aumentando a previsibilidade financeira.

# Empresa de entretenimento

*“Contar com a Cloud Target foi fundamental para transformar a TI da empresa em uma base confiável e eficiente”*

*Gestor de TI*

## Desafio

- O ambiente de TI baseado em Hyper-V, era mantido sem equipe especializada dedicada.
- Não havia monitoramento centralizado, o que dificultava a detecção precoce de incidentes e aumentava a dependência de ações corretivas.
- Sempre que surgiam necessidades envolvendo servidores ou infraestrutura crítica, dependia de apoio externo para garantir a continuidade das operações.

## Solução

- A Cloud Target assumiu a gestão completa do ambiente, estruturando processos e aplicando boas práticas para assegurar disponibilidade e desempenho.
- Implantamos rotinas de monitoramento contínuo e suporte remoto especializado.
- Nosso modelo de passou a atender integralmente o cliente, eliminando a dependência de recursos internos para tarefas críticas de TI.

## Impacto

- O ambiente ganhou estabilidade operacional, com redução de falhas e aumento da previsibilidade na gestão dos servidores.
- O monitoramento e a administração proativa garantiram mais agilidade na detecção e resolução de incidentes, mantendo os serviços disponíveis.
- A empresa passou a contar com uma operação de TI confiável, podendo dedicar-se totalmente ao seu core business enquanto a Cloud Target cuida da infraestrutura.



+55 11 3181-7011

contato@cloudtarget.com.br



# cloud.target