



## **Assessment de Segurança – Azure**

Cloud Team – Cloud Security

[@lanlink.com.br](https://lanlink.com.br)

# Visão Geral – Assessment



Diagnóstico rápido da postura de segurança no Azure

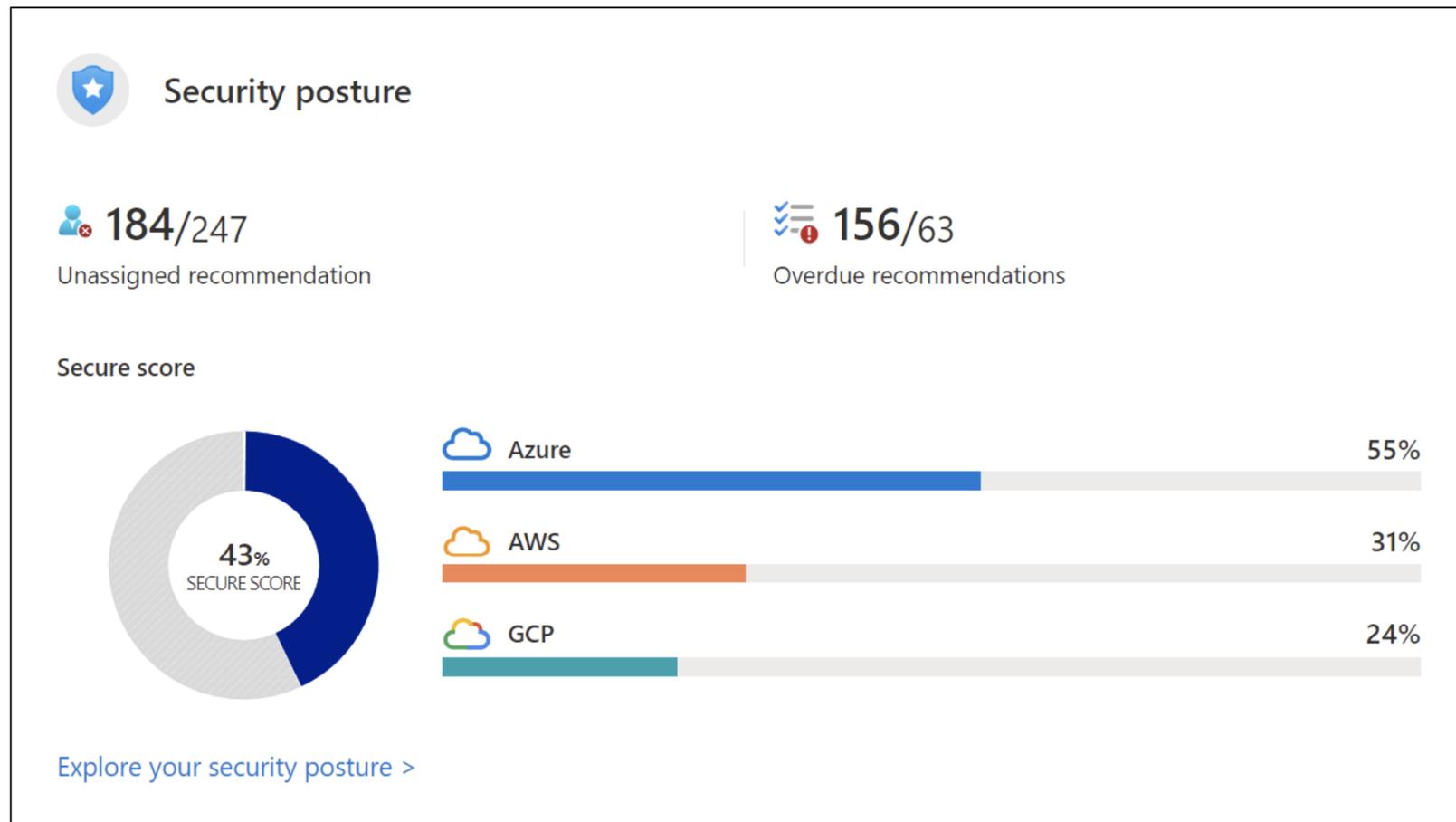
Identificamos riscos, falhas de configuração e oportunidades de melhorias

Alinhados as boas práticas Microsoft e CIS

Criamos um roadmap claro de mitigação.



# Objetivo & Proposta de Valor



“Exemplo ilustrativo

## Visibilidade 360° do ambiente

Geramos um raio-X de todo contexto de segurança do ambiente em até 10 dias, sem sobrecarregar a sua equipe interna.

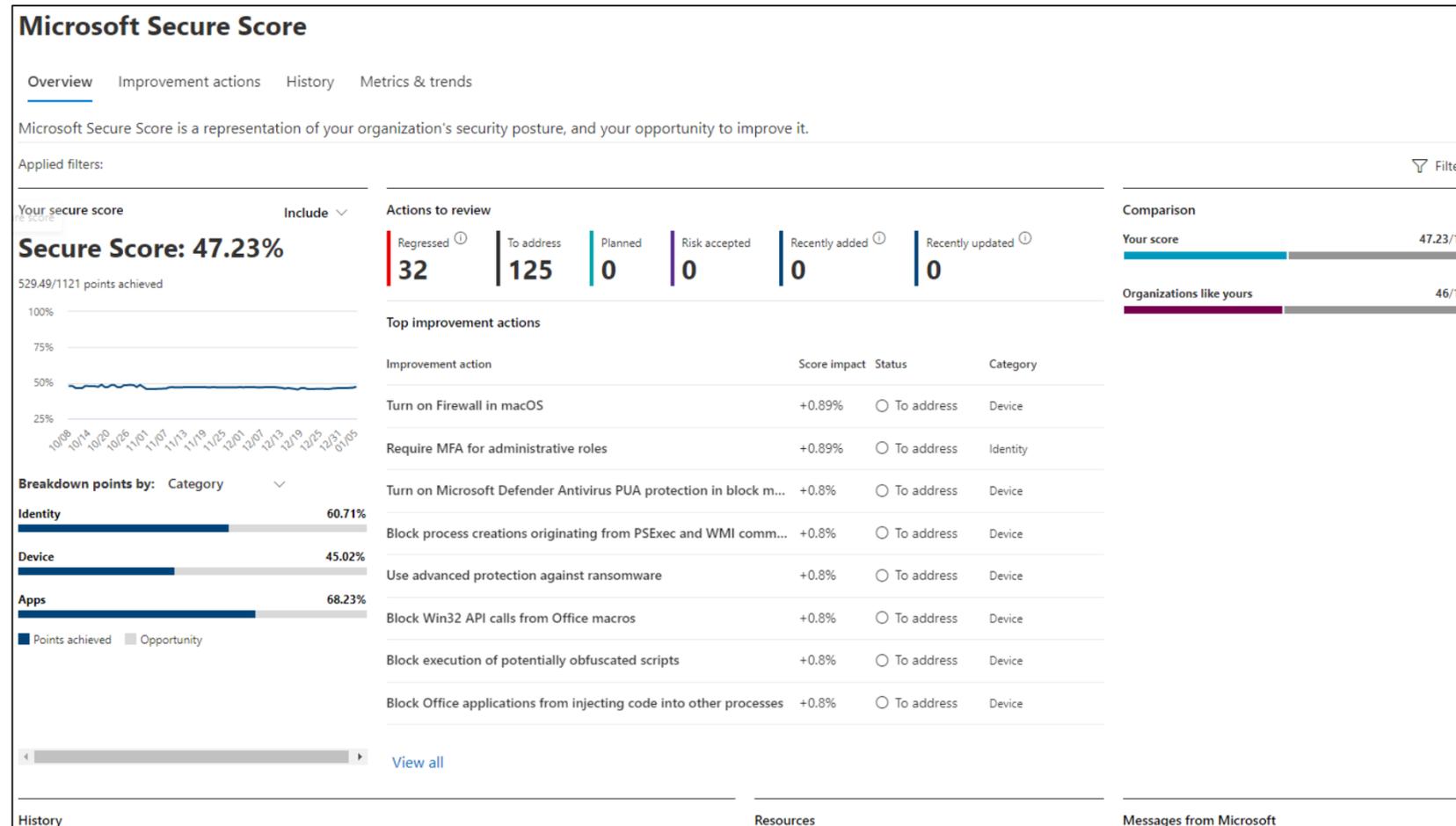
**Capacitação da equipe interna:** Entregamos ao time de TI um relatório com dados práticos para iniciar a remediação do ambiente imediatamente.

**Cultura de segurança :** O relatório de assessment pode ser o step inicial para uma campanha de segurança .

**Te ajudamos** a reduzir riscos críticos, e melhorar a postura de segurança no seu ambiente.



# Escopo do Assessment



“Exemplo ilustrativo

**Coletar recomendações** do Azure Advisor (segurança e confiabilidade)

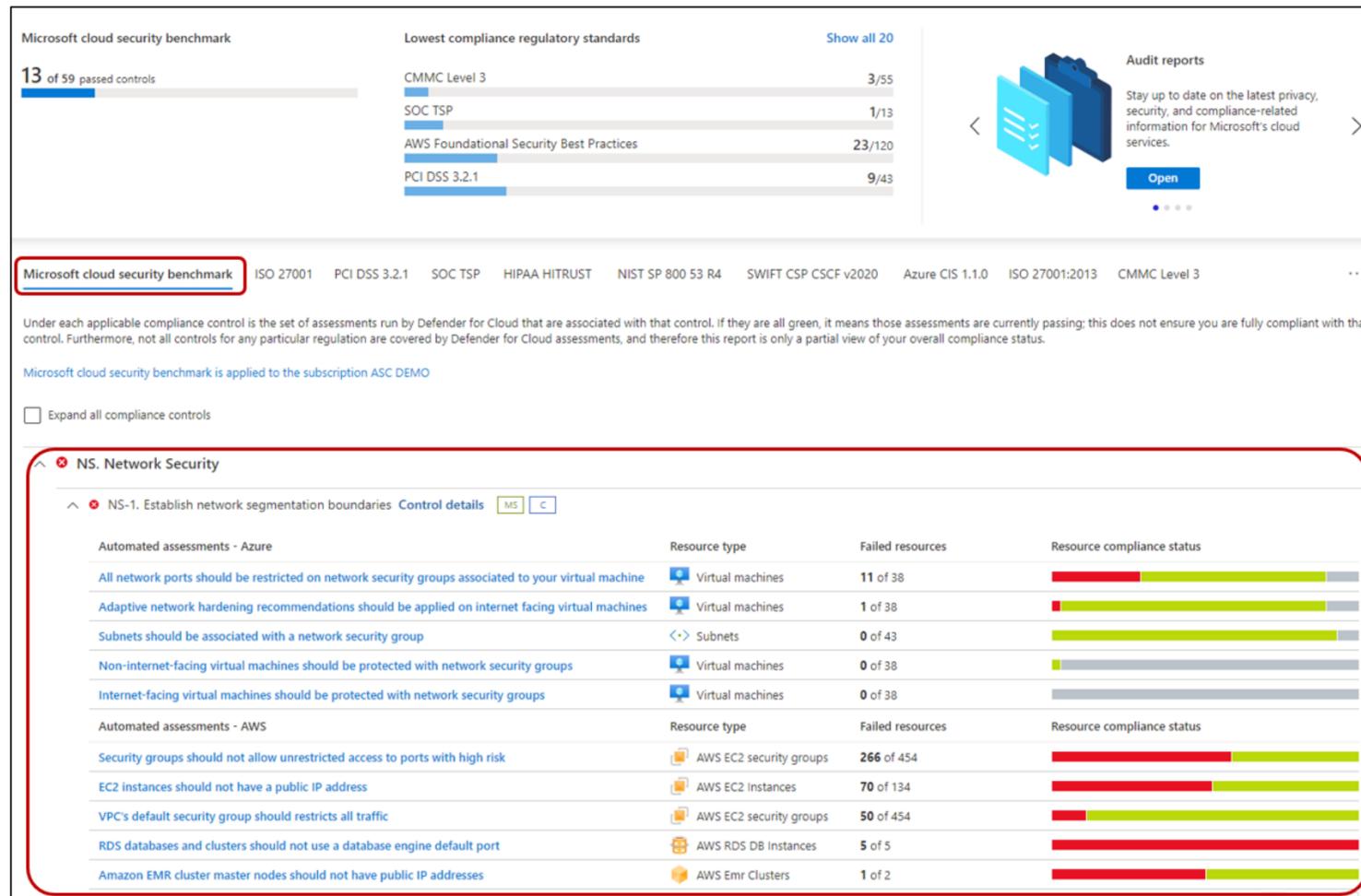
**Correlacionar alertas** e **Secure Score** do Microsoft Defender for Cloud

**Cobrir** VMs, redes, Storage, PaaS e identidades (Entra ID).

**Garantir avaliação** somente leitura, sem impacto na produção,



# Metodologia Aplicada ao Negócio



“Exemplo ilustrativo

**Coletar métricas** e exportações (Advisor, Defender e Secure Score)

**Classificar achados** por severidade, recurso e esforço de correção

**Correlacionar recomendações** eliminando redundâncias entre Advisor e Defender

**Mapear controles** aos benchmarks CIS, NIST CSF e matriz MITRE ATT&CK

**Priorizar riscos** com matriz impacto X prioridade de correção



# Entregáveis do Assessment

- **Resumo executivo** para C-level (1 página, infográficos claros)
- **Relatório técnico** detalhado, traz cada recomendação e passo de correção
- **Planos de ação** baseados na matriz Impacto x Prioridade
- **Debrief** de 1 hora para apresentação do relatório, quick wins e próximos passos

## Resumo Executivo

Durante a análise do ambiente Azure, foram identificadas oportunidades relevantes de melhoria nos pilares de segurança e confiabilidade. A seguir, apresentamos um panorama consolidado dos achados:

| Métrica                        | Segurança | Confiabilidade | Total Geral |
|--------------------------------|-----------|----------------|-------------|
| Nº de recomendações exportadas | 1 283     | 792            | 2 075       |
| Severidade Alta                | 337       | 423            | 760         |
| Severidade Média               | 760       | 298            | 1 058       |
| Severidade Baixa               | 186       | 71             | 257         |
| Top recurso impactado          | AKs (987) | VM (640)       | —           |

A maioria das recomendações de segurança possuem impacto **médio**, as recomendações de **alto** impacto também estão em número significativo (26%), indicando pontos críticos de atenção para mitigação imediata

As recomendações identificadas abrangem controles essenciais como a ausência de NSGs em sub-redes, recursos sem backup, identidades com permissões excessivas, e ausência de monitoramento ativo. O relatório propõe uma priorização das ações com base na criticidade e facilidade de remediação, oferecendo uma visão objetiva para decisões técnicas e de governança



**Obrigado!**

