overe

minitel NEXT CYBERSECURITY

MICROSOFT 365

GARANTIA DE SEGURANÇA CONTÍNUA

Ajude os seus clientes a manter ambientes Microsoft 365 seguros, alinhados e protegidos ao longo do tempo.

A SEGURANÇA MICROSOFT 365 NÃO É UMA CONFIGURAÇÃO ÚNICA.

Controlos, identidades, políticas e exceções mudam continuamente e devem ser monitorizados e revistos regularmente.

O DESAFIO

AS CONFIGURAÇÕES MUDAM AO LONGO DO TEMPO

Políticas, permissões e exceções evoluem continuamente, criando desvios face aos padrões definidos.

O RISCO DE IDENTIDADE ACUMULA-SE SILENCIOSAMENTE

Utilizadores, grupos, funções e acessos alteram-se diariamente sem revisão consistente.

AS REVISÕES MANUAIS NÃO ESCALAM

Verificações pontuais são difíceis de repetir e manter em ambientes Microsoft 365 dinâmicos.

A PLATAFORMA OVERE

4 PILARES PARA UMA POSTURA DE SEGURANÇA CONTÍNUA

AVALIAR

Machine learning e análise comportamental para todas as ameaças

REFORÇAR

Isolamento de dispositivos e malware para impedir propagação

MONITORIZAR

Visualização completa dos ataques com AI Advisor e recomendações

RESPONDER

Equipa MDR experiente a atuar rápida e eficazmente

REVISÃO DE GARANTIA MICROSOFT 365

UMA ABORDAGEM ESTRUTURADA E RECORRENTE PARA OS SEUS CLIENTES.

- Revisão do alinhamento dos controlos
- Resumo dos riscos de identidade
- Análise de desvios e exceções
- Definição e acompanhamento da remediação

CENÁRIOS IDEAIS

- Organizações fortemente dependentes do Microsoft 365.
- Clientes que necessitam de evidências contínuas de segurança.
- Clientes com necessidades recorrentes de remediação.
- MSPs e MSSPs que pretendem disponibilizar serviços geridos de segurança.

overe

minitel NEXT CYBERSECURITY

GARANTIA CONTÍNUA DE CONDITIONAL ACCESS

CONFIGURADO NÃO SIGNIFICA APLICADO.

Ter políticas de Conditional Access configuradas não garante que estão realmente a ser aplicadas. Utilizadores, dispositivos, grupos, aplicações e exceções criam caminhos de acesso não intencionais que passam despercebidos.

O QUE É CONDITIONAL ACCESS ASSURANCE?

Valida o enforcement
Confirma que as políticas de Conditional Access estão efetivamente a ser aplicadas.

Identifica caminhos de acesso ocultos
Descobre desvios, exceções e combinações que permitem acessos não intencionais.

Orienta a remediação
Fornece recomendações claras e priorizadas para corrigir riscos e reforçar a postura de segurança.

PORQUE É DIFICIL GARANTIR ENFORCEMENT?

O Conditional Access é complexo por natureza.

- Múltiplas políticas
- Grupos e utilizadores dinâmicos
- Dispositivos geridos e não geridos
- Aplicações e serviços diversos
- Exceções e overrides

Quem sabe qual política se aplica realmente?
Sem validação contínua, os riscos permanecem ocultos.

ONDE SURGEM OS CAMINHOS DE ACESSO OCULTOS

EXCLUSÕES ADMINISTRATIVAS	UTILIZADORES GUEST	DISPOSITIVOS NÃO GERIDOS	SOBREPOSIÇÃO DE POLÍTICAS	POLICY DRIFT	AUTENTICAÇÃO LEGADA
Contas privilegiadas podem contornar as políticas definidas.	Os acessos de convidados nem sempre seguem as mesmas regras.	Dispositivos fora da gestão podem permitir acessos inesperados.	Múltiplas políticas podem entrar em conflito e criar comportamentos inesperados.	As alterações ao longo do tempo criam desvios que deixam de ser revistos.	Métodos antigos podem ignorar os controlos modernos.

COMO A OVERE RESOLVE

1. **VALIDAR**
Testa continuamente se as políticas estão realmente a ser aplicadas.

2. **IDENTIFICAR**
Descobre desvios, exceções e caminhos de acesso ocultos.

3. **MONITORIZAR**
Acompanha alterações e garante visibilidade contínua.

4. **COMPROVAR**
Fornece evidências e acompanha a remediação até à resolução.

overe

minitel NEXT CYBERSECURITY

Sales Playbook

MICROSOFT 365 ASSURANCE

COMO RESPONDER ÀS OBJEÇÕES MAIS COMUNS

Utilize este guia para conduzir conversas mais eficazes, responder com confiança e demonstrar o valor da Overe.

1

"JÁ TEMOS A SEGURANÇA DO MICROSOFT 365

COMO RESPONDER

A Overe complementa a segurança existente do Microsoft 365, garantindo que os controlos permanecem corretamente configurados ao longo do tempo. Monitoriza alterações em utilizadores, grupos, políticas e exceções, identifica desvios face às boas práticas e fornece evidências contínuas da postura de segurança.

PERGUNTA PARA FAZER AO CLIENTE

- Quem valida regularmente que essas configurações continuam corretas?
- Com que frequência fazem essa revisão?
- Existe um relatório que demonstre essa conformidade?

A segurança não é estática. A garantia contínua reduz riscos e evita surpresas.

2

"O QUE É QUE VOCÊS VÃO AVALIAR EXATAMENTE?

COMO RESPONDER

A Overe avalia continuamente a postura de segurança do Microsoft 365, analisando controlos, identidades, configurações, desvios e exceções. O objetivo é identificar riscos reais, priorizar melhorias e fornecer uma visão clara do estado de segurança do ambiente.

PERGUNTA PARA FAZER AO CLIENTE

- Existem requisitos internos ou regulamentares que tenham de cumprir?
- Há algum standard que utilizem como referência?

Visibilidade completa. Prioridades claras. Ações com impacto.

3

"PORQUE É QUE PRECISAMOS DE MONITORIZAÇÃO CONTÍNUA?

COMO RESPONDER

A Overe complementa a segurança existente do Microsoft 365, garantindo que os controlos permanecem corretamente configurados ao longo do tempo. Monitoriza alterações em utilizadores, grupos, políticas e exceções, identifica desvios face às boas práticas e fornece evidências contínuas da postura de segurança.

PERGUNTA PARA FAZER AO CLIENTE

- Com que frequência ocorrem mudanças no vosso ambiente?
- Quem é responsável por acompanhar essas alterações?

O ambiente evolui todos os dias. A segurança deve evoluir com ele.

4

"ISSO VAI DAR MUITO TRABALHO?

COMO RESPONDER

A Overe avalia continuamente a postura de segurança do Microsoft 365, analisando controlos, identidades, configurações, desvios e exceções. O objetivo é identificar riscos reais, priorizar melhorias e fornecer uma visão clara do estado de segurança do ambiente.

PERGUNTA PARA FAZER AO CLIENTE

- Quem teria de estar envolvido?
- Existe um processo interno de aprovação?

Menos esforço para a equipa. Mais segurança para a organização.

4 “DEPOIS DA ANÁLISE, O QUE ACONTECE?

COMO RESPONDER

A Overe complementa a segurança existente do Microsoft 365, garantindo que os controlos permanecem corretamente configurados ao longo do tempo. Monitoriza alterações em utilizadores, grupos, políticas e exceções, identifica desvios face às boas práticas e fornece evidências contínuas da postura de segurança.

PERGUNTA PARA FAZER AO CLIENTE

- Como preferem receber os relatórios?
- Existem áreas críticas que pretendem acompanhar?

Da visibilidade à ação.

5 “JÁ TEMOS CONDITIONAL ACCESS.

COMO RESPONDER

A Overe avalia continuamente a postura de segurança do Microsoft 365, analisando controlos, identidades, configurações, desvios e exceções. O objetivo é identificar riscos reais, priorizar melhorias e fornecer uma visão clara do estado de segurança do ambiente.

PERGUNTA PARA FAZER AO CLIENTE

- Existem exceções configuradas atualmente?
- Com que frequência revêem essas políticas?

Ter Conditional Access não basta. É preciso garantir que continua alinhado.

O VALOR PARA O PARCEIRO

Serviço recorrente
Transforme auditorias pontuais num serviço contínuo.

Evidências contínuas
Forneça provas objetivas da postura de segurança dos clientes.

Monitorização permanente
Identifique alterações antes que se transformem em problemas.

Remediação estruturada
Acompanhe todas as ações até à sua conclusão.

Receita recorrente
Crie novos serviços geridos de segurança com faturação periódica.

O QUE EVITAR DIZER

- ✕ O Microsoft 365 não é seguro.
- ✕ A Microsoft não faz segurança.
- ✕ A vossa configuração está errada.
- ✕ Precisam de mudar tudo.

A segurança do Microsoft 365 precisa de ser validada continuamente, porque o ambiente está sempre a evoluir.