Tendências de cibersegurança para empresas em **2026**

O que muda na prática para médias e grandes empresas:

Segurança deixou de ser custo técnico. Em 2026, ela define:

- **eficiência**
- **confiança**
- **crescimento**

SUMÁRIO

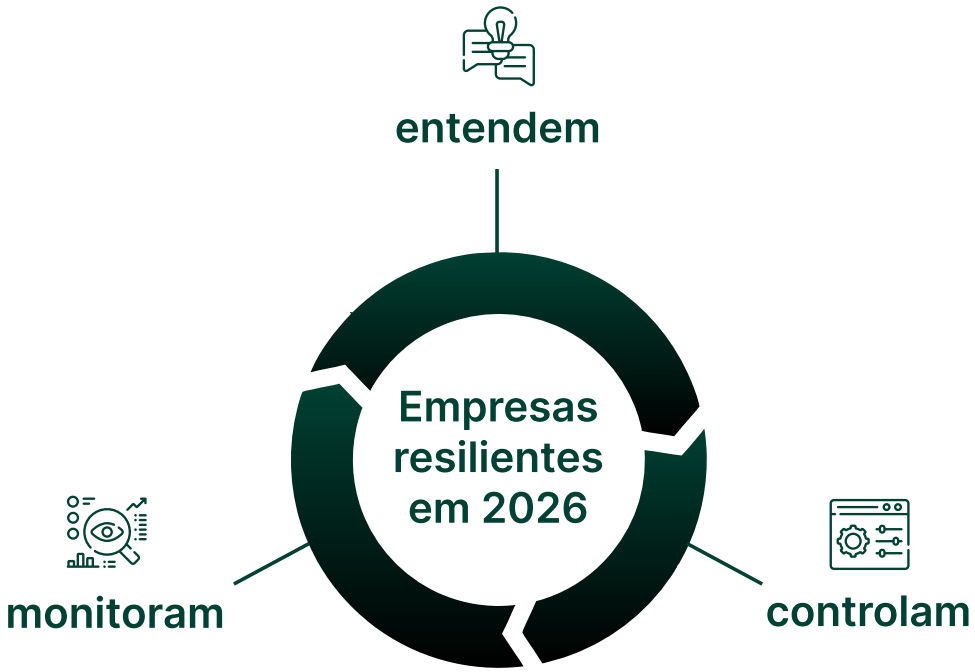
Por que 2026 é um ponto de virada para a cibersegurança?

A cibersegurança deixou de viver “nos bastidores” da TI.

Ela passou a influenciar diretamente a continuidade **operacional, reputação, compliance e decisões estratégicas.**

Ambientes híbridos, múltiplos fornecedores, trabalho distribuído, cloud e automação criaram um novo cenário: não existe mais um “lado de dentro” claramente protegido.

Em 2026, empresas resilientes não são as que tentam bloquear tudo, são as que **entendem, controlam e monitoram continuamente o que acontece na sua infraestrutura.**

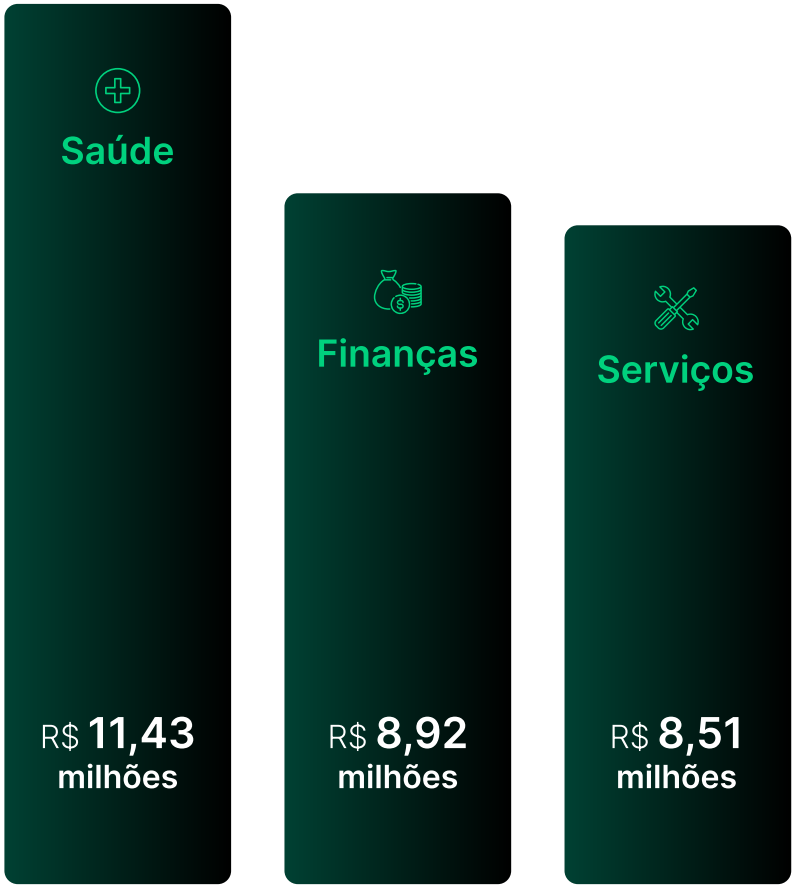


O cenário de ameaças que define 2026

O conceito tradicional de perímetro morreu. Hoje, **identidades, dispositivos, aplicações e integrações** são os novos pontos críticos.

Impacto financeiro no Brasil

(médias por violação)



Fonte: IBM - Cost of Data Breach

Segurança moderna não reduz só risco. Ela *acelera decisões, melhora negociações e aumenta a confiança do mercado.*

As 5 tendências que vão moldar a segurança corporativa

1 Extorsão digital sem criptografia

Quando o ataque não "quebra sistemas", ele rouba confiança.

O ransomware evoluiu. Em vez de criptografar tudo e parar a operação, atacantes agora **extraem dados aos poucos**, ficam invisíveis por mais tempo e só aparecem no final: com a *ameaça de exposição pública, chantagem a executivos e pressão reputacional.*

E tem uma camada nova deixando tudo mais difícil de identificar: **engenharia social com deepfakes de voz e imagem**. Em 2026, golpistas conseguem ligar como se fossem o CEO, um diretor ou até o time de TI, criando urgência para pedir credenciais, aprovações, acessos temporários ou “ajustes rápidos” que abrem a porta para o vazamento. ***O ataque não precisa invadir primeiro. Ele convence alguém a entregar.***

Por isso, **backup continua essencial, mas não é suficiente**. O novo jogo exige proteger o que acontece **antes** da exfiltração e reduzir a margem para decisões impulsivas baseadas em “parece legítimo”.

O que isso exige na prática:

Visibilidade sobre dados sensíveis

Onde estão? Quem acessa? Quando? Como?

Controle de acesso preciso

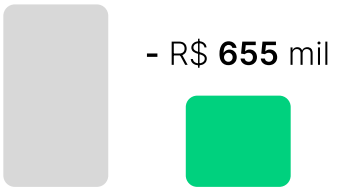
Menos privilégios, aprovações rastreáveis e regras claras

Detecção de comportamento anômalo

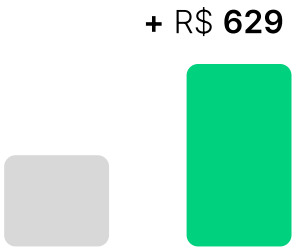
Sinais de movimentação, coleta e envio fora do padrão

As 5 tendências que vão moldar a segurança corporativa

Quanto mais tempo o atacante precisa ficar invisível, maior será a chance de você detectá-lo.



Uso de inteligência de ameaças reduz custos em ~R$ 655 mil (média por incidente)



Governança de IA economiza, em média, R$ 629 mil. Quanto mais tempo o atacante precisa ficar invisível, mais chance você tem de detectá-lo.

Fonte: IBM - Cost of Data Breach 2025

2 Gestão de identidades é o novo perímetro

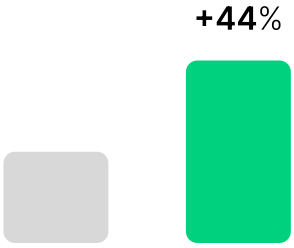
Não é mais sobre rede. É sobre quem (ou o quê) acessa.

Credenciais são hoje o principal vetor de ataque. O relatório **Verizon 2025** confirma: **senhas roubadas lideram as invasões corporativas.**

Mas existe um desafio maior: **identidades não-humanas** (*APIs, bots, serviços, IoT*).

Em algumas empresas:

Identidades de máquina para cada pessoa



Crescimento anual médio: 44%

As 5 tendências que vão moldar a segurança corporativa

Empresas maduras tratam todas as identidades com o mesmo rigor:

- **MFA inteligente**
- **Privilégios mínimos**
- **Análise comportamental**
- **Ciclo de vida automatizado**

Zero Trust entra aqui como evolução prática e não ruptura.

3 Observabilidade avançada: de reativo para preditivo

Parar de apagar incêndio. Começar a ler sinais.

Monitorar alertas não basta. Observabilidade significa **entender o contexto completo** do ambiente.

Com machine learning:

- **O sistema aprende o "normal";**
- **Detecta desvios sutis;**
- **Reduz falsos positivos;**
- **Prioriza o que realmente importa.**

Tempo médio global para identificar e conter uma violação

Detecção precoce virou vantagem competitiva.

As 5 tendências que vão moldar a segurança corporativa

4 Controle de acesso à rede

Wi-Fi, visitantes, terceiros e IoT viraram porta de entrada real.

Antes de pensar em SIEM, EDR ou SOC, tem uma pergunta básica: **quem está entrando na sua rede e com quais regras?**

Em 2026, a tendência é clara: empresas estão saindo do "Wi-Fi com senha" e indo para **autenticação, segmentação e rastreabilidade.**

O que essa camada limita na prática:

- **Acesso indevido por senha compartilhada**
- **Visitante ou terceiro caindo na rede errada**
- **Movimento lateral dentro da infraestrutura**
- **Conexões sem identidade (impossíveis de auditar)**

Por que funciona tão bem:

- ✓ **Organiza acesso por perfil: colaborador, visitante, terceiro, IoT**
- ✓ **Dá visibilidade e logs para investigação e compliance**
- ✓ **Reduz fricção para quem é legítimo: aumenta barreira para o suspeito**
- ✓ **Escala em operações multiunidade, sem virar "controle manual"**

Em 2026, **controle de acesso deixou de ser detalhe de rede.**

Virou fundamento para segurança, governança e continuidade operacional.

As 5 tendências que vão moldar a segurança corporativa

5 IA na segurança: velocidade com critério

Máquina rápida. Humano estratégico.

IA não substitui especialistas. Ela **amplifica capacidade.**

Na prática:

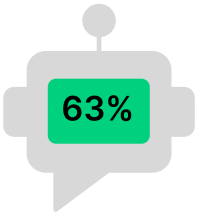
- **Automatiza respostas de baixo risco**
- **Detecta padrões invisíveis**
- **Analisa volumes impossíveis manualmente**
- **Entrega contexto rico para decisão humana**

Empresas sem IA têm prejuízo de
R$ **8,78** mi

Empresas com IA e automação têm prejuízo menor de
R$ **6,48** mi

Diminuição do custo por violação
-26%

O ponto crítico está na governança:



das empresas ainda não têm políticas claras de uso de IA. → Quem estrutura governança primeiro, **inova com menos risco.**

Como evoluir em 2026

1 Pequenas empresas

Para pequenas empresas, evoluir em 2026 significa **parar de buscar complexidade e focar no básico bem feito**. Priorize autenticação forte para contas críticas, especialmente administrativas, e implemente backups automatizados com testes regulares de restauração, porque backup que nunca foi testado não é plano de contingência, é aposta.

Além disso, crie uma rotina consistente de atualização de sistemas e trate o acesso à rede como parte da estratégia de segurança. **Substituir senha compartilhada por autenticação por perfil, com regras claras para visitantes e terceiros, reduz improvisos, melhora rastreabilidade e evita que o Wi-Fi se torne a porta de entrada para incidentes.**

2 Médias empresas

Em médias empresas, o crescimento desorganizado costuma gerar brechas invisíveis. Novas unidades, mais dispositivos e terceiros ampliam a complexidade, e a segurança vira um quebra-cabeça. Em 2026, **a prioridade deve ser estruturar a gestão de identidades humanas e não humanas, porque credenciais frágeis ainda são uma das principais portas de entrada.**

Também é **fundamental organizar o acesso à rede por perfil, com segmentação clara entre colaboradores, visitantes, terceiros e IoT.** Integrar logs e eventos em uma visão mais centralizada, mesmo que inicial, traz clareza para investigar mais rápido, responder melhor e reduzir o ruído operacional.

Como evoluir em 2026

3 Grandes empresas

Grandes organizações já entendem que segurança é operação contínua, não projeto com data final. **O desafio não é ter ferramentas, mas garantir consistência em ambientes complexos e distribuídos.** Avançar em Zero Trust de forma progressiva: testando, ajustando e escalando, tende a gerar mais maturidade do que grandes mudanças abruptas.

Observabilidade integrada, redução de falsos positivos e gestão rigorosa de risco de terceiros se tornam diferenciais estratégicos. **Governar o acesso à rede com autenticação por perfil, segmentação e rastreabilidade clara reduz zonas cinzentas, aumenta previsibilidade e fortalece a capacidade de resposta a incidentes.**

Comparativo de estratégias de segurança (2026)

	Pequenas empresas	Médias empresas	Grandes empresas
Foco principal	O básico bem feito: simplicidade e execução rigorosa.	Organização do crescimento: eliminar brechas de expansão.	Operação contínua: consistência em ambientes complexos.
Identidade e acesso	Autenticação forte para contas críticas (admin).	Gestão de identidades humanas e não humanas.	Governança rigorosa e autenticação por perfil.
Estratégia de rede	Substituir senhas compartilhadas por perfis de acesso.	Segmentação clara (Colaboradores, IoT, Visitantes)	Segmentação avançada e rastreabilidade total.
Resiliência	Backups automatizados com testes reais de restauração.	Visão centralizada de logs para resposta rápida.	Observabilidade integrada e redução de falsos positivos.
Relação com terceiros	Regras claras para visitantes e prestadores de serviço.	Gestão de acessos para terceiros integrada à rede.	Gestão rigorosa de risco de terceiros (estratégico).
Modelo de evolução	Rotina consistente de atualização de sistemas.	Redução de ruído operacional e investigação ágil.	Implementação progressiva de zero trust.

Segurança como habilitador de negócio

Clientes escolhem empresas confiáveis. Parceiros exigem maturidade. Investidores avaliam risco operacional.

As tendências de 2026 mostram um ponto claro: **segurança não trava crescimento. Ela sustenta.**

Empresas que tratam cibersegurança como estratégia:

Operam com mais previsibilidade

Constroem confiança de longo prazo

Escalam com menos atrito operacional

Onde o WiFeed entra nessa conversa

O WiFeed ajuda empresas a **controlar, organizar e dar visibilidade** a um dos pontos mais explorados (e menos protegidos) dos ambientes corporativos: **o acesso à rede Wi-Fi.**

Com foco em:

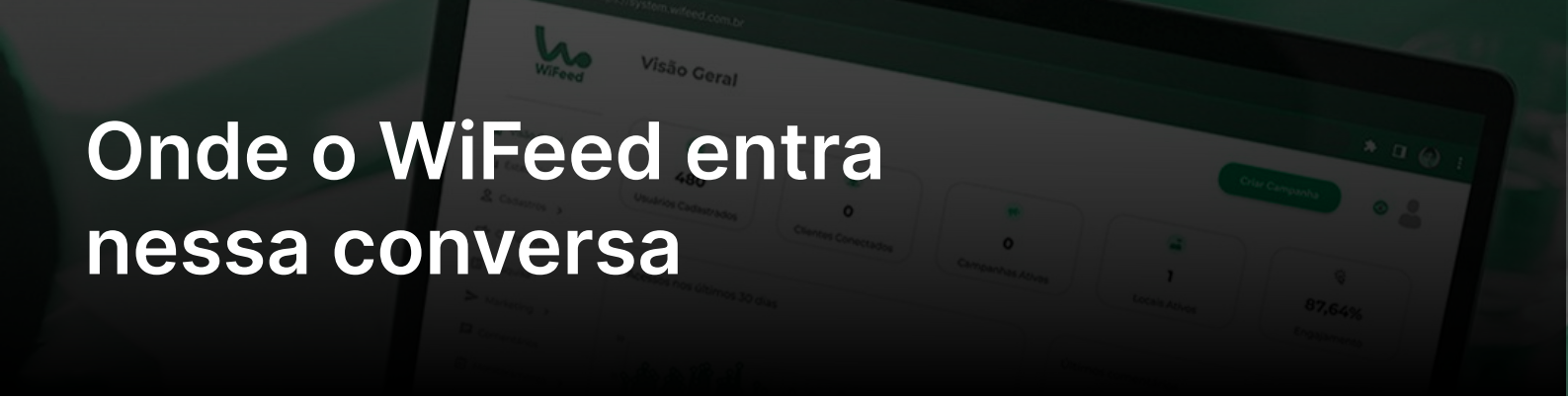
- **+15 métodos de autenticação e controle de acesso;**
- **Segmentação por perfil de usuário;**
- **Logs, rastreabilidade e compliance;**
- **Integração com +20 fabricantes de access points.**

Mais de 15 métodos de autenticação e controle de acesso;

Active Directory · LDAP e SAML · Google Workspace · gov.br · Voucher · OpenRoaming · Login e senha · mercado pago

Integração nativa com +20 fabricantes de access points

FORTINET · HUAWEI · UBIQUITI · cisco · aruba · tp-link · MikroTik · Cambium Networks · AEROHIVE



Onde o WiFeed entra nessa conversa

Ronaldo A da Rosa
Analista de Suporte Computacional
Pormade Portas

Nós gostamos bastante da ferramenta. **A autenticação ficou mais fácil e segura, e o controle de acessos melhorou significativamente.**

Para os visitantes, conseguimos personalizar vouchers e deixar tudo mais organizado e acolhedor.

Leandro Gomes de Souza
Analista de Segurança da Informação
Lojas REDE

O projeto Pix acelerou a necessidade de conectividade e as lojas novas passaram a operar com o padrão WiFeed.

O WiFeed trouxe o **nível de controle e gestão de tráfego necessário para que a TI priorizasse** o que é essencial para a loja sem comprometer a experiência do cliente.

Milton Cetto Neto
Coordenador de TI
nater coop

O WiFeed simplificou o **gerenciamento seguro** e eficiente de ***vários Access Points*** em nossas filiais, atendendo a todas as **exigências legais de segurança.**

É a solução ideal para quem busca um gerenciamento seguro e eficiente da rede Wi-Fi corporativa.

Estamos presentes em *setores como varejo, saúde, financeiro, indústria, educação e serviços*:

+ de 12.000	+ de 70 mil	+ 22 milhões	88
locais	access points sob gestão	de usuários autenticados	NPS

Reconhecidos como **TOP 10 em Cibersegurança pelo 100 Open Startups.**

O WiFeed já faz a diferença na gestão da rede Wi-Fi corporativa de **gigantes do mercado:**

DECATHLON · NIKE · CENTAURO · SICOOB · ASSAI ATACADISTA · Unimed · CLAMED FARMÁCIAS · brf · HOSPITAL CARE · vivo · Vero · unifique

Em 2026, a pergunta não é se sua empresa será testada.

É quão preparada ela estará para responder e evoluir a partir disso.

Clique aqui para ver uma demo do WiFeed.