Microsoft Security

Proteger identidades na era da IA

Microsoft Entra ID Protection para segurança de identidade moderna

Sumário

01
Resumo executivo

02
O cenário em constante evolução das ameaças à identidade

03
Diretrizes práticas para líderes em segurança de identidade

04
Aprimore a segurança de identidade com o Microsoft Entra ID Protection

05
Clientes em ação

06
Recursos

01

Resumo executivo

A identidade é a base da segurança moderna e constitui a primeira linha de defesa. À medida que as organizações migram para a nuvem e adotam a IA, os invasores estão avançando com a mesma rapidez. Eles estão automatizando ataques de identidade em um ritmo e escala que nunca vimos antes. No último relatório sobre Acesso Seguro, 97% das organizações pesquisadas sofreram um incidente de acesso à identidade e à rede no último ano, e 70% relataram incidentes relacionados à IA.[1] Na Microsoft, detectamos 38 milhões de riscos de identidade todos os dias, e o risco continua crescendo[2].

A IA está remodelando ambos os lados da equação de segurança. Invasores estão usando IA para explorar fraquezas de identidade e adaptar suas técnicas em tempo real, enquanto defensores a utilizam para oferecer uma proteção de identidade mais forte e resiliente. Na Microsoft, recomendamos a mudança da resposta reativa para a proteção autônoma orientada por IA, a fim de criar uma postura de segurança mais adaptável e em camadas.

Este momento exige proteção de identidade adaptativa em tempo real. As organizações precisam de avaliação contínua do risco de identidade e de controles automatizados que eliminem as vulnerabilidades antes que os invasores possam explorá-las. Quando devidamente protegida, a identidade é sua defesa mais poderosa. Este white paper fornece insight sobre como o **Microsoft Entra ID Protection** auxilia as organizações a aprimorar sua estratégia de segurança de identidade e a manter-se à frente das ameaças de identidade em evolução.

1. Relatório sobre Acesso Seguro 2026, Microsoft
2. Relatório de Defesa Digital da Microsoft 2025, Microsoft

02

O cenário em constante evolução das ameaças à identidade

O comprometimento de identidade continua sendo o principal ponto de entrada para ataques cibernéticos

Diversas tendências macro estão acelerando os riscos de identidade. A maioria dos ataques começa com uma identidade comprometida, escolhendo como destino o roubo de dados, extorsão ou interrupção, e agora acontecem mais rapidamente devido à IA.

Suas credenciais ainda são o primeiro alvo... mas os invasores estão avançando na cadeia de privilégios

À medida que os ambientes de identidade se tornam mais complexos, os invasores continuam a depender de táticas de alto volume baseadas em credenciais. As táticas mais predominantes incluem ataques de spray de senha, força bruta, phishing e ataques de preenchimento de credenciais.

Ao mesmo tempo, os invasores estão aprimorando seus métodos com as seguintes técnicas: adversário no meio (AiTM), código do dispositivo e roubo de token.

97% dos ataques de identidade são spray de senha ou ataque de força bruta[2]

85% dos nomes de usuário escolhidos em ataques de spray de senha constavam em vazamentos de credenciais conhecidos[2]

A explosão de identidades: Identidades humanas, workloads e agentes de IA

Já estamos vendo o número de identidades não humanas crescer exponencialmente. Ao mesmo tempo, os sistemas modernos de IA introduzem classes completamente novas de identidades e caminhos de acesso. Apesar do aumento de produtividade proporcionado pela IA, 70% dos clientes entrevistados tiveram incidentes de segurança vinculados ao uso da IA no último ano[1]. Como resultado, um grande risco emergente é a proliferação de agentes de IA. Havia 110 milhões de agentes em 2025, com projeções da IDC apontando para 1,3 bilhão até 2028[3]. Muitos agentes operam com privilégios elevados, ultrapassam seu ciclo de vida previsto ou não têm visibilidade sobre o que podem acessar ou fazer, criando lacunas críticas que os invasores podem explorar, especialmente o acesso desprotegido a recursos confidenciais.

Quando o excesso de ferramentas se torna a ameaça

As equipes de Identidade e SOC estão sobrecarregadas devido às ferramentas fragmentadas de fornecedores terceirizados, sem uma visão unificada para investigar ou remediar ameaças. As equipes pesquisadas que operam com 6 consoles diferentes observam um aumento de 11% nos incidentes como resultado, com 40% das organizações afirmando que têm fornecedores diferentes demais[1]. Nenhuma equipe pode fazer a triagem manual desse volume de risco.

3. IDC Info Snapshot, patrocinado pela Microsoft, maio de 2025 (#US53361825)

03

Diretrizes práticas para líderes em segurança de identidade

As defesas tradicionais já não conseguem acompanhar o ritmo das ameaças em constante evolução. A proteção de identidade moderna não é apenas uma prioridade de segurança, mas sim uma prioridade crucial para os negócios. Para se manterem à frente, os líderes em segurança de identidade devem se concentrar em cinco áreas.

1

Investir em proteção adaptável e em tempo real

Controles e políticas estáticas não são mais suficientes para ataques de identidade. A proteção deve avaliar continuamente o comportamento e o risco, detectar ameaças em tempo real e adaptar o acesso adequadamente.

2

Aliar a detecção à remediação automatizada

Somente as detecções não poderão acompanhar o ritmo se a resposta depender de intervenção manual. A autorremediação automatizada precisa ser sem atrito e conter rapidamente identidades comprometidas, minimizando a interrupção para usuários legítimos.

3

Escalar a proteção de identidade com IA

A velocidade e o volume de ataques de identidade excedem a capacidade humana. A IA permite que as equipes de segurança analisem sinais em escala e respondam na velocidade da máquina. Escalar com IA é essencial para manter o controle em ambientes complexos.

4

Proteger todas as identidades, não só as dos funcionários

Os invasores visam cada vez mais identidades não humanas como forma de obter acesso privilegiado. A segurança de identidade deve estender proteção consistente a todos os tipos de identidade. Fechar essas lacunas reduz pontos cegos e limita o movimento lateral em todo o ambiente.

5

Reduzir sua superfície de ataque simplificando sua pilha de identidades

Ferramentas de identidade fragmentadas aumentam a complexidade, criam lacunas na visibilidade e elevam o risco operacional. Uma pilha unificada de segurança de identidade ajuda as organizações a impor controles consistentes, fortalece a postura de segurança e reduz a carga administrativa.

04

Aprimore a segurança de identidade com o Microsoft Entra ID Protection

O **Microsoft Entra ID Protection** é a solução premium de segurança de identidade que aplica decisões de acesso em tempo real enquanto bloqueia ameaças em velocidade de máquina. Ele oferece proteção de identidade agente por meio de IA para **proteger qualquer identidade, em qualquer lugar,** e interromper ataques acelerados por IA.

O Microsoft Entra ID Protection analisa **trilhões de sinais** para identificar riscos de autenticação e comportamentos incomuns de usuários em diferentes ambientes, aplicando automaticamente controles de acesso adaptável para neutralizar ameaças. Permite a autorremediação de riscos em todos os métodos de autenticação modernos, de senhas a métodos sem senha, para restaurar o acesso seguro sem comprometer a produtividade.

Integrado ao ecossistema de segurança da Microsoft, oferece proteção unificada de identidade que opera mais rapidamente do que soluções de terceiros. Os clientes obtêm um único mecanismo para prevenção, detecção e correção e **uma base mais forte para a defesa de identidade moderna.**

"Impedimos 33.000 tentativas de burlar o sistema antibot durante nossas primeiras seis semanas... Também impedimos 96.000 ataques de força bruta..."

Roy Corneloues, Arquiteto Corporativo, BT Group

Por que o Microsoft Entra ID Protection?

1. Detecte riscos em tempo real para se antecipar aos invasores

Diferentemente das ferramentas tradicionais de segurança de identidade que dependem de regras estáticas ou alertas após uma violação de segurança, o Microsoft Entra ID Protection avalia anomalias de logon em tempo real, permitindo que os clientes bloqueiem, contestem ou modifiquem solicitações de acesso. É fundamentado em um mecanismo de políticas líder do setor que funciona continuamente 24 horas por dia, 7 dias por semana, habilitado por trilhões de sinais em toda a Segurança da Microsoft para detectar padrões de comportamento sutis que se desviam da norma. Essa política adaptável responde dinamicamente às táticas emergentes dos invasores, protegendo contra ataques que vão desde spray de senhas até roubo de tokens.

2. Remedie riscos automaticamente para restaurar o acesso seguro

Quando uma identidade é comprometida, cada segundo conta. Uma remediação rápida e adequada é fundamental para conter ameaças e manter uma postura de segurança robusta. O Microsoft Entra ID Protection remedia automaticamente os riscos, dispensando a intervenção manual na resposta a incidentes e restaurando o acesso seguro sem impactar os usuários.

O Microsoft Entra ID Protection funciona em todos os métodos de autenticação modernos, independentemente de seus usuários ainda utilizarem senhas ou já adotarem autenticação sem senha. Quando se suspeita de comprometimento baseado em senha, o sistema aciona uma redefinição de senha segura ou exige MFA para conter a ameaça. Para usuários sem senha, o sistema simplesmente revoga sessões ativas e requer uma nova autenticação.

3. Proteja as identidades: humanas, de workload e de agentes

Organizações modernas dependem de muito mais do que apenas usuários humanos, incluindo identidades de workload e agentes de IA que interagem com dados, sistemas e APIs. O Microsoft Entra ID Protection protege todos eles por meio da detecção contínua de riscos, políticas de resposta adaptativa e proteção em tempo real em todo o ecossistema de identidades.

Prevê-se que as organizações que implementam o acesso condicional baseado em risco alcancem os seguintes resultados:

de redução nos tíquetes anuais de suporte técnico para redefinição de senha[4]

custos evitados ajustados ao risco ao longo de três anos[4]

4. Forrester Consulting, "The Total Economic Impact™ Of Microsoft Entra Suite", julho de 2025, encomendado pela Microsoft

NOVO: O Microsoft Entra Agent ID estende os controles de identidade do Microsoft Entra para agentes de IA ao atribuir a cada agente uma identidade de primeira classe, permitindo a descoberta centralizada e o inventário das identidades dos agentes. Isso permite que as organizações apliquem as mesmas proteções do Entra usadas para identidades humanas a agentes de IA. Com o Acesso Condicional do Microsoft Entra, as organizações podem segmentar agentes usando atributos de segurança personalizados e restringir ou bloquear automaticamente o acesso quando os sinais de proteção de identidade indicarem risco elevado ou comportamento anômalo. Isso pode reduzir as lacunas de governança causadas pela proliferação de agentes e melhorar a responsabilidade, a auditabilidade e a supervisão, ajudando a garantir que cada agente permaneça associado a um humano responsável durante todo o seu ciclo de vida.

4. Fortaleça a segurança de identidade na velocidade e escala da IA

À medida que os agentes de ameaças aumentam a velocidade dos ataques, as organizações precisam tomar decisões mais rápidas sobre o gerenciamento e a mitigação de riscos. O Microsoft Security Copilot no Entra traz orientação baseada em IA diretamente para o Microsoft Entra ID Protection, destacando por que um usuário é considerado de risco, acompanhando mudanças ao longo do tempo e recomendando etapas de remediação. Isso fornece aos administradores de TI e analistas de SOC o contexto adequado para agilizar as investigações, ajudar a melhorar a tomada de decisões e dar suporte a uma resposta a incidentes de alta qualidade.

5. Integração nativa em todo o ecossistema de segurança da Microsoft

O Microsoft Entra ID Protection é um componente fundamental do Microsoft Identity Threat Detection and Response (ITDR). Transmite sinais de risco de identidade diretamente para o Microsoft Defender XDR e o Microsoft Sentinel (SIEM), proporcionando uma visão integrada orientada à identidade das ameaças em toda a cadeia de ataque para otimizar os fluxos de trabalho de segurança de identidade. Isso permite que as equipes de SOC e de identidade previnam, detectem e respondam a ataques de identidade no contexto mais amplo da atividade de pontos de extremidade, emails, aplicativos e nuvem.

Como esses sinais abrangem toda a Segurança da Microsoft, o Microsoft Entra ID Protection pode fornecer insights mais completos por meio de sinais de risco unificados, decisões de acesso adaptáveis em tempo real e interrupção automatizada de ataques de identidade, sem a fragmentação de ferramentas. Essa abordagem unificada de ITDR ajuda a eliminar silos entre IAM e SOC, o que pode acelerar as investigações e fortalecer a resposta.

Prevê-se que as organizações que unificam sua pilha de segurança alcancem os seguintes resultados:

80% de redução no tempo médio de resposta graças ao contexto compartilhado e aos fluxos de trabalho coordenados[5]

60% de redução nos custos de ferramentas de segurança ao consolidar fornecedores[5]

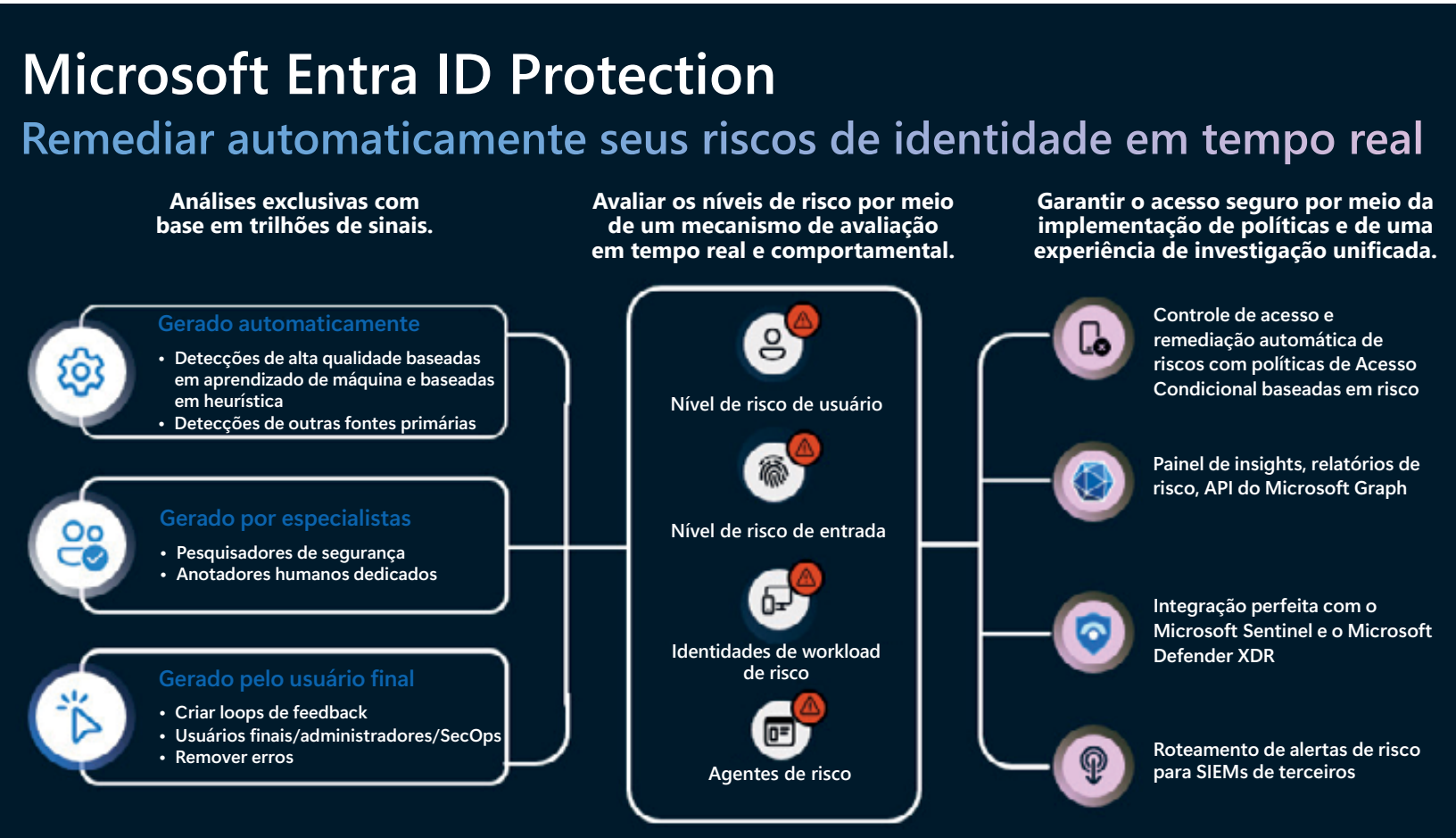
5. Forrester Consulting, "The Total Economic Impact™ Of Microsoft Defender", julho de 2025, encomendado pela Microsoft

Como funciona o Microsoft Entra ID Protection?

O Microsoft Entra ID Protection utiliza IA avançada e aprendizado de máquina baseado em nuvem, habilitado por **trilhões de sinais** em soluções de segurança da Microsoft, para bloquear ou mitigar riscos de identidade e impor políticas de acesso adaptativas.

Identificar entradas arriscadas e padrões de comportamento suspeitos do usuário, o Microsoft Entra ID Protection protege contra ataques de identidade, como ataques de força bruta, vazamento de credenciais ou tokens anômalos. Seus recursos principais:

- Impor políticas de acesso adaptativas baseadas em risco que funcionam 24 horas por dia, sete dias por semana para proteger qualquer identidade, humana ou não humana.
- Remediar automaticamente o comprometimento de identidade com suporte em todos os métodos modernos de autenticação, de senhas a chaves de acesso.
- Obter insights detalhados sobre sua postura de segurança de identidade para cenários de recuperação de desastre de TI (ITDR) de ponta a ponta.



Tipos de políticas de risco

As organizações podem usar as políticas do Microsoft Entra ID Protection para responder automaticamente a riscos de identidade, permitindo a autorremediação segura dos usuários quando atividades suspeitas são detectadas.

- As **Políticas de risco de entrada** avaliam se uma tentativa específica de autenticação provavelmente está sendo realizada por alguém que não seja o usuário legítimo. O Microsoft Entra ID Protection analisa centenas de sinais em tempo real (como endereço IP, token anômalo e padrões de autenticação) para calcular um nível de risco. Esse sinal de risco é encaminhado para o Acesso Condicional do Microsoft Entra, que pode aplicar controles como exigir verificação adicional ou bloquear o acesso.
- As **políticas de risco do usuário** avaliam a probabilidade de que uma conta tenha sido comprometida. Sinais como credenciais vazadas, atividade suspeita de API e comportamento arriscado do usuário contribuem para uma pontuação de risco do usuário. O Acesso Condicional aplica proteções para proteger a conta quando há suspeita de comprometimento.

Juntas, essas políticas oferecem uma defesa por camadas: As políticas de risco de entrada protegem tentativas de autenticação individuais, enquanto as políticas de risco do usuário protegem a conta como um todo.

Tipos de remediação automática de risco

As organizações podem automatizar a correção de problemas usando ações predefinidas, inclusive desafios de MFA, redefinição de senhas, revogação de sessões ou bloqueio de acesso. Selecionar os limites de risco apropriados (baixo, médio ou alto) permite que as equipes equilibrem uma segurança de identidade robusta com a experiência do usuário.

05

Clientes em ação

Estas histórias de clientes mostram como as organizações fortaleceram a segurança de identidade ao integrar o Microsoft Entra ID Protection em todo o ecossistema de segurança da Microsoft.

O **BT Group**, uma empresa global de telecomunicações, aprofunda a proteção contra sequestro de contas com o Microsoft Entra ID Protection, que utiliza IA para identificar e bloquear tentativas de acesso suspeitas. O BT Group criou sua estrutura de autenticação única (SAF) com base no Microsoft Entra ID, nas soluções de segurança da Microsoft e nas tecnologias Microsoft Azure. A solução SAF é uma grande usuária do P2, o nível de licenciamento premium do Entra.

"Bloqueamos 33.000 tentativas contra o sistema antibot durante as nossas primeiras seis semanas... Também bloqueamos 96.000 ataques de força bruta... Passamos de 6 milhões para 10 milhões de IDs em poucos meses após implementar nossa solução SAF baseada no Microsoft Entra ID..."

Roy Corneloues, Arquiteto Corporativo, BT Group

A **ElringKlinger**, uma fornecedora global do setor automotivo, protege identidades com várias soluções de identidade da Microsoft, construindo uma base Confiança Zero com o Microsoft Entra ID sem comprometer a produtividade dos colaboradores. Ajusta controles de acesso com políticas baseadas em risco no Microsoft Entra ID Protection, que transmite sinais para o Microsoft Defender para Identidade para uma proteção de identidade abrangente de ponta a ponta em ambientes na infraestrutura local e em nuvem. A ElringKlinger orquestrou sua migração para o Azure com uma reformulação da solução de segurança, implementando o Microsoft Defender para Nuvem, o Defender para Ponto de extremidade e o Defender para Office 365. Reforçou a segurança de identidade com o Microsoft Entra ID Protection.

"A combinação das soluções individuais de identidade da Microsoft é excelente. Isso nos ajuda a encontrar problemas que talvez não descobríssemos se tivéssemos soluções de identidade em silos, e facilita o trabalho da nossa equipe."

Alexander Maute, Diretor de Tecnologia de TI, ElringKlinger

O Microsoft Entra ID Protection oferece segurança de identidade em tempo real, impulsionada por IA, para proteger suas identidades humanas, de workload e de agentes. Integrado aos fluxos de trabalho nativos de Identity Threat Detection and Response (ITDR), permite identificar riscos com mais agilidade, responder mais rapidamente e reduzir a carga de trabalho das equipes de identidade e SOC.

Os ataques à identidade estão se tornando mais rápidos e sofisticados. O momento de agir é agora. Aprimore a segurança de identidade da sua organização com o Microsoft Entra ID Protection e antecipe-se às ameaças.

Comece a usar o Microsoft Entra ID Protection

Veja preços agora e entre em contato com a equipe de vendas

Inicie sua avaliação gratuita do Microsoft Entra ID P2 ou da Microsoft Defender Suite

Recursos:

- Aprofunde-se em como detecções de riscos e políticas de acesso baseadas em riscos funcionam
- Leia sobre tópicos relacionados: Detecção e resposta a ameaças à identidade
- Saiba mais sobre o Security Copilot no Microsoft Entra e o Microsoft Entra Agent ID
- Saiba como usar o Microsoft Entra ID Protection
- Planeje uma implantação do Microsoft Entra ID Protection