frame Trends

A NOVA LÓGICA DA CIBERSEGURANÇA PARA 2030

Transição da inteligência artificial para um arsenal estratégico e a redefinição da resiliência corporativa.

framework

PRODUCT · STRATEGY · ENGINEERING · GROWTH · AI

//intro

O fim do perímetro tradicional e a nova dinâmica de risco sistémico

Cloud, automação, analytics, IA generativa. Cada onda tecnológica chegou com a mesma promessa: fazer mais, mais rápido e com menos. O que raramente entra na pauta dos boards é o custo oculto dessa aceleração, uma dependência profunda de software, dados e terceirizações que expandiu a superfície de ataque para além de qualquer perímetro tradicional.

No ano de 2026, essa dinâmica muda de patamar. A Inteligência Artificial deixou de ser uma ferramenta periférica para ocupar o centro de um novo arsenal cibernético. De um lado, capacidades que blindam defesas. De outro, as mesmas tecnologias amplificando a escala e o impacto dos ataques. O fiel da balança é a governança.

A Inteligência Artificial deixou definitivamente de atuar como uma mera ferramenta periférica ou um facilitador de processos isolados para assumir a posição central de um novo e complexo arsenal cibernético.

Hoje, CEOs já posicionam a fraude cibernética e as vulnerabilidades de IA como riscos críticos, superando ameaças que dominaram a última década. Nesse cenário, a competitividade deixou de ser uma corrida por eficiência pura para se tornar uma disputa por resiliência cibernética: a capacidade de absorver choques, manter a operação durante incidentes e recuperar a normalidade antes que a relevância de mercado seja comprometida.

A pergunta estratégica não é mais "quanto a IA aumenta a eficiência?". É: qual parcela dessa eficiência sobrevive ao próximo incidente de grande escala? Responder a essa questão não é mais tarefa exclusiva do CISO. Exige uma liderança executiva que compreenda o impacto de cada decisão sobre alocação de capital e reputação de marca. Caso contrário, a cibersegurança continuará sendo vista como centro de custo quando, na verdade, é a condição de existência do negócio.

> A competitividade passou a depender da resiliência cibernética: a capacidade de absorver incidentes, manter a operação e recuperar a normalidade antes que o impacto comprometa o negócio.

#01

Redefinição do arsenal digital

A ascensão da IA agêntica e os novos vetores de risco de proporções inéditas

O núcleo da arquitetura de defesa e ataque contemporânea

Para entender a nova lógica da cibersegurança, é preciso começar pelos armamentos digitais: as tecnologias que executam decisões, movimentam dados e mantêm a operação funcionando. Estes não se referem a malwares tradicionais, mas sim às próprias capacidades tecnológicas de ponta adotadas pelas organizações, com destaque absoluto para a IA agêntica e as automações em larga escala que formam, atualmente, a linha de frente da execução produtiva nas corporações.

IA não é ferramenta, é armamento. Quando um agente executa sem supervisão, ele dispara riscos. A governança exige que alguém tenha o poder de desarmar a autonomia antes que o dano seja irreversível.

VULNERABILIDADE

EchoLeak

Em junho de 2025, pesquisadores revelaram uma falha crítica no Microsoft 365 Copilot. O vetor: um e-mail com instruções ocultas de prompt injection. Ao interagir com o Copilot, a ferramenta executava essas ordens silenciosamente acessando arquivos no Outlook, OneDrive e SharePoint e desviando-os para servidores externos. Para o usuário, tudo parecia normal. O problema não era técnico. Era de governança: a decisão de implantar o agente foi tomada sem que ninguém fizesse a pergunta fundamental quem responde por este agente quando algo der errado?

O Google Cloud Cybersecurity Forecast aponta que a adoção de agentes de IA para executar fluxos e decisões cresce a ponto de criar uma nova categoria de risco: o shadow agent, agentes implementados por áreas de negócio sem governança central, operando com acesso a dados e sistemas sensíveis. O World Economic Forum mostra que 94% dos líderes veem a IA como principal driver de mudança em cibersegurança, e 87% já percebem vulnerabilidades relacionadas à IA como o risco que mais cresce. Os armamentos digitais não são uma aposta de futuro. Eles já estão em uso.

Compressão crítica do tempo de resposta

BREAKOUT TIME

29 minutos

Tempo médio para expansão lateral após violação inicial redução de 65% em relação a ciclos anteriores

O ecossistema corporativo enfrenta, no atual panorama, uma assimetria severa e punitiva em relação à variável do tempo. As informações institucionais, as bases de clientes, a telemetria comportamental e a inteligência de negócios que, na taxonomia do novo arsenal cibernético, são rigorosamente classificadas como as "munições" estão a ser expostas num ambiente operacional onde o tempo de reação humano se tornou estatisticamente insuficiente e taticamente obsoleto.

Em 2025, o breakout time médio de eCrime caiu para 29 minutos — 65% mais rápido do que no ciclo anterior, com casos extremos em segundos. Em paralelo, 82% das detecções já são malware-free: ataques baseados em abuso de credenciais e superfícies pouco monitoradas. Isso elimina a ilusão de que equipes podem parar, analisar e depois reagir. Os adversários modernos não invadem sistemas. Eles se autenticam neles.

A esmagadora maioria das deteções de intrusão mais recentes explora identidades válidas, configurações incorretas e credenciais roubadas ataques malware-free que simplesmente contornam a infraestrutura tradicional.

Os adversários modernos não necessitam de invadir os sistemas; eles autenticam-se neles.

VOLUME EXPOSTO

16TB

Base MongoDB não protegida

PERFIS COMPROMETIDOS

4.3B

Perfis profissionais detalhados

Quando bases de dados massivas são expostas em infraestruturas na nuvem devido a negligência configuracional, o impacto transcende largamente as severas sanções regulatórias relativas à proteção de dados. Um estudo de caso incontornável desta realidade foi a exposição pública de uma base de dados MongoDB contendo 16 Terabytes de informação não protegida por qualquer mecanismo de autenticação.

Este repositório, acumulado à escala industrial, albergava cerca de 4,3 mil milhões de perfis profissionais detalhados, contendo o histórico empregatício, contactos diretos e cruzamentos organizacionais.

Valor tático dos dados expostos

Este incidente é um exemplo crítico de como o acúmulo de dados em larga escala, quando exposto, alimenta campanhas globais de phishing, engenharia social e ataques de prompt injection potencializados por IA. Dados sem contexto não são munição. O perigo não está nos dados em si, está em não saber o que eles podem fazer quando alimentam uma IA que age sozinha.

#02

Imperativos arquiteturais

O deslocamento para a prevenção ativa e a arquitetura resiliente por design

Garantia de sobrevivência e migração para prevenção

PROJEÇÃO ORÇAMENTAL

50%

ATÉ 2030
do orçamento total de cibersegurança

Migração substancial de recursos para soluções preemptivas e infraestrutura segura

A garantia de sobrevivência corporativa perante um cenário de ameaças tão agudo exige o abandono definitivo da dependência exclusiva de soluções e processos focados na deteção e resposta a posteriori, impondo a adoção de uma arquitetura que seja inequivocamente resiliente por design.

Esta realocação reflete-se na exigência imperativa de implementação de projetos de defesa estruturais. Torna-se estritamente necessário, por exemplo, o estabelecimento de ecossistemas de identidade e gestão de acessos (IAM) desenvolvidos especificamente para atores não humanos.

A Gartner projeta que soluções preemptivas chegarão a 50% do gasto em segurança de TI até 2030, vindo de menos de 5% em 2024. Agentes de IA precisam de identidades próprias — com propósito declarado, dono humano responsável e políticas de menor privilégio específicas para atores de máquina. Sem arquitetura sólida de identidade e dados, a diferença de tempo entre ataque e resposta favorece o atacante.

IMPERATIVO

Identidades digitais autónomas para automações e agentes de IA com políticas de menor privilégio

Colapso operacional e defesa em profundidade

ATACANTE

Scattered Spider

VETOR

Fornecedor terceiro

MÉTODO
Engenharia social

ALVO
Cadeia de fornecimento

IMPACTO
Centenas de milhões £

A vulnerabilidade inerente à ausência desta arquitetura de defesa integrada foi severamente exposta no colapso operacional sofrido pela gigante retalhista britânica Marks & Spencer. O ataque, orquestrado pelo grupo especializado Scattered Spider, não visou a infraestrutura primária da empresa de forma direta, mas sim um fornecedor terceiro de extrema confiança dentro da sua malha de fornecimento.

Através do comprometimento de credenciais parceiras e de técnicas avançadas de engenharia social, os atacantes infiltraram-se de forma silenciosa e procederam à inativação em cascata dos sistemas críticos de automação de inventário, plataformas de pagamento e redes logísticas da retalhista.

O resultado não foi um mero constrangimento técnico, mas uma paralisação sistémica que forçou uma operação global multimilionária a retroceder a processos manuais baseados em papel.

Este colapso não foi causado por uma falha direta na M&S, mas pela ausência de controles integrados. O problema não foi técnico foi arquitetural. Nenhum terceiro deveria ter esse nível de acesso sem controles de identidade equivalentes aos internos. Defesa sem arquitetura é apenas um catálogo de ferramentas boas. E catálogos não impedem colapsos em cadeia.

#03
Governança integrada

A orquestração sistémica como condição indispensável para a resiliência operacional em escala

Orquestração da resposta e governança do ecossistema de IA

MODELO DE ORQUESTRAÇÃO INTEGRADA

01
Inventário
Mapeamento contínuo de agentes e automações

02
Identidade
Credenciais e privilégios mínimos por contexto

03
Monitorização
Telemetria unificada em tempo real

04
Resposta
Playbooks automatizados e testados sob stress

A tecnologia dita a velocidade do ataque. A governança dita a velocidade da sobrevivência. Quando o CISO não tem mandato real sobre a IA, a governança não quebra por falta de software, ela quebra porque a máquina é mais rápida do que uma liderança sem poder para dizer não.

O primeiro imperativo da governança integrada reside no inventário exaustivo e contínuo de todos os agentes autónomos e automações em execução no ecossistema corporativo. Sem visibilidade total, a capacidade de deteção e contenção torna-se estruturalmente impossível.

Paralelamente, a resposta a incidentes exige deixar de ser um exercício reativo e esporádico para se tornar um processo orquestrado, testado em simulações de adversário realistas e integrado em todas as unidades de negócio. A cadeia de comunicação entre o CISO, o conselho de administração e as equipas operacionais deve estar codificada e treinada.

REQUISITO CRÍTICO

Os planos de continuidade de negócio devem contemplar explicitamente a falha de componentes de IA, não apenas de infraestrutura física ou humana.

Vácuo de autoridade e a cascata de privilégios não controlada

SEQUÊNCIA DO INCIDENTE — CLASSIFICAÇÃO SEV-1

01

Agente sem restrições

IA interna publica recomendações proativas em fóruns de engenharia

02

Validação inadvertida

Engenheiro valida sugestão sem reconhecer o escalonamento implícito

03

Cascata automática

Propagação de privilégios em 2 horas para bases de dados ultrassecretas

04

Paralisia de comando

Kill switch não existia — dobro do tempo para estabelecer cadeia de autoridade

A consequência nefasta da ausência de estrutura de comando e controlo ficou severamente evidenciada no incidente de gravidade extrema classificado como Sev-1 pela Meta. O colapso teve origem num agente interno de inteligência artificial que, desprovido de restrições rígidas de atuação, iniciou a publicação de recomendações proativas em fóruns corporativos de engenharia. Numa janela de apenas duas horas, utilizadores sem as credenciais adequadas obtiveram acesso a bases de dados ultrassecretas da companhia.

> **Não havia uma política escrita sobre o que a IA podia fazer. Pior: ninguém sabia quem tinha autoridade para desligá-la.**
>
> A falha técnica levou 90 minutos para comprometer a infraestrutura. A organização levou 180 minutos apenas para descobrir quem podia tomar uma decisão acima do nível operacional. Esse atraso dobrou o tempo de exposição ao risco.

Proibir IA sem governança não reduz o risco empurra o uso para o shadow AI, onde dados sensíveis alimentam ferramentas externas sem supervisão e criam decisões que ninguém consegue auditar depois. O resultado é mais exposição, menos controle e zero valor gerado.

#04

Mandato executivo

A coesão da liderança executiva e o papel do CISO como vetor estratégico de sobrevivência corporativa

O papel do CISO e a coesão da liderança na era da IA adversarial

01

Visibilidade

Relatórios executivos traduzindo risco técnico em impacto financeiro e reputacional mensurável

02

Advocacia

Posicionamento da cibersegurança como imperativo estratégico, não custo operacional isolado

03

Coesão

Alinhamento transversal entre CISO, CFO, COO e conselho de administração nos cenários de crise

A maturidade cibernética de uma organização é, em última análise, um reflexo direto da maturidade da sua liderança executiva. Em 52% das organizações, o CISO já responde por estratégias de risco de IA e pelos controles de cibersegurança associados. O que falta é transformar esse movimento em mandato claro. A liderança precisa escolher: segurança responde apenas pelos aspectos técnicos, ou também participa das decisões sobre onde IA pode ser usada, com quais dados, sob quais limites de risco?

REALIDADE ORGANIZACIONAL

73%

das organizações não possuem um plano de resposta a incidentes testado e atualizado para cenários de falha de IA

73% das organizações não possuem um plano de resposta a incidentes testado para cenários de falha de IA. Se você não valida aquilo que prometeu que funcionaria, você não tem um plano de continuidade, você tem um documento de fé cega.

> "A ausência de simulação é, por si só, um vetor de risco de primeira ordem."

As organizações que emergirão desta era com competitividade intacta serão aquelas cujos conselhos de administração compreenderem que a cibersegurança não é uma questão de tecnologia é uma questão de governança corporativa, responsabilidade fiduciária e continuidade de valor para todas as partes interessadas.

Governança como determinante inexorável da sobrevivência

A assimetria instaurada pela adoção massiva e não criteriosa da inteligência artificial transformou, em caráter permanente e definitivo, o cenário corporativo global. Este novo paradigma impõe uma velocidade de execução tática predatória, onde os ataques adversários não apenas se multiplicam, mas ocorrem num formato de hiperescala automatizada e adaptativa.

Neste contexto de hostilidade latente, os ativos de informação não governados de uma organização convertem-se, invariavelmente, nas armas empunhadas pelo próprio adversário.

PILAR 1

Prevenção

Arquitetura resiliente por design

PILAR 2

Governança

Orquestração integrada e testada

PILAR 3

Liderança

Coesão executiva e maturidade

A maioria das empresas já opera com agentes de IA, fluxos automatizados e dados em massa. O que separa organizações resilientes das que sucumbirão ao primeiro incidente real é a transição de uma coleção de iniciativas para um ecossistema operacional integrado. Não é a velocidade de adoção da IA que faz essa diferença. É a capacidade de continuar operando quando esse arsenal for testado sob fogo real.

> Não controlamos o ritmo da inovação tecnológica global, nem a audácia dos adversários. Controlamos a forma como conectamos visão, engenharia e resiliência para responder a eles. O próximo passo é transformar as brechas do seu arsenal atual em barreiras de defesa.

Fontes e referências

- Gartner. A CISO's Guide to AI Cyber Stewardship. 21 jul. 2025. ID G00833612.
- Gartner. Top Trends in Cybersecurity for 2026. ID 840672.
- Gartner. Cybersecurity Trend / material complementar de tendências de cibersegurança para 2026.
- World Economic Forum. Global Cybersecurity Outlook 2026.
- Google Cloud. Cybersecurity Forecast 2026.
- CrowdStrike. 2026 Global Threat Report.
- Verizon. 2025 DBIR Manufacturing Snapshot.
- Cybersecurity Ventures. Estimating Global Yearly Cybercrime Damage Costs.
- Gartner. Cybersecurity Leadership Vision for 2026.

Caso 1 — EchoLeak / Microsoft 365 Copilot

Microsoft Security Response Center. CVE-2025-32711.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32711

NIST NVD. CVE-2025-32711 Detail.
https://nvd.nist.gov/vuln/detail/cve-2025-32711

CVE.org. CVE-2025-32711 Record.
https://www.cve.org/CVERecord?id=CVE-2025-32711

Caso 2 — Exposição de 16TB no MongoDB

Security Affairs. Experts found an unsecured 16TB database containing 4.3B professional records.
https://securityaffairs.com/185661/data-breach/experts-found-an-unsecured-16tb-database-containing-4-3b-professional-records.html

Paubox. Unsecured 16TB database exposes billions of professional profiles.
https://www.paubox.com/blog/unsecured-16tb-database-exposes-billions-of-professional-profiles

Caso 3 — Marks & Spencer / Scattered Spider

The Hacker News. Scattered Spider Behind Cyberattacks on M&S and Co-op.
https://thehackernews.com/2025/06/scattered-spider-behind-cyberattacks-on.html

Vorboss. Marks & Spencer cyberattack: Scattered Spider.
https://vorboss.com/blog/marks-spencer-cyberattack

Caso 4 — CrowdStrike Falcon / apagão global

CrowdStrike. Falcon Content Update Preliminary Post Incident Report.
https://www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/

Microsoft. Helping our customers through the CrowdStrike outage.
https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

Caso 5 — Agentes de IA e incidente SEV-1 na Meta

AGAT Software. AI Agent Security: Meta's Rogue AI Agent Incident.
https://agatsoftware.com/blog/ai-agent-security-meta-rogue-agent-incident/

Kiteworks. AI Agent Errors Trigger Sev-1 Security Incident at Meta.
https://www.kiteworks.com/cybersecurity-risk-management/meta-rogue-ai-agent-data-exposure-governance/

frameTrends

framework

PRODUCT · STRATEGY · ENGINEERING · GROWTH · AI