

cirion

FORTINET

Cibersegurança:

Quando a IA altera riscos, a segurança altera sua arquitetura



Índice

1. Introdução: O que a IA mudou para a empresa	3
IA e cibersegurança: dados “ameaçadores”	4
2. A segurança começa com a conectividade	5
Segurança avançada na arquitetura de rede	5
Recursos do Serviço Gerenciado SD-WAN da Cirion	6
3. Identidade: matéria-prima para atacantes	7
Zero trust: o fim da confiança automática	7
Identidade: os números de risco	7
4. A aceleração dos ataques e o limite da resposta manual	8
DDoS Mitigation: evitar que o problema chegue ao negócio	8
5. O desafio de gerenciar uma arquitetura de segurança cada vez mais complexa	9
Compromissos do SNOC (caixa)	9
6. Segurança como capacidade operacional	10
7. Diferenciadores: Por que Cirion	11
8. Conclusões	12

1. Introdução: O que a IA mudou para a empresa



Muito se fala sobre como a IA evolui a forma como as empresas trabalham, tomam decisões e escalam suas operações. Mas, ao mesmo tempo, outra transformação paralela está acontecendo: como as organizações devem proteger seus dados e seus sistemas.

O cenário tecnológico já vem crescendo em complexidade nos últimos anos. As aplicações não estão mais concentradas em um único ambiente. As organizações combinam servidores próprios, nuvens públicas, edge, serviços SaaS, filiais, trabalhadores remotos, dispositivos móveis e provedores externos. Cada nova conexão adiciona capacidade ao negócio, mas também introduz um novo relacionamento que precisa ser gerenciado e protegido.

A IA adiciona um ingrediente adicional a esse mapa de complexidade. Porque, assim como permite automatizar tarefas que antes exigiam intervenção humana, acelera a tomada de decisão e impulsiona a eficiência, também acelera a geração de ataques e amplia o volume de tentativas em infraestruturas cada vez mais distribuídas.

O fenômeno está acelerando. Segundo a consultoria McKinsey, 88% das organizações já utilizam IA em pelo menos uma função, enquanto 62% experimentam agentes de IA. Cerca de dois terços das organizações

ainda estão em estágios piloto. A tecnologia está avançando a passos largos, enquanto muitas vezes as arquiteturas ainda não foram adaptadas para suportá-la.

Ao mesmo tempo, a IA está envolta em um paradoxo, especialmente quando se trata de cibersegurança. Por um lado, ela oferece às empresas ferramentas poderosas para antecipar ataques, investigar padrões de comportamento anômalos e acelerar defesas. Mas, por outro, essas mesmas ferramentas estão disponíveis para atacantes, que podem automatizar tarefas e alcançar escalas nunca antes vistas.

A corrida está acontecendo agora: contra um oponente correndo em velocidade máxima, confiando em estruturas onde as pessoas são alertadas, interpretam, determinam sua relevância, identificam o ativo afetado e decidem o que fazer pode ser sinônimo de chegar tarde demais.

O relatório M-Trends 2026, do Google Cloud e Mandiant, apresenta números sobre essa possível assimetria: a transferência mediana de um incidente passou de mais de oito horas em 2022 para apenas 22 segundos em 2025. Isso, em termos simples, significa que o tempo que um atacante leva para se mover de um sistema comprometido para outro caiu drasticamente.

Além disso, há o crescimento da exposição regional. A Check Point registrou em média 3.561 ataques semanais por organização em abril de 2026 na América Latina (a mais afetada do mundo), o que representa um aumento de 19% ano a ano. E o World Economic Forum identificou uma lacuna crítica de talentos em cibersegurança que atinge 65% das organizações na América Latina e no Caribe.

Em outras palavras, há mais ameaças, elas chegam mais rápido e não necessariamente há mais pessoas para gerenciá-las. À medida que a velocidade dos negócios aumenta, o tempo disponível para detectar, analisar e responder a um incidente é reduzido.

Nesse contexto, adicionar ferramentas de segurança não é mais sinônimo de estar melhor protegido. Quando cada camada funciona de forma independente, a organização também adiciona consoles, políticas, integrações e processos que alguém deve gerenciar. A complexidade pode se tornar, por si só, uma nova superfície de risco. A estratégia deve

se concentrar, então, em definir uma arquitetura capaz de conectar, proteger, observar e responder de forma consistente.

Cobertura contínua, visibilidade e capacidade de responder em tempo real agora são capacidades indispensáveis. Mas o desafio não é apenas detectar mais rápido. Também se torna imperativo fazer isso sem adicionar mais complexidade. A segurança deve ser integrada à arquitetura da rede, operar de forma consistente e ajudar o negócio a continuar funcionando mesmo diante de uma ameaça.

Este whitepaper analisa como o cenário de cibersegurança muda com a expansão da IA e infra-estruturas cada vez mais distribuídas. Aborda a ligação entre conectividade e segurança, o papel crítico da identidade, a aceleração de ataques e os limites de uma resposta baseada exclusivamente em intervenção manual, bem como o desafio de gerenciar arquiteturas cada vez mais complexas. O objetivo é avançar para uma concepção de segurança como uma capacidade operacional, integrada à infraestrutura e operação do negócio.

IA e cibersegurança: dados “ameaçadores”

- **O atacante não só consegue invadir os sistemas em 22 segundos: M-Trends detectou que, uma vez que entra, permanece em média 14 dias antes de ser detectado ou o incidente terminar.**
- **Reguladores da região estão estabelecendo prazos de detecção muito abaixo dessa média: Chile exige alerta precoce em 3 horas e relatório completo em 72 horas (Lei 21.663), Colômbia, 24 horas no setor financeiro (Circular Externa 007 de 2018 da Superintendência Financeira) e Brasil dois dias úteis antes da ANPD (Agência Nacional de Proteção de Dados). A Cirion permite que as empresas cumpram esses prazos.**
- **De acordo com o World Economic Forum, 94% apontam a IA como o principal motor de mudança e 87% colocam as vulnerabilidades da IA como o risco que mais cresce..**
- **De acordo com o Cost of a Data Breach Report 2026, preparado pela IBM e pelo Ponemon Institute, 19% dos ataques maliciosos são habilitados por IA.**
- **O FortiGuard Labs indica que as vítimas confirmadas de ransomware passaram de cerca de 1.600 para 7.831 em um ano: um aumento de 389%, impulsionado por kits de cibercrime baseados em IA.**

2. A segurança começa com a **conectividade**



A conectividade hoje representa mais nas empresas do que o transporte de dados de um lugar para outro. Na verdade, quando não é bem resolvida, constitui um grande obstáculo à inovação e ao crescimento. O relatório Enterprise Horizons 2025, da consultoria de mercado IDC, detectou que 94% das organizações encontram em sua rede o limite para avançar em projetos tecnológicos de grande escala, especialmente aqueles envolvendo IA. Além disso, outros 45% relatam problemas específicos de latência.

Quando falamos sobre o modelo de segurança, a primeira referência que temos é aquela que foi construída em torno da ideia de "proteger o perímetro". Mas esse perímetro tem se tornado cada vez mais difícil de definir. Hoje, usuários, aplicações e dados podem ser encontrados em diferentes redes, nuvens, ramificações e locais. Proteger o ponto de entrada está longe de ser suficiente. O tráfego deve ser observado e protegido em toda a arquitetura.

A rede é consolidada como um ponto estratégico de controle. Não pode haver janela de tempo entre o momento da conexão e o momento em que a proteção é ativada. Quando a segurança faz parte do serviço de conectividade, essa lacuna desaparece.

Segurança avançada na arquitetura de rede

Esse princípio está por trás do Secure SD-WAN da Cirion, que integra segurança avançada diretamente à arquitetura da rede. A solução otimiza o tráfego, prioriza aplicações críticas e gerencia centralmente políticas de segurança, incorporando capacidades como firewall de próxima geração, criptografia e proteção de sites remotos e ramificados. Ela também combina diferentes tipos de acesso, incluindo links Cirion e acesso fornecido pelo cliente.

A vantagem é operacional. Quando conectividade e segurança são gerenciadas a partir de uma arquitetura integrada, o número de componentes que precisam ser gerenciados separadamente é reduzido e obtém-se uma visão mais consistente do que está acontecendo na rede.

A mesma lógica aparece na proposta SASE da Cirion, que converge funções de rede e segurança em um único serviço baseado na nuvem. Nesse modelo, Secure SD-WAN, ZTNA (zero trust network access, conceito que explicaremos mais adiante) e outras capacidades de segurança funcionam dentro de uma arquitetura unificada, com políticas consistentes e gestão centralizada.

Historicamente, os gerentes de cibersegurança enfrentavam o desafio de encontrar mecanismos para proteger a rede. Hoje, porém, está sendo feito um trabalho para projetar uma rede que já incorpore proteção desde o próprio projeto.

Recursos de Serviço Gerenciado SD-WAN da Cirion



A Cirion atende 7x24x365 das plataformas SD-WAN e de segurança que gerencia, com escalonamento para especialistas e práticas de gestão de Nível 2 e 3 sob ITIL v4.



Orquestrar a gestão usando o FortiManager e análises e relatórios usando o FortiAnalyzer.



Não entrega um produto, mas opera uma arquitetura que permite consultar registros e eventos, gerar relatórios e adaptar dashboards às necessidades operacionais, auditorias ou requisitos regulatórios.



Dados de conectividade e segurança não são mais distribuídos entre diferentes ferramentas sem uma leitura comum e podem se tornar evidências para entender o que está acontecendo, acelerar a análise da causa raiz e tomar decisões.



É oferecido em três modalidades: Connect, quando a segurança está concentrada no hub; Pro-tect, quando cada local precisa de sua própria proteção; AI, quando funções de prevenção de vazamento de dados e assistência por IA são adicionadas.

3. Identidade: **matéria-prima para atacantes**

Outra transformação torna insuficiente o perímetro antigo: a identidade. Um usuário pode se co-nectar a partir de um escritório, de casa, de um dispositivo móvel ou de um local de terceiros. Uma aplicação pode estar em uma nuvem pública, e um provedor externo pode precisar de acesso temporário a um recurso corporativo. Nesses cenários, saber que alguém tem uma se-nha não é prova suficiente.

Credenciais são um componente central de incidentes que afetam ambientes cloud. O problema vai muito além de uma senha sendo roubada: uma credencial válida é um portal legítimo para recursos que o atacante não deveria ser capaz de usar.

Zero trust: o fim da confiança automática

Em vez de assumir que uma identidade é confiável porque entrou, cada sessão deve ser avalia-da de acordo com sua identidade, contexto, dispositivo e postura.

Zero trust (confiança zero) é um modelo de segurança baseado na premissa de nunca confiar per se que um usuário é válido, mesmo que esteja dentro da rede, mas verificar toda vez. Ele assu-me que ameaças já podem ter invadido sistemas ou que podem vir de qualquer lugar. Portanto, não concede automaticamente confiança a ninguém, independentemente de ser o CEO da em-presa conectado ao escritório central. O acesso não é herdado: é conquistado.

ZTNA é a implementação desse conceito. Na Cirion, assume o nome de Identidade do Usuário. A permissão não é mais uma propriedade permanente de uma credencial e é avaliada por sessão, reduzindo o acesso ao mínimo necessário. Isso é especialmente relevante quando terceiros es-tão envolvidos: contratados, fornecedores, parceiros de tecnologia e outros colaboradores po-dem precisar de acesso a certos recursos sem que isso signifique que devem se juntar à rede corporativa com os mesmos privilégios que um funcionário.

A identidade deve ser vista como uma política de segurança e não como um simples mecanismo de autenticação. Se uma credencial pode ser comprometida, é necessário determinar quais condições adicionais devem ser atendidas para conceder acesso. Uma arquitetura integrada é fundamental: a SD-WAN pode evoluir para modelos de segurança mais amplos e facilitar a tran-sição para arquiteturas SASE/SSE, sempre de acordo com a viabilidade e o escopo específico de cada implantação.

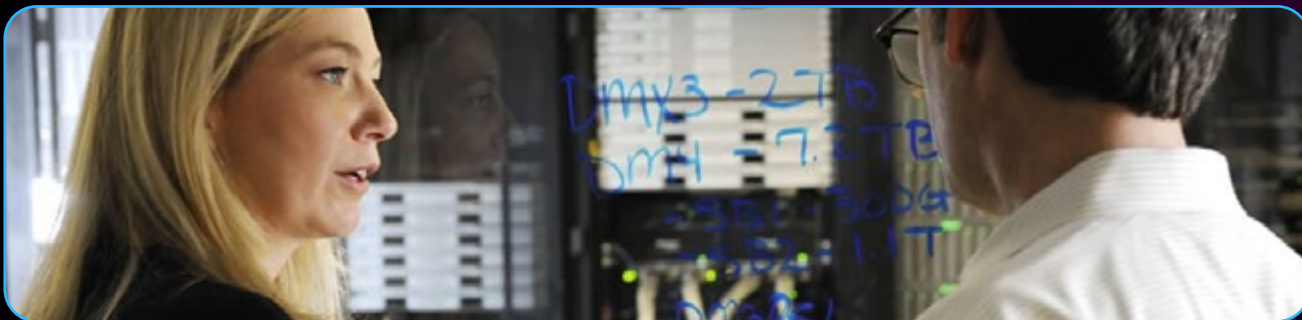
Nessa jornada, não é necessário substituir a arquitetura existente de uma vez. É possível trans-ferir progressivamente o controle para onde reside o risco: o usuário, o dispositivo, a aplicação e o contexto de cada conexão. A tendência, nesse sentido, é imparável: a Gartner sustenta que 70% das compras de SD-WAN farão parte de uma plataforma SASE de um único fornecedor em 2028, em comparação com 25% em 2025.

Identidade: os números de risco

- **35,4 milhões** de acessos corporativos comprometidos disponíveis até 2025.
- **67.650 bilhões** de tentativas de força bruta durante o ano: cerca de 185 milhões por dia.
- **Crescimento anual de 79%** nos registros disponíveis de roubo de credenciais.

(Fuente: Global Threat Landscape Report 2026, FortiGuard Labs)

4. A aceleração dos ataques e o limite da resposta manual



Detectar um ataque não é o mesmo que chegar a tempo de detê-lo. Ataques DDoS (distributed denial of service), que buscam derrubar um site, servidor ou serviço digital inundando-o com uma enorme quantidade de tráfego falso até que fique saturado, extremamente lento ou trave completamente, mostram essa diferença de forma particularmente clara.

A Cloudflare registrou um ataque de 31,4 Tbps durante o primeiro semestre de 2026 que durou apenas 35 segundos. No mesmo período, 90,6% dos ataques na camada de rede duraram me-nos de dez minutos. Quando um incidente pode começar e terminar nessa velocidade, as limita-ções dos modelos baseados apenas na reação humana são mais do que evidentes.

Se a organização primeiro precisar detectar a anomalia, confirmar que é um ataque, abrir um chamado e solicitar ação, é cada vez mais provável que o tempo de resposta seja maior do que a duração do próprio incidente. A proteção deve estar próxima ao local onde o tráfego ocorre. Para usar o exemplo acima: um ataque de 35 segundos não é mitigado com uma equipe na borda do cliente ou uma ligação para o provedor, mas sim no backbone, de forma automatizada e sempre ativa, antes que o tráfego chegue ao negócio.

DDoS Mitigation: evitar que o problema chegue ao negócio

DDoS Mitigation da Cirion detecta, filtra e limpa o tráfego volumétrico, de protocolo e de aplica-ção dentro do seu backbone antes que ele chegue à infraestrutura do cliente. O serviço pode operar sob demanda ou sempre ativo, com assistência do centro de operações.

O mesmo princípio se aplica ao roteamento. A proteção contra sequestro de prefixos e desvio malicioso não começa necessariamente com um firewall, mas primeiro, pela própria infraestrutura que determina para onde o tráfego flui.

A implementação do RPKI no backbone AS3356 que a Cirion opera na América Latina adiciona essa camada de proteção no roteamento. O AS3356 identifica um backbone Tier 1 com escopo regional, conectada a milhares de sistemas autônomos. Essa escala permite que a segurança do tráfego seja abordada a partir da própria infraestrutura de rede.

A lógica por trás disso: algumas ameaças só podem ser efetivamente abordadas quando são abordadas na camada onde se originam. Em um mundo distribuído, a cibersegurança não pode ser concentrada no perímetro da empresa.

5. O desafio de gerenciar uma arquitetura cada vez mais complexa



O atacante trabalha em velocidade de máquina e a região, como mencionado, não é talentosa o suficiente para lidar com essa escala. Ninguém ganha comprando mais ferramentas desconexas: a defesa é sustentada por pessoas, processos e vigilância contínua.

É aí que surge o conceito de operação como parte da segurança. Historicamente, as empresas gerenciavam, por um lado, o NOC (network operations center), que cuidava de que a internet não caísse e que os servidores funcionassem rápido, e, por outro, o SOC (security operations center), que procurava hackers, vírus e violações de segurança. Hoje, o SNOC quebra essa barreira: no mundo real, uma queda de sistema e um ataque cibernético são frequentemente o mesmo problema visto sob ângulos diferentes.

Se, além disso, esse serviço for gerenciado, a empresa tem a possibilidade de transferir grande parte da carga diária (monitoramento, gestão de mudanças, gerenciamento de incidentes, análise, relatórios e escalonamento) para equipes especializadas, sem que a organização perca o controle sobre suas políticas.

Nenhum alerta deve ser deixado esperando a próxima vez para ser interpretado. O desafio não é apenas incorporar mais ferramentas, mas também ter cobertura contínua e a capacidade de correlacionar informações em tempo real. Um centro de operações que monitora a rede pode detectar sinais antes que se tornem um ticket, porque rede e segurança fazem parte da mesma operação e não sistemas independentes que precisam cruzar registros depois do fato. Além dessa vigilância 24x7, o SNOC adiciona serviços profissionais que incluem avaliação, design, implantação e reforço da infraestrutura.

Compromissos SNOC

- Tempos de escalabilidade comprometidos atendem às demandas cada vez mais exigentes dos reguladores.
- Gestão de mudanças.
- Serviços profissionais: avaliação, configurações avançadas, reforço e ethical hacking (testes de penetração e análise de vulnerabilidades).
- Evidência para o regulador: Análises centralizadas fornecem relatórios padrão ou personalizados e retêm registros para responder quando foram detectados, quando foram contidos e quando foram reportados.

6. Segurança como **capacidade operacional**



A transformação digital não termina com uma certa tecnologia. Depois da nuvem vieram os ambientes híbridos. Depois, o trabalho distribuído. Agora, inteligência artificial e agentes estão incorporando novas formas de interagir entre usuários, aplicações e dados. Cada etapa coloca a arquitetura à prova novamente.

Por isso, a segurança precisa ser projetada com capacidade de evolução. A convergência entre conectividade, segurança e operação modifica o objetivo da arquitetura.

Estratégias antigas, como acumular controles para cobrir todas as ameaças possíveis, estão se tornando obsoletas. Hoje, é necessário definir uma arquitetura que permita reduzir a exposição, aplicar políticas de forma consistente, detectar mudanças e responder rapidamente sem transferir toda a complexidade para a equipe interna.

Essa mudança é particularmente relevante à medida que as empresas incorporam mais IA. Cada novo agente, aplicação ou fluxo automatizado aumenta a velocidade dos negócios, é verdade, mas também aumenta o número de interações que precisam ser controladas.

A arquitetura deve acompanhar esse crescimento sem se tornar um gargalo. Nesse contexto, uma rede inteligente precisa de muito mais do que disponibilidade de conectividade:

- **Visibilidade.**
- **Políticas.**
- **Controle de identidade.**
- **Capacidade de inspeção.**
- **Mecanismos de resposta.**
- **Operação.**

E, talvez o mais importante: a arquitetura de cibersegurança deve estar preparada para evoluir junto com o negócio.

7. Diferenciadores: Por que Cirion



A rede da Cirion é a base sobre a qual essas capacidades são integradas. A empresa possui mais de 105.000 quilômetros de sua própria fibra na América Latina, uma rede Tier 1, com pre-sença direta em 12 mercados e alcance de rede em mais de 20 países. Esse controle sobre a infraestrutura permite que certas capacidades de segurança sejam aplicadas mais próximo da origem do tráfego e não apenas no perímetro do cliente.

Mas, além disso, a diferença entre uma estratégia de segurança e um conjunto de ferramentas está na capacidade de mantê-la ao longo do tempo. A Cirion integra conectividade, segurança e operação sobre essa infraestrutura regional própria e implanta capacidades que respondem a diferentes pontos da arquitetura: Internet dedicada com segurança integrada, IP VPN, Cloud Connect, Secure SD-WAN, User Identity (ZTNA), Firewall & UTM e DDoS Mitigation.

O modelo incorpora operação contínua. O NOC/SOC 24x7x365 na mesma rede que transporta o tráfego do cliente permite que a segurança não se limite à tecnologia instalada, mas faça parte de uma capacidade permanente de monitoramento e gestão.

No Secure SD-WAN, essa integração é expressa em uma plataforma que combina conectividade, segurança,

análises e gerenciamento centralizado. As políticas podem ser gerenciadas a partir de uma camada comum de orquestração, enquanto a solução incorpora capacidades de segurança diretamente nos pontos de acesso.

Na DDoS Mitigation, a diferença está em outro lugar: a capacidade de detectar e limpar tráfego malicioso dentro da rede antes que ele alcance a infraestrutura protegida.

Na ZTNA, o foco se desloca para a identidade e o contexto de cada acesso.

No Cloud Connect, para a privacidade e rastreabilidade do caminho que os dados percorrem.

Quando a IA acelera os negócios e também aumenta riscos, melhor proteção não significa necessariamente adicionar mais ferramentas. Significa reduzir as distâncias entre conexão, proteção, visibilidade e resposta. Em um ambiente onde os ataques podem ocorrer em segundos, a segurança não pode começar quando alguém descobre que há um problema. Ela precisa estar presente desde o momento em que a empresa se conecta. E fornecer as ferramentas para que possa continuar operando. Porque a resiliência é projetada antes do incidente e demonstrada depois.

8. Conclusões



A América Latina está passando por um paradoxo estrutural: suporta o maior volume de ataques cibernéticos do planeta e, ao mesmo tempo, tem a maior escassez de talentos em segurança do planeta.

Quando a ameaça cresce mais rápido do que uma região pode contratar alguém para detê-la, a resposta não pode ser comprar mais ferramentas para uma equipe inexistentes usarem, mas sim fazer com que a segurança esteja dentro da rede e que a operação seja delegada para aqueles que já gerenciam essa rede 24 horas por dia.

A Cirion opera a camada onde se decide o que entra e o que sai: uma plataforma pan-americana com mais

de 105.000 km de fibra própria, presença direta em 12 mercados com alcance em mais de 20 países, mais de 160 data centers interconectados, mitigação de negação de serviço no backbone e operação 24x7x365 NOC/SOC, tudo com neutralidade estrutural: não compete com o cliente, nem com sua nuvem, nem com seus clientes.

Como tudo isso impacta o negócio dos nossos clientes? Menor exposição, maior continuidade, políticas consistentes entre países, menos terceiros para auditoria, rastreabilidade comprovável até o regulador e capacidade de detectar dentro dos prazos legais de relatório. Resiliência não é mais uma despesa de TI, mas uma proteção direta de receita e reputação.

Fontes

- McKinsey, <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2025>
- M-Trends, <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026>
- CheckPoint, <https://blog.checkpoint.com/research/cyber-threats-spike-in-april-2026-as-ransomware-expands-and-attack-volumes-climb-after-short-lived-moderation/>
- WEF, <https://www.weforum.org/publications/global-cybersecurity-outlook-2026/>
- IBM, <https://www.ibm.com/downloads/documents/us-en/16dd90a741c46c2c>
- FortiGuard Labs, <https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2026/fortinet-2026-global-threat-landscape-report-reveals-surge-in-ai-enabled-cybercrime-increase-ransomware-victims-year-over-year>
- IDC, citado em <https://www.expereo.com/resources/reports/enterprise-horizons-2025>
- Gartner, citado em <https://www.paloaltonetworks.com/resources/research/gartner-2025-strategic-roadmap-sase-convergence>
- Cloudflare, <https://blog.cloudflare.com/ddos-threat-report-2026-h1>