

cirion

FORTINET

Cybersecurity:

Cybersecurity: When AI changes risk, security changes its archi-tecture



Table of Contents

1. Introduction: What AI Changed for the Company	3
AI and cybersecurity: “threatening” data	4
2. Security starts with connectivity	5
Advanced security in network architecture	5
Cirion SD-WAN Managed Service Features	6
3. Identity: raw material for attackers	7
Zero trust: the end of automatic trust	7
Identity: the numbers of risk	7
4. The acceleration of attacks and the limit of manual response	8
DDoS Mitigation: Preventing the problem from reaching the business	8
5. The Challenge of Managing an Increasingly Complex Security Architecture	9
SNOC commitments	9
6. Security as an operational capability	10
7. Differentiators: Why Cirion	11
8. Conclusions	12

1. Introduction: What AI Changed for the Company



Much is said about how AI evolves the way companies work, make decisions, and scale their operations. But, at the same time, another parallel transformation is happening: how organizations should protect their data and their systems.

The technology landscape has already been growing in complexity over the past few years. Applications are no longer concentrated in a single environment. Organizations combine owned servers, public clouds, edge, SaaS services, branch offices, remote workers, mobile devices, and thirdparty providers. Each new connection adds capacity to the business, but it also introduces a new relationship that must be managed and protected.

AI adds an additional ingredient to this complexity map. Because just as it allows automating tasks that previously required human intervention, accelerates decision-making and drives efficiency, it also accelerates the generation of attacks and expands the volume of attempts on increasingly distributed infrastructures.

The phenomenon is accelerating. According to the consulting firm McKinsey, 88% of organizations already use AI in at least one function, while 62% experiment with AI agents. About twothirds of organizations are still in pilot stages. Technology is advancing by leaps and bounds

while many times architectures are not yet adapted to support it.

At the same time, AI is shrouded in a paradox, especially when it comes to cybersecurity. On the one hand, it offers companies powerful tools to anticipate attacks, investigate anomalous behavior patterns, and accelerate defenses. But on the other, those same tools are available to attackers, who can automate tasks and reach scales never before known.

The race is being played out right now: against an opponent running at full speed, relying on structures where people are alerted, interpret it, determine its relevance, identify the affected asset, and decide what to do can be synonymous with being too late.

The M-Trends 2026 report, by Google Cloud and Mandiant, puts figures on this potential asymmetry: the median handover of an incident went from more than eight hours in 2022 to just 22 seconds in 2025. This, in simple terms, means that the time it takes for an attacker to move from one compromised system to another fell dramatically.

Added to this is the growth of regional exposure. Check Point registered an average of 3,561 weekly attacks per organization in April 2026 in Latin America (the most affected in the world), which represents a 19% year-on-year increase. And the World Economic Forum identified a critical cybersecurity talent gap that reaches 65% of organizations in Latin America and the Caribbean.

In other words, there are more threats, they arrive faster, and there are not necessarily more people to manage them. As the speed of business increases, the time available to detect, analyze, and respond to an incident is reduced.

In this context, adding security tools is no longer synonymous with being better protected. When each layer works independently, the organization also adds consoles, policies, integrations, and processes that someone must manage. Complexity can become, by itself, a new risk surface. The strategy must focus, then, on defining an architecture capable of connecting, protecting, observing, and responding consistently.

Continuous coverage, visibility, and the ability to respond in real time are now must-have capabilities. But the challenge is not just to detect faster. It also becomes imperative to do so without adding more complexity. Security must be integrated into the network architecture, operate consistently, and help the business continue to function even in the face of a threat.

This whitepaper analyzes how the cybersecurity scenario changes from the expansion of AI and increasingly distributed infrastructures. It addresses the link between connectivity and security, the critical role of identity, the acceleration of attacks and the limits of a response based exclusively on manual intervention, as well as the challenge of managing increasingly complex architectures. The objective is to move towards a conception of security as an operational capacity, integrated into the infrastructure and operation of the business.

AI and cybersecurity: “threatening” data

- **The attacker not only manages to breach the systems in 22 seconds: M-Trends detected that once it enters, it remains on average 14 days before being detected or the incident ends.**
- **Regulators in the region are setting detection deadlines well below that average: Chile requires early warning in 3 hours and complete reporting in 72 hours (Law 21,663), Colombia, 24 hours in the financial sector (External Circular 007 of 2018 of the Financial Superintendence) and Brazil two business days before the ANPD (National Data Protection Agency). Cirion allows companies to meet those deadlines.**
- **According to the World Economic Forum, 94% point to AI as the main driver of change and 87% place AI vulnerabilities as the fastest-growing risk.**
- **According to the Cost of a Data Breach Report 2026, prepared by IBM and the Ponemon Institute, 19% of malicious attacks are enabled by AI.**
- **FortiGuard Labs indicates that confirmed ransomware victims went from about 1,600 to 7,831 in one year: an increase of 389%, driven by AI-based cybercrime kits.**

2. Security starts with connectivity



Connectivity today represents more in companies than the transport that carries data from one place to another. In fact, when it is not well resolved, it constitutes a major obstacle to innovation and growth. The Enterprise Horizons 2025 report, by the market consulting firm IDC, detected that 94% of organizations find in their network the limit to advance in large-scale technological projects, particularly those involving AI. In addition, another 45% report specific latency problems.

When we talk about the security model, the first reference we have is the one that was built around the idea of “securing the perimeter.” But that perimeter has become increasingly difficult to define. Today, users, applications, and data can be found in different networks, clouds, branches, and locations. Securing the point of entry is far from enough. Traffic must be observed and protected throughout the architecture.

The network is consolidated as a strategic point of control. There can be no window of time between the moment of connection and the moment in which protection is activated. When security is part of the connectivity service, that gap disappears.

Advanced security in network architecture

That principle is behind Cirion’s Secure SD-WAN, which integrates advanced security directly into the network architecture. The solution optimizes traffic, prioritizes critical applications, and centrally manages security policies, while incorporating capabilities such as next-generation firewall, encryption, and protection of remote and branch sites. It also combines different types of access, including Cirion links and customer-provided access.

The advantage is operational. When connectivity and security are managed from an integrated architecture, the number of components that need to be managed separately is reduced and a more consistent view of what’s happening in the network is obtained.

The same logic appears in Cirion’s SASE proposal, which converges network and security functions into a single cloud-based service. In this model, Secure SD-WAN, ZTNA (zero trust network access, a concept we’ll expand on later), and other security capabilities work within a unified architecture, with consistent policies and centralized management.

Historically, cybersecurity managers had the challenge of finding mechanisms to protect the network. Today, however, work is being done to design a network that already incorporates protection from the very design.

Cirion SD-WAN Managed Service Features



Cirion serves 7x24x365 of the SD-WAN and security platforms it manages, with escalation to Level 2 and 3 specialists and management practices under ITIL v4.



Orchestrate management using FortiManager and analytics and reporting using FortiAnalyzer.



It does not deliver a product, but operates an architecture that allows records and events to be consulted, reports to be generated and dashboards to be adapted to operational needs, audits or regulatory requirements.



Connectivity and security data are no longer distributed among different tools without a com-mon reading and can become evidence to understand what is happening, accelerate root cause analysis and make decisions.



It is offered in three modalities: Connect, when security is concentrated in the hub; Protect, when each site needs its own protection; AI, when data leak prevention and AI-assisted functions are added.

3. Identity: raw material for attackers

Another transformation renders the old perimeter insufficient: identity. A user can connect from an office, from their home, from a mobile device, or from a third-party location. An application may be in a public cloud, and a third-party provider may need temporary access to a corporate re-source. In these scenarios, knowing that someone has a password is not sufficient proof.

Credentials are a central component of incidents affecting cloud environments. The problem goes far beyond a password being stolen: a valid credential is a legitimate gateway to resources that the attacker should not be able to use.

Zero trust: the end of automatic trust

Rather than assuming that an identity is trustworthy because it got in, each session should be evaluated according to its identity, context, device, and posture.

Zero trust is a security model that is based on the premise of never trusting per se that a user is valid, even if they are inside the network, but verifying every time. It assumes that threats may have already breached systems or that they may come from anywhere. Therefore, it does not automatically grant trust to anyone, regardless of whether it is the company's CEO connected from the central office. Access is not inherited: it is earned.

ZTNA is the implementation of this concept. In Cirion, it takes the name of User Identity. The permission is no longer a permanent property of a credential and is evaluated on a persession basis, reducing access to the minimum necessary. This is especially relevant when third parties are involved: contractors, suppliers, technology partners, and other collaborators may need access to certain resources without this meaning that they must join the corporate network with the same privileges as an employee.

Identity should be viewed as a security policy and not as a simple authentication mechanism. If a credential can be compromised, it is necessary to determine what additional conditions must be met to grant access. An integrated architecture is critical: SD-WAN can evolve towards broader security models and facilitate the transition to SASE/SSE architectures, always according to the feasibility and specific scope of each deployment.

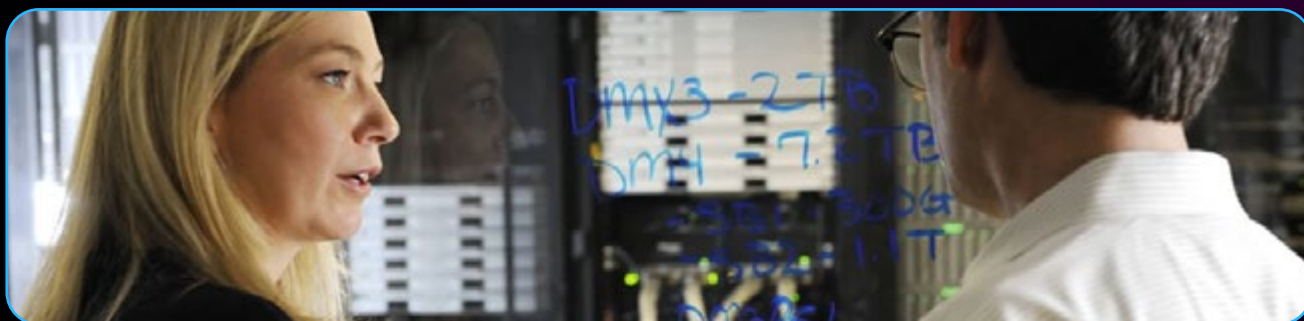
On this journey, it is not necessary to replace the existing architecture at once. It is possible to progressively shift control to where the risk lies: the user, the device, the application and the context of each connection. The trend, in this regard, is unstoppable: Gartner maintains that 70% of SD-WAN purchases will be part of a SASE platform from a single vendor in 2028, compared to 25% in 2025.

Identity: the risk numbers

- **35.4 million corporate accesses compromised available by 2025.**
- **67.65 billion brute force attempts during the year: about 185 million per day.**
- **79% year-over-year growth in available credential theft records.**

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

4. The acceleration of attacks and the limit of manual response



Detecting an attack is not the same as arriving in time to stop it. DDoS (distributed denial of service) attacks, which seek to crash a website, server, or digital service by flooding it with a massive amount of fake internet traffic until it becomes saturated, extremely slow, or crashes entirely, show that difference particularly clearly.

Cloudflare recorded a 31.4 Tbps attack during the first half of 2026 that lasted just 35 seconds. In the same period, 90.6% of networklayer attacks lasted less than ten minutes. When an incident can start and end at that speed, the limitations of models based solely on human reaction are more than evident.

If the organization must first detect the anomaly, confirm that it is an attack, open a ticket, and request action, it is increasingly likely that the response time will be longer than the duration of the incident itself. Protection must be close to where the traffic occurs. To use the example above: a 35-second attack is not mitigated with a team at the customer's edge or a call to the provider, but on the backbone, in an automated and always-on way, before the traffic reaches the business.

DDoS Mitigation: Preventing the problem from reaching the business

Cirion's DDoS Mitigation detects, filters, and cleans volumetric, protocol, and application traffic within your backbone before it reaches the customer's infrastructure. The service can operate on-demand or always-on, with assistance from the operations center.

The same principle applies to routing. Protection against prefix hijacking and malicious bypassing doesn't necessarily start with a firewall, but first, with the infrastructure itself that determines where traffic flows.

The implementation of RPKI on the AS3356 backbone that Cirion operates in Latin America adds that layer of protection in the routing. AS3356 identifies a Tier 1 backbone with a regional scope, connected to thousands of autonomous systems. This scale allows traffic security to be addressed from the network infrastructure itself.

The logic behind this: some threats can be effectively addressed only when they are addressed at the layer where they originate. In a distributed world, cybersecurity cannot be concentrated at the enterprise perimeter.

5. The challenge of managing an increasingly complex architecture



The attacker works at machine speed and the region, as mentioned, is not talented enough to cope with that scale. No one wins by buying more disjointed tools: defense is sustained by people, processes and continuous surveillance.

This is where the concept of operation as part of security appears. Historically, companies managed on the one hand the NOC (network operations center), which took care that the internet did not go down and that the servers worked fast, and on the other hand the SOC (security operations center), which looked for hackers, viruses and security breaches. Today, the SNOC breaks that barrier: in the real world, a system crash and a cyberattack are often the same problem seen from different angles.

If, in addition, this service is managed, the company has the possibility of transferring a large part of the day-to-day load (monitoring, change management, incident management, analytics, reporting and escalation) to specialized teams, without the organization losing control over its policies.

No alert should be left waiting for the next turn to be interpreted. The challenge is not only to incorporate more tools, but also to have continuous coverage and the ability to correlate information in real time. An operations center that monitors the network can detect signals before they become a ticket, because network and security are part of the same operation and not independent systems that must cross-reference records after the fact. In addition to this 24x7 surveillance, SNOC adds professional services that include evaluation, design, deployment and hardening of the infrastructure.

SNOC commitments

- Committed scaling times meet the increasingly demanding demands of regulators.
- Change management.
- Professional services: valuation, advanced configurations, hardening and ethical hacking (penetration testing and vulnerability analysis).
- Evidence for the regulator: Centralized analytics delivers standard or custom reporting and retains records to answer when it was detected, when it was contained, and when it was reported.

6. Security as operational capability



Digital transformation doesn't end with a certain technology. After the cloud came hybrid environments. Then, distributed work. Now, artificial intelligence and agents are incorporating new ways of interacting between users, applications, and data. Each stage puts the architecture to the test again.

That is why security needs to be designed with the capacity to evolve. The convergence between connectivity, security and operation modifies the objective of the architecture.

Old strategies, such as accumulating controls to cover every possible threat, are becoming obsolete. Today, it is necessary to define an architecture that allows you to reduce exposure, apply policies consistently, detect changes and respond quickly without transferring all the complexity to the internal team.

That shift is particularly relevant as companies incorporate more AI. Each new agent, application, or automated flow increases the speed of business, it's true, but it also increases the number of interactions that need to be controlled.

The architecture must accompany this growth without becoming a bottleneck. In this context, a smart grid needs much more than connectivity availability:

- **Visibility.**
- **Policies.**
- **Identity control.**
- **Inspection capacity.**
- **Response mechanisms.**
- **Operation.**

And, perhaps most importantly: cybersecurity architecture must be prepared to evolve along with the business.

7. Differentiators: **Why Cirion**



Cirion's network is the foundation on which these capabilities are integrated. The company has more than 105,000 kilometers of its own fiber in Latin America, a Tier 1 network, with a direct presence in 12 markets and network reach in more than 20 countries. This control over the infrastructure allows certain security capabilities to be applied closer to the origin of the traffic and not only at the customer's perimeter.

But, beyond that, the difference between a security strategy and a collection of tools is in the ability to sustain it over time. Cirion integrates connectivity, security and operation on top of this proprietary regional infrastructure and deploys capabilities that respond to different points of the architecture: Dedicated Internet with integrated security, IP VPN, Cloud Connect, Secure SD-WAN, User Identity (ZTNA), Firewall & UTM and DDoS Mitigation.

The model incorporates continuous operation. NOC/SOC 24x7x365 on the same network that transports the customer's traffic allows security not to be limited to the technology installed, but to be part of a permanent monitoring and management capacity.

In Secure SD-WAN, that integration is expressed in a platform that combines connectivity, security, analytics, and centralized management. Policies can be managed

from a common orchestration layer, while the solution embeds security capabilities directly at the access points.

In DDoS Mitigation, the differential lies elsewhere: the ability to detect and clean up malicious traffic within the network before it reaches the protected infrastructure.

At ZTNA, the focus shifts to the identity and context of each access.

In Cloud Connect, to the privacy and traceability of the path that the data travels.

When AI accelerates business and also accelerates risk, better protection doesn't necessarily mean adding more tools. It means reducing the distances between connection, protection, visibility, and response. In an environment where attacks can unfold in seconds, security can't start when someone discovers there's a problem. It has to be present from the moment the business connects. And provide the tools to be able to continue operating. Because resilience is designed before the incident and demonstrated afterward.

8. Conclusions



Latin America is experiencing a structural paradox: it supports the highest volume of cyberattacks on the planet and, at the same time, has the greatest shortage of security talent on the planet.

When the threat grows faster than a region can hire someone to stop it, the answer cannot be to buy more tools for non-existent equipment to use, but rather to make security live within the network and for the operation to be delegated to those who already manage that network 24 hours a day.

Cirion operates the layer where it is decided what goes in and what goes out: a Pan-American platform with

more than 105,000 km of its own fiber, direct presence in 12 markets with reach to more than 20 countries, more than 160 interconnected data centers, denial of service mitigation in the backbone network and 24x7x365 NOC/SOC operation, all with structural neutrality: it does not compete with the customer, nor with its cloud, nor with its customers.

How does all this impact our clients' business? Less exposure, greater continuity, consistent policies across countries, fewer third parties to audit, demonstrable traceability to the regulator, and ability to detect within legal reporting deadlines. Resilience is no longer an IT expense but a direct revenue and reputation protection.

Sources

- 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 en <https://www.expereo.com/resources/reports/enterprise-horizons-2025>
- Gartner, citado en <https://www.paloaltonetworks.com/resources/research/gartner-2025-strategic-roadmap-sase-convergence>
- Cloudflare, <https://blog.cloudflare.com/ddos-threat-report-2026-h1>