LINK11

Trends

2026

Web application security,
Resilience, Digital Sovereignty

2025: Cyberattacks reach new dimensions

The threat posed by DDoS attacks reached unprecedented levels in 2025. In the first half of the year, we observed a 225 percent increase in attacks on the Link11 network compared to the previous year. Not only did the number of attacks increase, but so did their complexity and scale.

The technical dimension is only part of this development, however. Politically motivated attacks, which are increasingly orchestrated and automated through the use of artificial intelligence, are targeting critical infrastructure – often against the backdrop of geopolitical tensions. The lines between state actors and cybercriminals are becoming increasingly blurred, while companies on the other side are struggling with growing attack surfaces, outdated technologies, and a lack of resilience.

Turning point in security policy

The German Federal Office for Information Security (BSI) emphasizes that protecting one's own attack surfaces is key to strengthening cybersecurity. The conclusion is clear: those who fail to strengthen their digital resilience will remain vulnerable in an environment that is more professional, networked, and dynamic than ever before.

For companies, administrations, and critical infrastructures in Europe, 2026 could mark a turning point in security policy. The threat situation is intensifying as cyberattacks become increasingly dynamic, AI-driven, and geopolitically charged. At the same time, regulatory pressure is growing, and with it the need for resilient, sovereign security architectures.

LINK11

Outlook for 2026

Web application security,
resilience, digital sovereignty

LINK11

Next-generation web application security

Web applications and APIs are now at the functional heart of modern business processes, from login mechanisms and payment processes to communication between internal and external systems. This is precisely why they are increasingly becoming the focus of attackers who not only exploit technical vulnerabilities but also manipulate business logic in a targeted manner. As a result, WAAP (Web Application and API Protection) is becoming a central component of digital resilience.

Unlike traditional WAFs (Web Application Firewalls), WAAP combines four protection disciplines – WAF, DDoS defense, bot management, and API protection – into one integrated platform. This consolidation reduces complexity, improves threat analysis, and provides effective protection against combined attacks.

Several other trends further shape the development of WAAP:

- **API-first security:** Complete visibility across all APIs through discovery, schema validation, and protection against business logic attacks, scraping, credential stuffing, and API-specific vulnerabilities.
- **Consolidation:** A unified, platform-based model correlates threats across all levels and simplifies management.
- **Positive security models:** Permitted behavior is clearly defined, which more effectively defends against zero-day attacks and new exploit patterns.
- **AI-powered behavioral analysis:** ML-based systems detect complex bot activity and anomalies in API traffic in real time.
- **DevSecOps integration:** Security policies are managed as code and automatically integrated into CI/CD processes.
- **Client-side security:** Protection against attacks in the browser, such as Magecart or manipulated third-party scripts, is becoming increasingly important.

WAAP is thus evolving into a comprehensive ecosystem that holistically protects web applications, APIs, and user interactions. In an age of increasing automation and attack complexity, it is becoming a central foundation of digital security.

"AI is both an accelerator and a challenge. We use AI-based technologies to detect attack patterns in real time, better understand anomalies, and continuously optimize our protection mechanisms. However, I believe it is crucial that we do not use AI as a 'black box'. Security needs explainability."

Marc Lamik
Chief Product Officer
Link11

"DDoS attacks will not only become larger in 2026, but also more precise. We are seeing a clear trend toward multi-vector and API-centric attacks that overwhelm traditional defense mechanisms. Only AI-powered, cloud-native protection systems that detect attacks in real time and respond autonomously can withstand this new dynamic."

Jag Bains
VP Solution Engineer
Link11

AI-driven DDoS dynamics

In 2026, DDoS attacks will continue to be among the most visible and unpredictable threats. While the volume and frequency of attacks continue to rise, the nature of the attacks themselves is changing fundamentally: AI-supported botnets operate autonomously, test defense mechanisms in real time, and change their patterns within seconds. Traditional, signature-based systems are easily overwhelmed by this.

Hybrid attacks on layers 3, 4, and 7 become the norm, hyperscale attacks via IoT botnets reach new records, and ransom DDoS campaigns put additional pressure on companies. At the same time, APIs are coming into sharper focus as attackers deliberately overload resource-intensive endpoints to cause maximum downtime with minimal effort.

Defense is increasingly shifting to always-on and cloud-first architectures: Global, cloud-native networks mitigate attacks directly at the edge, reduce latency, and protect central systems from overload.
Two developments will shape the future: First, AI will become the basis of modern DDoS mitigation, as autonomous systems detect attack patterns in real time and respond independently. Rule-based legacy solutions are rapidly losing their effectiveness. Second, DDoS attacks are increasingly being used as a diversionary tactic for more complex incidents such as data theft or malware installations. Security teams must therefore view DDoS as part of multi-stage attacks.

This will make DDoS protection a strategic security factor in 2026: Companies will need automated, predictive, and robust defense systems to combat these new threat vectors.

Focus on digital sovereignty

Europe is at a turning point in terms of security policy: the ability to control central digital infrastructures and security mechanisms itself will be a crucial component of modern resilience strategies in 2026. Digital sovereignty is more than a political promise – it is developing into an operational protection principle that determines a state's ability to act in an emergency.

Geopolitical pressure, economic dependencies, and extraterritorial legislation are forcing companies to fundamentally reassess their infrastructures. Where is data processed? Which security platforms control critical defense mechanisms? Which providers have access to sensitive systems in an emergency? Sovereign security architectures based on European infrastructure that offer complete control over data flows, key management, and AI-supported protection mechanisms are increasingly becoming a competitive advantage – especially for critical sectors such as energy, finance, healthcare, and public administration.

What digital sovereignty will mean in 2026, then, is the ability to fend off attacks independently, transparently, and in real time—even under geopolitical or regulatory pressure.

"Digital sovereignty means one thing above all else: preserving our freedom of choice in the digital space. To do this, we need to realistically assess risks and dependencies and take a much closer look at which technologies and providers we use. It's not about self-sufficiency, but rather the ability to remain capable of acting in a connected world – technically, legally, and strategically."

Prof. Dr. Dennis-Kenji Kipker
Research Director and Founder
of Cyberintelligence.institute

"NIS2, the KRITIS umbrella law, and the CRA are not here to annoy us, but to ensure the ability of our economy to act. Security is no longer a nice-to-have, but a public service."

Uwe Bergmann
managing director
Nethinks GmbH

Regulatory pressure is increasing

Parallel to the growing threat situation, governments are intensifying their regulatory requirements, which is having a noticeable impact on companies in all industries. 2026 will therefore be the year when compliance becomes a strategic success factor rather than an organizational obligation. Requirements such as NIS2 and DORA, alongside stricter reporting obligations, set clear expectations in terms of transparency, incident response, and secure software development.

In particular, the mandatory 72-hour notification requirement will change the operational reality of many organizations. It is no longer enough to detect attacks – they must also be clearly documented, evaluated, and reported using robust processes. At the same time, the responsibility of software providers is coming into sharper focus. Secure-by-design, SBOM creation, and securing software supply chains are required by regulation and are changing the way digital products are developed and operated. Companies must understand compliance as a continuous process that influences technological, organizational, and strategic decisions equally.

The security architecture of tomorrow

Organizations are at a turning point. The following measures form the basis for a resilient security architecture:

- **Anchor WAAP as an integral part of IT security.** Include API discovery, behavioral analysis, and positive security models.
- **Modernize DDoS protection.** Use autonomous, AI-powered technologies that defend against multi-vector attacks in real time.
- **Make sovereign infrastructure decisions.** Prioritize European hosting models and controlled security platforms.
- **Standardize compliance.** Use security platforms that provide continuous transparency about risks and requirements.
- **Anchor a resilience program at the C-level.** Cybersecurity in 2026 is no longer a technical issue, but part of corporate strategy.

Conclusion

2026 will be a test of Europe's digital sovereignty. In the face of AI-driven cyberattacks and rising geopolitical risks, companies must regain control of their infrastructure. Security should no longer be a cost factor, but rather the strategic foundation for innovation and growth. Those who now focus on dynamic, integrated security architectures, autonomous defense, and sovereign technology will create the transparency required by regulators and gain decisive entrepreneurial leeway for sustainable success.

Contact

Michael Scheffler
Vice President Sales

+49 69 58004926-306
m.scheffler@link11.com

link11.com

linkedin.com


LINK11