



FACT SHEET

BITKOM ECONOMIC SECURITY 2025

**How to tackle around 50%
of the most critical
cyber threats with a digitally
sovereign platform**



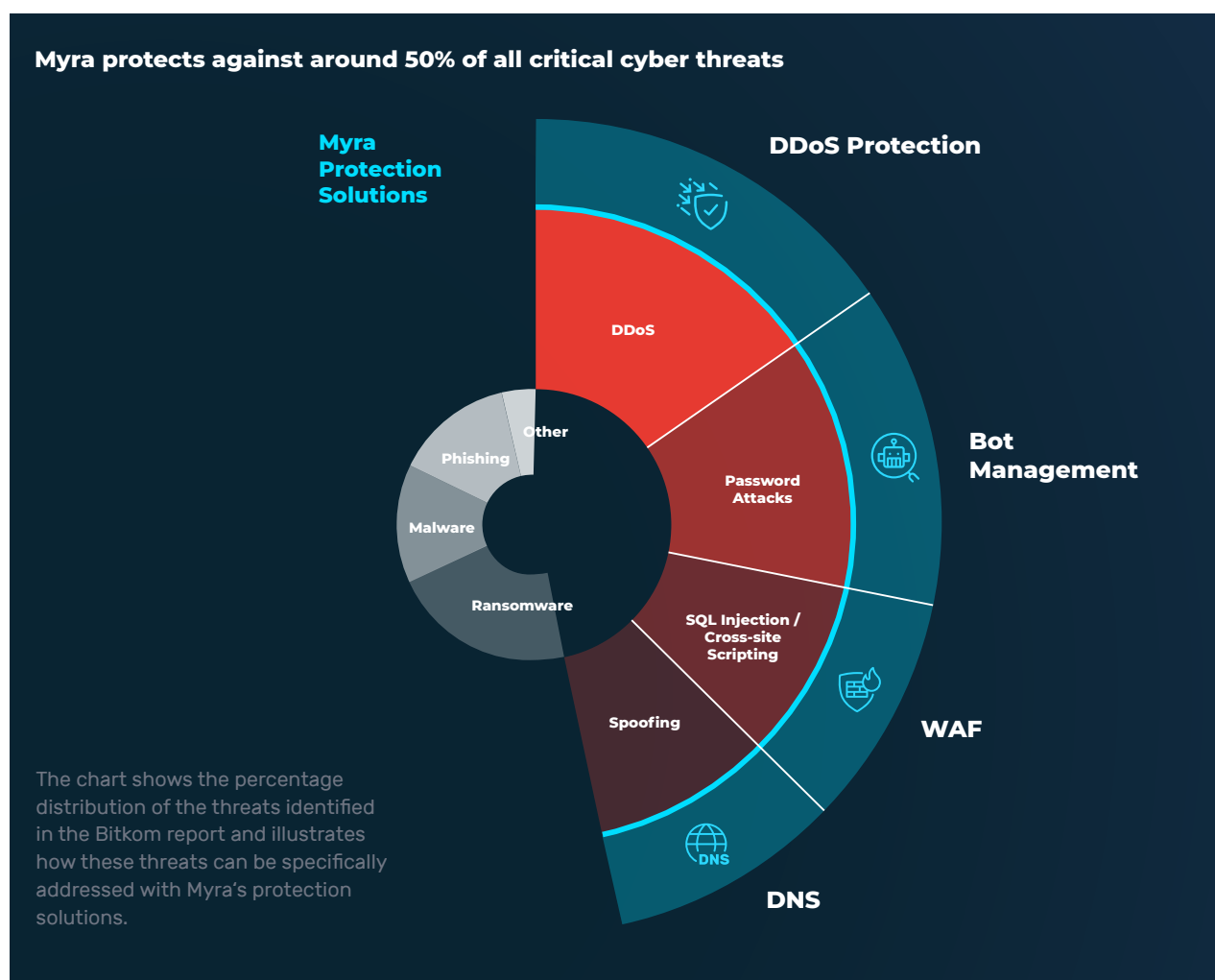
How to tackle around 50% of the most critical cyber threats with a digitally sovereign platform

IT managers today face a wide range of cyber threats and often have to rely on a collection of specialized individual solutions to defend against these dangers – but this increases the complexity of the tech stack, slows down deployment, and makes the defense system as a whole prone to errors. Holistically designed platforms that address many risks are therefore becoming increasingly important.

The 2025 Economic Security Report published by the German digital association Bitkom shows which types of attacks cause damage particularly frequently: ransomware (34%), DDoS attacks (25%), malware infections (24%), phishing (22%), attacks on passwords (21%), SQL injection and cross-site scripting (15%), and spoofing (15%). In addition, there are newer threats such as deepfakes (4%) and robo calls (3%).

Myra counters this threat with a highly certified, digitally sovereign platform that protects web applications, online portals, APIs, and IT infrastructures from malicious attacks from the internet, thereby addressing most of the core threats identified in the Bitkom study. Operators of critical infrastructures, financial institutions, government agencies, and other highly regulated organizations in particular benefit from this combination of efficient protection technology, regulatory compliance, and reduced operating costs.

This paper provides a concise overview of the key cyber threats that can be effectively combated with Myra's integrated solutions – and how Myra can help you reduce the complexity of your security stack in the long term.



Myra Security – protection against key threats

Myra's solutions safeguard your business against the most critical cyber threats – delivering efficiency, performance, and trusted German engineering.



Myra DDoS Protection provides comprehensive defense for web applications, online portals, and APIs, as well as the underlying network and IT infrastructure. It protects against the full spectrum of DDoS attacks – from complex application-layer assaults to large-scale volumetric attacks at the network level. Suspicious traffic is efficiently filtered by Myra, while legitimate requests continue to perform seamlessly. This ensures that your digital business operations remain available, even under heavy attack.



Myra Bot Management accurately identifies and categorizes automated traffic, enabling the efficient blocking of malicious bots. With precise bot detection and control, it protects applications and APIs from abuse such as credential stuffing, brute-force attacks, account takeovers, and click fraud – while legitimate users and useful bots benefit from noticeably improved performance. At the same time, infrastructure and operational costs are reduced, as unwanted and harmful traffic is filtered out at an early stage.



Myra WAF protects web applications and APIs from attacks that exploit vulnerabilities to infiltrate systems or manipulate data. The WAF inspects incoming requests before they reach the customer's server infrastructure, blocking malicious traffic based on proven rule sets (including OWASP Top 10, Log4J, SQL injection, and cross-site scripting). It can be seamlessly integrated into existing IT environments – regardless of where applications are hosted.



Myra DNS ensures that domain name resolution – a critical foundation of digital services – functions reliably at all times. With hardened servers, DNSSEC support, and a globally distributed, fully redundant anycast network, domains remain available and high-performing even during attacks such as DDoS, spoofing, or DNS hijacking.



Additional advantages of the platform: comprehensive compliance and digital sovereignty

Beyond mitigating concrete attacks, Myra's Security-as-a-Service platform provides a consistent foundation for compliance and digital sovereignty. All services are operated in German or European high-security data centers, subject to strict data protection standards, and support regulatory compliance with frameworks such as NIS-2, DORA, and the GDPR. An intuitive management interface enables CISOs and IT leaders to centrally control protection services, while extensive certifications based on established standards demonstrate adherence to stringent security requirements.

Through automation and configuration via Infrastructure as Code and APIs, Myra integrates seamlessly into existing processes. Role-based access control (RBAC) ensures clearly defined responsibilities, while SLAs offering service availability of up to 99.999 % highlight the platform's focus on resilience for business-critical applications.

Use Myra as a strategic platform that unites cyber defense, compliance, and digital sovereignty within a unified European security architecture.

Made in Germany



Myra protects what matters. In the digital world.

Would you like to learn more about how our sovereign solutions can strengthen your digital independence, reduce costs, and protect your web applications against malicious attacks? Our experts will be happy to provide individual guidance and develop a tailored solution for your organization. Schedule a non-binding consultation today.

**Cyberattacks are costly.
A conversation with us is not.**

Myra Security GmbH



+49 89 414141 - 345



www.myrasecurity.com



info@myrasecurity.com