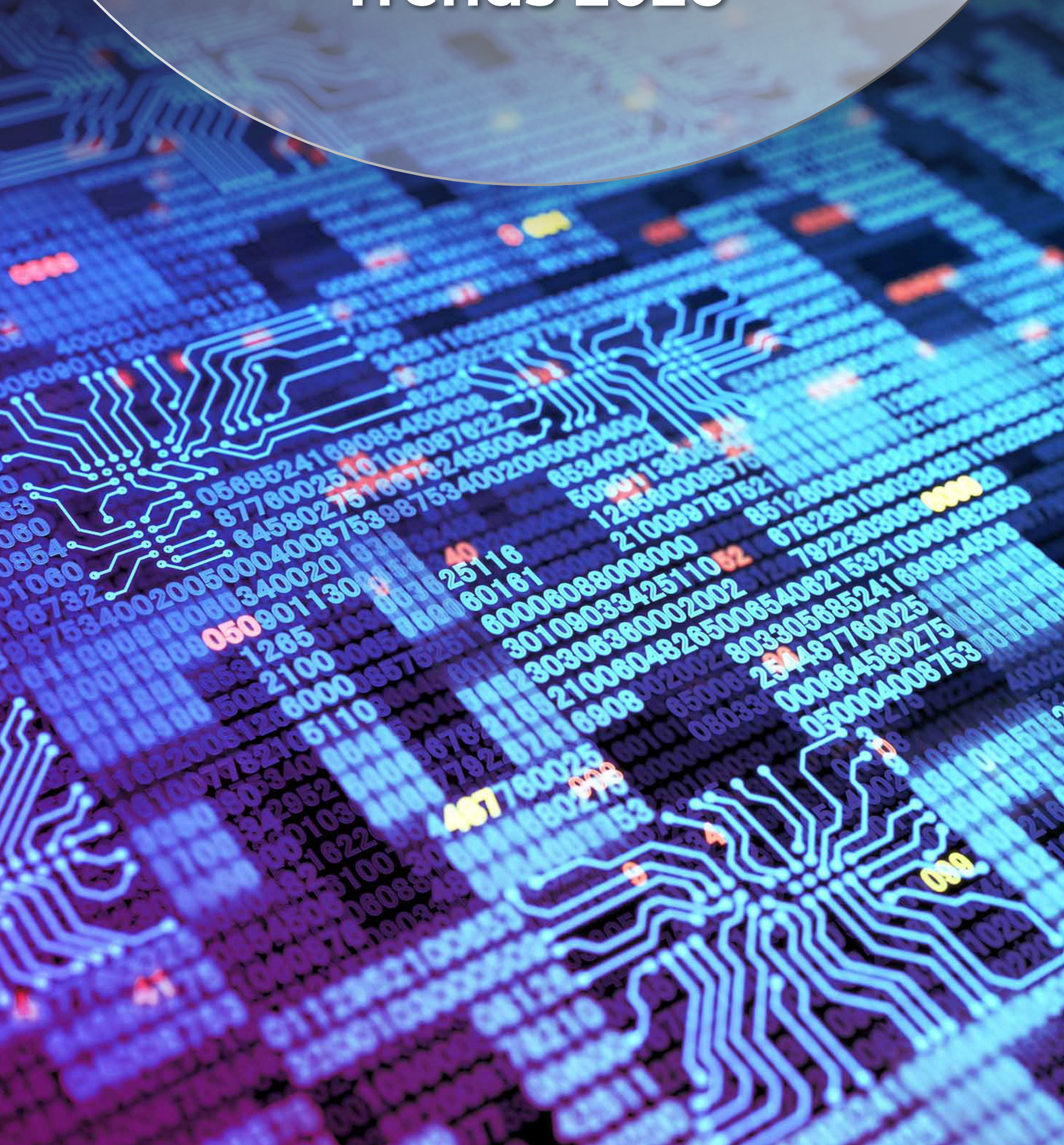
devoteam

Cybersecurity Trends 2026



About Devoteam

Devoteam is a premium consultancy firm driving digital business and transformation through innovative technology.

Tech native for over 30 years, we deliver lasting results in Cloud, Data, Cyber and AI for industries and public institutions across EMEA.

At Devoteam, tech entrepreneurship is at the core of our values, fostering our spirit as a learning company. Within this culture, we attract and train top professionals, creating high talent density across our 11,000 specialists. Strong partnerships have always been central to our DNA, which is why we collaborate closely with both well-known tech giants and emerging innovative startups. This ecosystem enables us to provide long-lasting solutions that help clients lead in their industries.

AI-driven tech consulting

Cybersecurity Trends 2026

Content

Introduction

The year 2026 promises to be a milestone in the evolution of cybersecurity, driven by an ever-accelerating digital transformation and a constantly shifting threat landscape. The convergence of artificial intelligence, quantum computing, and global connectivity is creating new opportunities but also unprecedented vulnerabilities. Organisations and governments face the challenge of protecting critical infrastructures, sensitive data, and highly interconnected value chains. In this context, cybersecurity is establishing itself as a strategic pillar of competitiveness and trust, making it essential to anticipate emerging trends to face the risks of the digital future with efficiency, ethics, and foresight.

Top 10 Trends

Trend 1

AI Everywhere: Security at Machine Speed

AI is now embedded in almost every layer of security: anomaly detection, SOC support, automated response, and analysis of large data volumes. At the same time, attackers are using AI to create more convincing fraud campaigns, deepfakes, and faster intrusions. The trend is not merely to use AI in security, but to govern and secure AI itself, including models, data, and decisions as a new critical organisational asset.

Trend 2

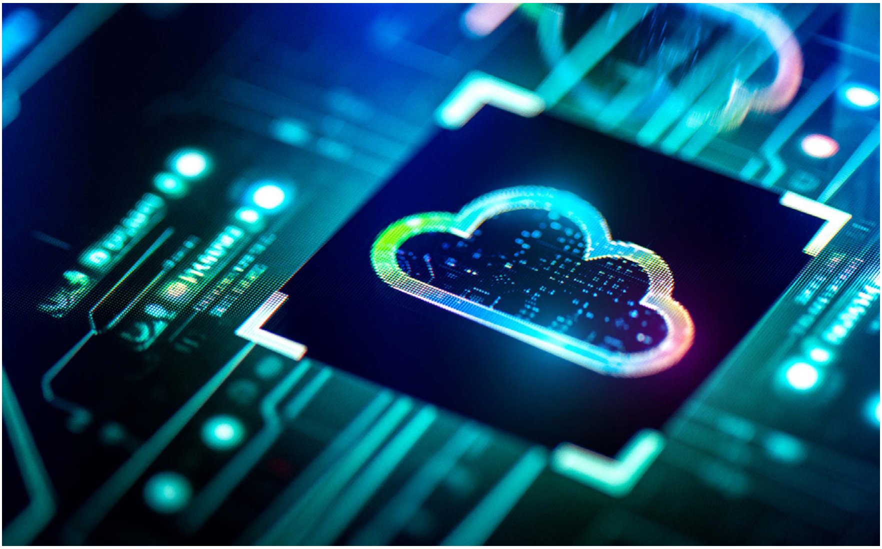
The Beginning of the Transition to Post-Quantum Cryptography

The risk of harvesting encrypted data to decrypt it in the future is pushing organisations to prepare for the quantum era before it fully arrives. In 2026, momentum grows around encryption inventorying, identifying long-term sensitive systems, and defining roadmaps for adopting post-quantum algorithms. The key change is to treat cryptography as something dynamic and manageable, not as a one-off decision to be forgotten.

Trend 3

Operational Zero Trust in Hybrid and Multicloud Environments

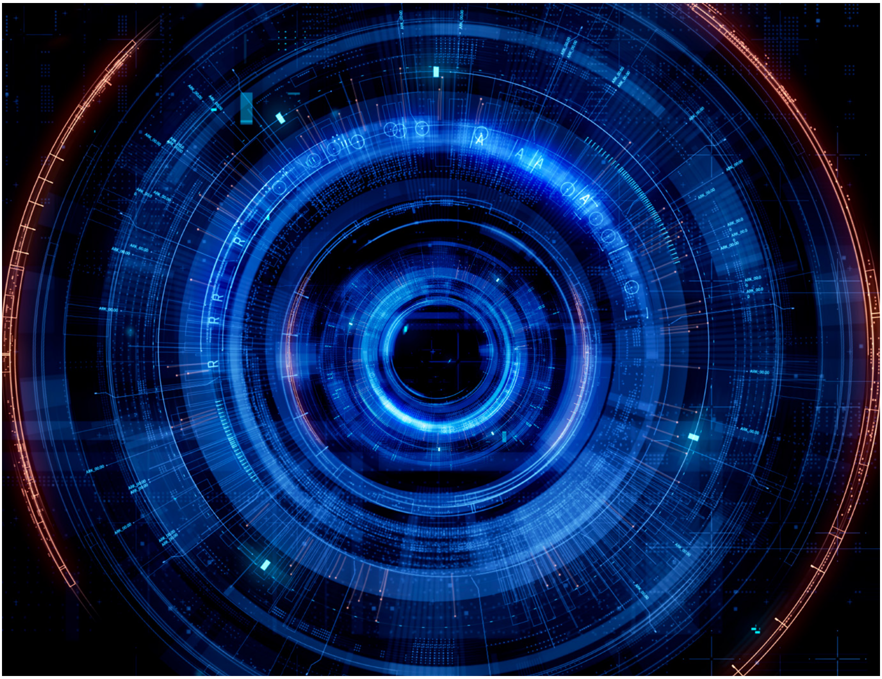
Zero Trust is no longer an abstract concept, it becomes a visible transformation programme shaping how access is designed and controlled. In 2026, networks and applications are segmented according to critical systems, traditional VPNs with broad access are replaced by identity, context, and device-based access models, and access policies become consistent across datacentres, cloud, and SaaS. The result: more contained environments, reduced incident impact, and access decisions aligned with business workflows.



Trend 4

CTEM as the Common Language of Risk Exposure

Continuous Threat Exposure Management (CTEM) replaces sporadic vulnerability reports with a live view of risk. Organisations begin to integrate vulnerabilities, configurations, access, third parties, and processes into a single exposure matrix. The 2026 trend is to use CTEM not merely as a technical tool, but as a shared language between security, risk, and business teams to decide what to fix, when, and why.



Trend 5

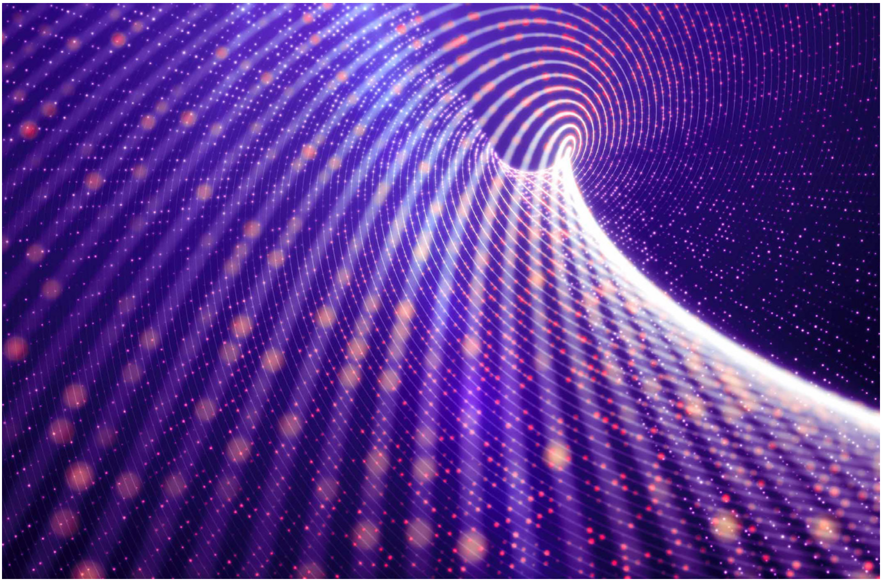
Identity and Behaviour as the Main Control Plane

Identity is no longer just about logging in, it becomes the plane where most security controls are applied. In 2026, the shift is towards treating identities, sessions, and behaviours as a cross-cutting operating system: everything that matters, including applications, data, and cloud, is governed by identity policies and real usage analysis. The novelty lies not in phishing itself, but in how identity is managed with metrics, continuous privilege review, and anomaly detection as central risk indicators.

Trend 6

Cloud, Data, and the Software Supply Chain as a Unified Attack Surface

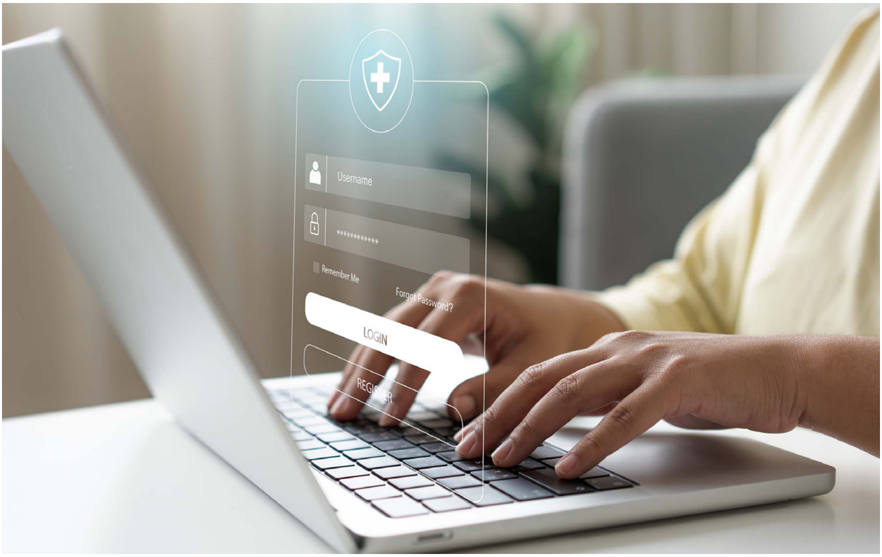
Cloud, data, and the software supply chain cease to be separate topics. Cloud protection platforms, software bills of materials (SBOMs), and data security posture management tools converge into a single view of the digital attack surface. The 2026 trend is to regard code, infrastructure, and data as parts of the same problem: knowing exactly what runs where, who developed it, what it depends on, and what sensitive information is at stake.



Trend 7

Industrialisation of Cybercrime, Ransomware-as-a-Service, and the Democratisation of the Target

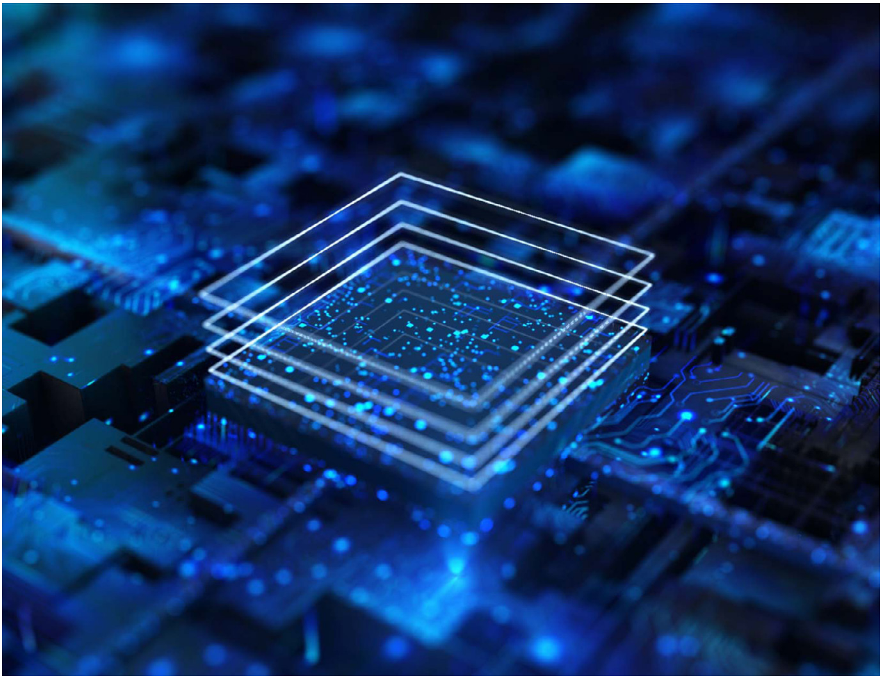
Digital crime is organised into a value chain: some sell access, others develop malware, manage extortion, launder funds, or provide ransomware-as-a-service as a ready-to-use product. This industrialisation drastically reduces costs and lowers the barrier to entry for attackers. In 2026, the key implication is that more organisations, including smaller ones, become economically attractive targets, as the marginal effort to attack them is very low. The response can no longer rely on the notion of being “too small to matter”.



Trend 8

High-Impact Regulation and Risk Expressed in Euros

NIS2, DORA, and the European AI framework consolidate a new level of cyber resilience requirements. The trend is not just more regulation, but greater scrutiny over real control evidence and increased pressure to translate cyber risk into economic impact. Risk quantification models linking technical failures to financial losses gain traction as decision-making tools, placing security on par with other strategic risks.



Trend 9

IT/OT Convergence and Digital Sovereignty as Architectural Drivers

Industrial systems, healthcare, energy, and transport are becoming increasingly connected to IP networks and the cloud, bringing technology decisions closer to physical operations. As IT and OT begin sharing infrastructures, vendors, and cloud services, choices such as data residency, applicable jurisdiction, and trusted manufacturers are no longer technical details but structural decisions on digital sovereignty. Crucially, this convergence dramatically expands the attack surface. Architects must fundamentally address the security of operational technology (OT) systems, which were often air-gapped or designed without robust security protocols, by implementing deep-seated security controls, zero-trust models, and continuous monitoring from the ground up. In 2026, architectures and technology partnerships are designed with not only performance and cost in mind, but also resilience against cyber-physical threats, strategic dependencies and the regulatory and geopolitical contexts in which organisations operate.

Trend 10

People-Centred Security and Digital Sustainability

Most significant incidents still depend on human decisions, and security teams continue to face high levels of stress and fatigue. In 2026, a people-centred approach to security gains strength: processes, interfaces, and incentives are designed to reduce human error and promote safe everyday behaviours. At the same time, digital sustainability translates into fewer redundant data, simpler systems, and well-managed life cycles, reducing risk, cost, and complexity simultaneously.

Conclusion

In 2026, cybersecurity is solidified as an essential strategic element for organisational sustainability and competitiveness. In a context marked by advanced technology integration and the rise of digital threats, protecting data, infrastructures, and operations is no longer optional, it is a management imperative. Digital trust will become the foundation of business and institutional relationships, requiring a proactive, collaborative, and continuous approach to ensure resilience and secure innovation.

Bibliography

Gartner: The CIO's 2026 Cybersecurity Playbook
https://nationalcioreview.com/articles-insights/live-from-gartner-the-cios-2026-cybersecurity-playbook/

Top Strategic Technology Trends for 2026
https://www.gartner.com/en/articles/top-technology-trends-2026

Forrester forecasts agentic AI breaches & quantum spending surge by 2026
https://itbrief.asia/story/forrester-forecasts-agentic-ai-breaches-quantum-spending-surge-by-2026

ENISA Threat Landscape (ETL) 2025 report
https://www.iisf.ie/ENISA-Threat-Landscape-2025-report

CrowdStrike 2025 Ransomware Report: AI Attacks Are Outpacing Defenses
https://www.crowdstrike.com/en-us/press-releases/ransomware-report-ai-attacks-outpacing-defenses/

Cybersecurity in 2026: A Strategic Road Map for US Businesses
https://www.forvismazars.us/forsights/2025/10/cybersecurity-in-2026-a-strategic-road-map-for-us-businesses

NIST Post-Quantum Cryptography Standardization
https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization

2025 Identity Security Landscape Report
https://www.cyberark.com/threat-landscape

A Guide to CTEM
https://seemplicity.io/remops-glossary/ctem-continuous-threat-exposure-management/

Forrester’s 2026 Cybersecurity and Risk Predictions
https://www.forrester.com/blogs/predictions-2026-cybersecurity-and-risk/

Google Cloud – Cybersecurity Forecast 2026
https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2026

AWS – Post-Quantum Cryptography Migration Plan
https://aws.amazon.com/pt/blogs/security/aws-post-quantum-cryptography-migration-plan/

BeyondTrust – Top Cybersecurity Predictions for 2026
https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions

Center for Internet Security – CIS Cyber Predictions 2026
https://www.cisecurity.org/insights/blog/7-cis-experts-2026-cybersecurity-predictions

Questions?

Get in touch!

Where are you on your Cybersecurity Journey?

Let’s find out. We’re here to help you.

devoteam

AI-driven tech consulting

devoteam.ai