AQ SECURE

CYBERSECURITY FOR SMEs

IN THE AGE OF AI

Whitepaper

An executive guide for CEOs, CIOs and CISOs of small and medium-sized enterprises for building a resilient security posture and safely adopting generative and agentic AI.

AQ SECURE GmbH
info@aqsecure.de
www.aqsecure.de

Table of Contents

Executive Summary **3**

PART I — THE SME CYBERSECURITY REALITY

1. Why Cybersecurity Is No Longer Optional for SMEs **4**

2. The Cybersecurity Challenges SMEs Face Today **5**

3. Why Classical IT Security Approaches Fall Short **6**

4. The Illusion of Complete Cloud Security **7**

5. Phishing: The Real-World Threat in SMEs **8**

PART II — THE MODERN SME SECURITY PLATFORM

6. An Integrated Platform, Not Isolated Tools **9**

6.1 Endpoint Protection (EDR / XDR) 10

6.2 Mobile Security 10

6.3 Email Security with Integrated DLP 11

6.4 Browser Security: The New Perimeter 11

6.5 Zero Trust Network Access (ZTNA) 12

6.6 Cloud Access Security Broker (CASB) 12

6.7 Firewall and SD-WAN 13

6.8 Data Security Posture Management (DSPM) 13

PART III — SECURING GENERATIVE AND AGENTIC AI

7. The AI Risk Landscape and Shadow AI **14**

8. Eight Capabilities for AI-Specific Security **15**

PART IV — FROM STRATEGY TO ACTION

9. The 90-Day Executive Action Plan **16**

10. Cybersecurity as the Foundation for Cyber Insurance **17**

Partner with AQ SECURE **18**

Executive Summary

Cybersecurity has moved from being a concern reserved for large enterprises to becoming an existential issue for small and medium-sized enterprises. Today, **43 % of all cyberattacks target SMEs** – yet only **14 % are adequately prepared** to defend themselves. At the same time, generative and agentic AI is reshaping how every business operates, creating both unprecedented productivity opportunities and an entirely new category of risk.

For SME leaders, three numbers define today's reality: 43 % of cyberattacks target SMEs. 77 % of employees paste company data into public AI tools – 82 % through personal accounts that bypass corporate controls. In Germany, **87 % of companies** were hit by data theft, espionage or sabotage in 2025, with damages reaching **€289 billion** – €202 billion of that from cyberattacks alone.

Many SMEs still rely on classical defenses – antivirus, perimeter firewalls, basic VPNs – that were designed for the threat landscape of a decade ago. Meanwhile, attackers have automated and industrialized their methods, regulators have raised the bar through the **GDPR, NIS2, DORA and the EU AI Act**, and employees have already started using AI tools that the IT team has never approved or even seen. The **GDPR** can fine serious infringements **up to €20 million or 4 % of global annual turnover**; the **NIS2 Directive** now adds personal accountability for the management body and exposes essential entities to fines of **up to €10 million or 2 %**. The good news for SMEs: NIS2 explicitly requires controls to be **"appropriate and proportionate"** to the size and risk exposure of the entity – not Fortune 500-grade for everyone.

What this whitepaper delivers

- **Part I** – a clear, business-language picture of the SME cybersecurity reality and why classical approaches no longer suffice.
- **Part II** – the eight foundational security capabilities every modern SME needs, organized as one integrated platform rather than disconnected tools.
- **Part III** – the additional eight capabilities required to safely adopt generative and agentic AI.
- **Part IV** – a 90-day executive action plan, the cyber-insurance angle, and a clear path to partnership.

The bottom line: modern cybersecurity is not a cost center, and neither is AI security. Done right, both become the foundation that lets your organization adopt new technology faster than competitors – with confidence rather than fear.

1. Why Cybersecurity Is No Longer Optional for SMEs

Cyberattacks were once associated primarily with large enterprises – the Fortune 500s with valuable data and deep pockets. That assumption is dangerously outdated. According to recent industry studies, **43 % of all cyberattacks now target small and medium-sized enterprises**, and only **14 % of SMEs are adequately prepared** to defend themselves. This combination of increasing exposure and limited preparedness is exactly what makes SMEs the most attractive target on the threat map.

Cybercriminals have **industrialized their operations**. They no longer rely solely on highly targeted, custom-built attacks. Instead, they use automated network scanning, mass-distributed phishing campaigns, and **Ransomware-as-a-Service** offerings that allow even unsophisticated attackers to launch business-disrupting attacks. These automated campaigns make no distinction between a Fortune 500 and a 50-person company – in fact, the smaller company is often a softer target.

Why SMEs are particularly exposed

- **Limited resources** – SMEs rarely have the budget, time or specialist headcount that larger enterprises invest in cybersecurity.
- **False sense of security** – relying on classical antivirus alone covers only a fraction of today's threat landscape.
- **The "we're too small to be a target" myth** – attackers value any data they can monetize: customer records, financials, IP, or simply your network as a stepping stone into larger partners.
- **The AI factor** – the rapid integration of generative and agentic AI into business processes adds new risk classes that go beyond traditional cybersecurity.

The consequences of a successful attack on an SME can be devastating: financial losses, customer-data breaches, reputational damage, and in the worst case complete operational shutdown. **Cybersecurity is no longer optional – it is a precondition for staying in business.** And the threat is escalating quickly: in Germany, **28 % of companies** now report that they have been targeted by foreign intelligence services – up from just 7 % in 2023, a **fourfold increase in two years** (Bitkom 2025). State-backed actors no longer go after large enterprises only; they specifically target the SME suppliers, technology firms and research organizations that sit deep in supply chains.

2. The Cybersecurity Challenges SMEs Face Today

SMEs face a fundamental asymmetry. Their **digital attack surface keeps expanding** – through cloud services, AI tools, remote work, and an ever-growing number of SaaS applications. At the same time, the **security resources available to them remain limited**. This gap is exactly what makes SMEs vulnerable, and what attackers exploit.

The challenges that recur in nearly every SME

- **Few or no dedicated security professionals:** IT is often handled "on the side" by a generalist or by management itself. Cybersecurity becomes ad-hoc rather than strategic, leading to knowledge gaps, reactive postures and overlooked risks.
- **Decentralized work:** Remote and hybrid work have dissolved the traditional network perimeter. Employees access company data from home networks, public Wi-Fi, and personal devices (BYOD), multiplying the attack vectors.
- **Sophisticated, hard-to-detect threats:** Modern phishing, malicious downloads disguised as legitimate software, and manipulated cloud logins are nearly impossible for untrained users to spot. SMEs typically lack the advanced detection systems and threat-intelligence platforms that larger enterprises rely on.
- **Burdensome updates and policy compliance:** Continuous patching, user-rights administration, and policy enforcement quickly become unmanageable without central control and automation – tying up the few resources SMEs do have.
- **Limited visibility and incident response:** Many SMEs detect attacks too late, or respond in an uncoordinated way. Without clear incident-response playbooks, sufficient logging, and network visibility, the time to contain a breach grows – and so does the damage. Under **NIS2 Article 23**, in-scope entities now have only **24 hours** to issue a first warning to authorities, **72 hours** for the formal notification, and **one month** for the final report.
- **New executive accountability: NIS2 Article 20** makes the management body – CEO, board, C-suite – directly accountable for approving and overseeing cybersecurity measures, and personally liable for non-compliance. Senior leaders must also undergo cybersecurity training. "We delegated this to IT" is no longer a defensible position.

This combination of valuable data on one side and limited defensive capability on the other makes SMEs particularly attractive to attackers. The good news: German companies are responding – the share of IT budget devoted to security has risen to **18 %** in 2025, up from just 9 % in 2022 (Bitkom). Closing the gap does not require building a Fortune 500 security organization – it requires the **right priorities, the right platform and the right partner**.

3. Why Classical IT Security Approaches Fall Short

Most SME security architectures grew organically over years and are based on technologies designed for **yesterday's threat landscape**: classical perimeter firewalls, traditional VPNs, and endpoint antivirus. On paper, this looks reasonable. In today's reality, it leaves serious gaps.

Where traditional approaches break down

- **Insufficient phishing detection:** Classical solutions rely on signatures of **known** threats. They struggle with the dynamic, AI-generated phishing variants that target employees today, and they rarely inspect content in real time or in context.
- **VPNs as a wide-open door:** Once a user authenticates to a traditional VPN, they often gain broad access to the entire internal network. A single compromised account becomes a launching pad for the attacker to move laterally to data and systems they should never have reached.
- **No migration plan to modern models:** Cloud and remote work are now everyday reality, but many SMEs still lack a roadmap to **Zero Trust** or **Secure Access Service Edge (SASE)** – the architectures designed for a world without a fixed perimeter.
- **Overestimating cloud security:** Moving to the cloud reduces hardware costs, but security responsibility doesn't move with it. Many SMEs assume the cloud provider "handles security," when in fact most cloud breaches are caused by **customer-side misconfiguration**.
- **Manual processes, no transparency:** Without automation, central policy management and full network visibility, security teams can't detect issues fast, can't respond consistently, and can't prove compliance to auditors – exactly the kind of evidence regulators now demand under **NIS2 Article 21(2)(f)** ("policies and procedures to assess the effectiveness of cybersecurity risk-management measures").

The implication for executives: continuing to layer point products onto an outdated foundation is the most expensive form of security – and increasingly, a regulatory liability. NIS2 fines reach **€10 million or 2 % of global turnover** for essential entities, and **€7 million or 1.4 %** for important entities. The right move is to consolidate onto a modern, integrated platform that delivers both protection and audit-ready evidence – exactly the approach we describe in Part II.

4. The Illusion of Complete Cloud Security

One of the most dangerous misconceptions in modern IT is the assumption that **moving to the cloud automatically means "the provider handles security."** It does not. Cloud security is governed by a **Shared Responsibility Model**, in which both the cloud provider and the customer have specific obligations.

What the cloud provider handles

The provider secures the **"cloud itself"** – the physical and platform layer:

- **Physical security** – data centers, servers, network hardware, protection from physical threats
- **Platform security** – patching of operating systems, virtualization layers and provider-managed services
- **Foundational protection** – baseline firewalls, intrusion detection, DDoS mitigation at infrastructure level

What you are still responsible for

The customer secures **"what's in the cloud"** – data, applications, identities and configurations:

- **Data:** Encryption at rest and in transit, strict access controls, data residency and compliance.
- **Applications:** Patch management, secure configuration, API protection, security testing.
- **Access:** Identity and access management, multi-factor authentication, least-privilege principles.
- **Configuration:** Network segmentation, firewall rules, storage configuration. **Misconfiguration is the single most common cause of cloud breaches.**

Most cloud security incidents do not come from weaknesses in the cloud itself, but from **gaps the customer leaves open** – misconfigured services, weak access controls, and missing protections at the browser, email and mobile-device layers, which sit outside the cloud provider's scope. Treat the cloud as you would any other operating environment: assume responsibility, not magic.

5. Phishing: The Real-World Threat in SMEs

Phishing remains the **single most common entry point** for cyberattacks against SMEs – and the one that most consistently succeeds. It works not by exploiting a technical flaw, but by exploiting **trust, urgency and human attention**. With AI now in attackers' hands, phishing is more convincing than ever: perfect grammar, accurate context, and personalized references that look indistinguishable from a real internal email.

The phishing scenarios SMEs encounter most often

- **CEO Fraud / Whaling:** An email apparently from the CEO instructs the finance team to urgently transfer funds for a "confidential acquisition" or new supplier. The signature, tone and timing all look authentic. The money goes to the attacker.
- **Credential Harvesting:** A message – seemingly from Microsoft, the bank, or internal IT – warns of "suspicious activity" or a required password reset. The link leads to a perfectly cloned login page. The captured credentials are then reused everywhere.
- **Invoice Phishing (BEC / Malware):** A realistic-looking invoice from a known service provider arrives with a PDF or link. Clicking either drops malware on the system (often the first step toward ransomware) or redirects payment to the attacker (Business Email Compromise).
- **Spear Phishing:** Highly targeted attacks built on LinkedIn research, public org charts and social media. The attacker knows your project names, your colleagues, your suppliers – and uses this to craft a request the target has every reason to trust.
- **Quishing (QR-code Phishing):** Fake QR codes on flyers, in emails or on documents redirect smartphones to malicious sites. Users instinctively trust QR codes – which is exactly why this technique works.

What every one of these has in common is that **the technology is just the delivery mechanism – the actual target is the human**. Defending against phishing therefore requires a combination of **strong technical controls** (email security with link analysis, attachment sandboxing, browser-based detection) and **continuous awareness training**. Either alone is not enough; together, they cut successful phishing by an order of magnitude.

6. An Integrated Platform, Not Isolated Tools

Many SMEs still rely on a patchwork of point products: an antivirus on the endpoint, a VPN for remote access, a separate email gateway, a different vendor for the firewall. Each may work in isolation – but together they are slow to operate, expensive to maintain, and **blind to attacks that cross between them**.

The modern answer is a **unified cybersecurity platform** that delivers visibility, control and automation through a single management plane. For SMEs in particular, this is transformational: the platform compensates for the lack of a large security team, enforces consistent policies across every channel, and provides the audit-ready evidence regulators and insurers now expect.

What an integrated platform delivers

- **Single Pane of Glass** – one console for endpoints, mobile, email, web, cloud, identity, and AI usage.
- **Policy-based management with RBAC** – role-based control across multiple sites and user groups.
- **AI-driven risk correlation** – detection of complex attack patterns mapped to frameworks like MITRE ATT&CK.
- **Open APIs** – clean integration with SIEM, SOAR and MDM solutions you may already use.
- **Zero-touch device onboarding** – simple to scale as the business grows.

The eight capabilities below are the building blocks of this platform. They are not all required from day one – but every one of them addresses a risk that is now mainstream, and an integrated platform makes it possible to activate them in the right order, without rebuilding everything you already have.

6.1 Endpoint Protection (EDR / XDR)

Endpoint protection has moved far beyond classical antivirus. **EDR (Endpoint Detection and Response)** and **XDR (Extended Detection and Response)** combine behavioral analysis, heuristics, ransomware rollback, script and fileless-attack detection, and lateral-movement monitoring – stopping threats that signature-based tools miss entirely.

- **Behavioral and heuristic detection** of unknown threats, not just known signatures
- **Ransomware rollback** – restore systems to their pre-attack state
- **Script, PowerShell and fileless-attack detection**
- **Application and device control** for USB, Wi-Fi, Bluetooth
- **SIEM / SOAR integration** for full telemetry across the organization

Why this matters for SMEs under NIS2: EDR/XDR is the technical foundation that makes the **24-hour early warning, 72-hour notification and 1-month final report** required by NIS2 Article 23 actually achievable. Without it, you cannot detect significant incidents fast enough to meet the deadlines – let alone produce the evidence regulators expect.

6.2 Mobile Security

Mobile devices are now central to how SMEs operate – and are an equally central attack surface. Modern mobile security combines app control, network protection and real-time anti-phishing for messaging and mobile browsers.

- **App control and signature checks** to block unauthorized or tampered apps
- **Jailbreak / root and emulator detection**
- **Geofencing and context-based access** (time, location, network)
- **VPN enforcement** and encrypted communications
- **Zero-Phishing for mobile browsers and messengers** (SMS, WhatsApp, etc.)
- **Native MDM integration** (Microsoft Intune, VMware Workspace ONE)

6.3 Email Security with Integrated DLP

Email is still the **primary vector** for cyberattacks. An effective email-security solution – ideally with **integrated Data Loss Prevention (DLP)** – is therefore non-negotiable. For SMEs, cloud-delivered solutions deliver enterprise-grade protection in days rather than months.

- **Anti-malware, anti-phishing and link rewriting** to neutralize threats before delivery
- **Attachment sandboxing** for suspicious files in an isolated environment
- **Domain-spoofing detection** to identify forged sender addresses
- **Built-in DLP** to prevent confidential data leaving via email or cloud collaboration tools (Microsoft 365, Google Workspace)
- **Automatic sensitive-content detection** (PII, financial data, IP) to support compliance

Why this matters for SMEs: consolidating email protection and DLP into one solution removes complexity, lowers cost, and gives a small team the same coverage as an enterprise SOC.

6.4 Browser Security: The New Perimeter

The modern workplace runs in the **web browser**. SaaS apps, cloud collaboration, AI tools, contractor and BYOD access – all happen there. Yet legacy security tools were not designed for this. Modern **enterprise browser security** addresses risks at the point of interaction, where employees actually work.

- **Isolation of malicious websites** before content reaches the device
- **Protection of sensitive data** from accidental disclosure (paste, screenshot, upload)
- **Visibility and control over AI tool usage** – including consumer accounts
- **Context-based policies** for generative AI (e.g., read-only mode, clipboard blocking)
- **Safe BYOD and contractor access** without VPN complexity

Why this matters for SMEs: the browser is the single fastest and lowest-friction control point for both general SaaS use and emerging AI risks. It often delivers the highest security ROI in the first 90 days.

6.5 Zero Trust Network Access (ZTNA)

Traditional VPNs grant a user broad access to the network the moment they authenticate – a model designed for offices, not for cloud and remote work. **ZTNA** replaces this with the principle **"never trust, always verify."** No user or device is trusted by default; access is granted only to specific resources, only when justified by context (device posture, role, location, time).

- **Multi-Factor Authentication (MFA)** and **SSO** via SAML/OIDC – MFA is an **explicit NIS2 Article 21 requirement**, not a nice-to-have
- **Just-in-Time access** – permissions granted only when and as long as needed
- **Device posture checks** – non-compliant devices cannot connect
- **Least-privilege access** by design
- **Granular, adaptive policies** that respond to risk in real time
- **Audit-grade logging** for forensics and compliance

Why this matters for SMEs: ZTNA dramatically reduces blast radius. A single compromised credential can no longer mean access to everything – it means access to one specific application, observed and time-limited.

6.6 Cloud Access Security Broker (CASB)

With cloud and SaaS adoption now mainstream, **CASB** provides the missing visibility and control over how cloud applications are actually used. It identifies **shadow IT**, governs sanctioned services, and prevents data leakage through cloud channels.

- **Shadow IT discovery** – every cloud and SaaS app actually in use
- **Inline and API-based control** of approved applications
- **Built-in DLP** with pattern matching, templates and automatic classification
- **Anomaly detection** – mass downloads, geographic impossibilities, suspicious behavior
- **Tokenization, encryption and watermarking** for data uploaded to the cloud
- **Cloud-to-cloud traffic monitoring** for Office 365, Salesforce, Dropbox and others

Why this matters for SMEs: CASB closes the cloud blind spot. Without it, you have no visibility into the shadow IT your business is running on – and no way to govern it.

6.7 Firewall and SD-WAN

For SMEs with multiple locations, branch offices or complex network needs, a **cloud-delivered Next-Generation Firewall (NGFW)** combined with **SD-WAN** delivers both security and network performance through one stack.

- **TLS inspection and application awareness** – security that sees inside encrypted traffic
- **Intelligent path selection, QoS and load balancing** for SaaS and cloud apps
- **Dynamic site-to-site and site-to-cloud VPNs**
- **GeoIP filtering, URL categorization and centralized logging**
- **Single pane** for network and security policy management

Why this matters for SMEs: consolidating networking and security cuts both cost and operational overhead, and is often the foundation for a modern SASE architecture.

6.8 Data Security Posture Management (DSPM)

DSPM answers a question every executive should be able to answer in a board meeting and most cannot: **"Where is our most sensitive data right now, and who can reach it?"** It continuously scans hybrid clouds, SaaS platforms, file shares, employee laptops and AI-tool histories to identify sensitive data and rank the risks.

Typical DSPM components

Component	Function	Business Outcome
DSPM Scanner	Discovers sensitive data across systems	No more blind spots
Risk Analytics Dashboard	Ranks and visualizes exposures	Board-ready risk picture
Access-rights review	Verifies who can access what	Least-privilege enforcement
Policy recommendations	Automated remediation guidance	Faster cleanup, less manual effort

Why this matters for SMEs: DSPM transforms cybersecurity from **reactive perimeter defense** into a **data-centric, proactive strategy** – and is the foundation needed before deploying any AI program at scale. It also directly supports **NIS2 Article 21** requirements around **asset management, access control and data encryption** by inventorying what you have, who can reach it, and how it is protected.

7. The AI Risk Landscape and Shadow AI

Generative and agentic AI is reshaping the way SMEs work: drafting emails, summarizing reports, analyzing customer data, accelerating development. But this productivity comes with an entirely new class of risk – risks that the foundational platform from Part II reduces, but does not eliminate.

The hidden front line: 77 % of employees paste company data into public AI tools, with **82 %** doing so via personal accounts that bypass corporate controls (LayerX 2025). According to **IBM's 2025 Cost of a Data Breach Report**, shadow AI is now involved in **20 % of all breaches** and adds **$670,000** to the average cost. **63 % of breached organizations have no AI governance policy at all**, and of those that suffered an AI-related breach, **97 % lacked proper access controls**.

What makes AI risk different

- **Confidential data leakage:** Customer lists, source code, contracts, financial data and HR files pasted into public AI tools may be retained, used to train future models, or stored on infrastructure outside your control.
- **Regulatory exposure:** GDPR fines reach **€20 million or 4 % of global annual turnover** for serious infringements. NIS2 and DORA introduce executive liability. The **EU AI Act** adds new obligations for any company deploying AI in regulated processes.
- **Intellectual property erosion:** Proprietary methods, designs and pricing models can be unintentionally embedded in third-party AI systems and resurface in answers given to your competitors.
- **Agentic incidents:** Autonomous AI agents with access to email, calendars, code and CRM systems can be tricked into sending data to attackers or executing fraudulent actions through **prompt injection**.

The executive takeaway: banning AI doesn't work – employees just go further underground, and you lose the productivity. The remedy is to make sanctioned AI **faster and easier than shadow AI**, while putting visibility and AI-specific controls in place. The eight capabilities in Section 8 do exactly that.

8. Eight Capabilities for AI-Specific Security

On top of the foundational platform from Part II, eight additional capabilities address risks unique to generative and agentic AI. Few SMEs need all eight from day one – the right path depends on which AI use cases you are deploying. Match each capability to one of three buckets: **"have today," "need in six months," "watch for the next wave."** That becomes your AI security roadmap.

8.1 AI Security Posture Management (AI-SPM)

Inventories every AI model, agent, copilot and embedding in use; detects shadow AI and insecure configurations; maps your AI estate to the GDPR, EU AI Act, ISO 42001 and NIS2.

8.2 AI Runtime Protection / LLM Firewall

Inspects prompts and outputs in real time – the front line against **prompt injection, jailbreaks, sensitive-data leaks and toxic responses**. Essential for any customer-facing AI feature.

8.3 Agent IAM and Secure Tool / MCP Integration

Treats every autonomous agent as a non-human identity with **least privilege, just-in-time access** and clear separation. Hardens the connectors agents use through protocols such as the Model Context Protocol (MCP): authentication, allowlisting, sandboxing, human-in-the-loop approvals.

8.4 Prompt-Injection Defense and RAG Permission Layer

Sanitizes external content before it reaches the model and ensures **AI search respects real user access controls** – so Copilot and other RAG-based tools never surface documents an employee shouldn't see. The single most common Copilot rollout pitfall.

8.5 AI Observability and Governance

End-to-end tracing of agent steps integrated into your SIEM, plus a short usage policy, a fast approval process for new AI tools, and brief recurring awareness moments. **Culture is your cheapest control.**

9. The 90-Day Executive Action Plan

Modernizing both your cybersecurity foundation **and** your AI security can feel overwhelming. The good news: you don't have to solve everything in the first quarter. You need a **clear sequence** that delivers visibility first, control second, and AI-readiness third. Below is what we recommend to most SME executives we work with.

Days 1–30: See the truth

- Run a **cybersecurity and AI exposure assessment** – inventory current tools, identify gaps, and discover every AI tool actually in use.
- Map your **most sensitive data** (PII, IP, financials, regulated content) and where it currently lives.
- Identify **two to three quick wins** – usually a sanctioned AI tool, a one-page AI usage policy and an executive sponsor.

Days 31–60: Put a floor under the risk

- Activate or upgrade **EDR/XDR, email security with DLP, and enterprise browser security** – the fastest path to broad coverage.
- Deploy **DSPM** to continuously monitor where sensitive data lives and how it moves.
- Roll out a **short, mandatory awareness moment** – fifteen minutes, not two hours – plus board-level cybersecurity training to satisfy NIS2 Article 20.
- Build a **lightweight AI approval process** so business teams adopt new AI tools quickly **and** safely.
- Document an **incident-response playbook with the NIS2 24h / 72h / 1-month reporting timeline**, and start mapping critical suppliers for supply-chain risk.

Days 61–90: Modernize access and get ahead of agentic AI

- Replace legacy VPN with **ZTNA** for least-privilege access; activate **CASB** for SaaS visibility.
- Inventory all **agents, copilots and AI integrations** – Microsoft Copilot, custom GPTs, MCP-connected tools.
- Apply **least-privilege access** to every agent; require human-in-the-loop for sensitive actions.
- Activate **AI-specific monitoring** with SIEM integration; align controls to **GDPR, NIS2, DORA, ISO 42001 and the EU AI Act**.

The strategic payoff: within 90 days, you move from "flying blind" to **"security-mature and AI-confident"** – defending against today's threats while adopting new AI capabilities faster than competitors.

10. Cybersecurity as the Foundation for Cyber Insurance

A modern, integrated cybersecurity platform doesn't just protect against attacks – it produces the **evidence and transparency** that cyber insurers now require. With the **global average data breach now costing $4.44 million** and US incidents reaching an all-time high of **$10.22 million** (IBM 2025), and with **phishing alone driving 16 % of breaches at $4.8 million each**, underwriters have tightened their criteria dramatically. Without demonstrable controls, an SME may pay higher premiums – or be unable to obtain a policy at all.

What insurers actually look for

- **Transparency and monitoring:** Verifiable logs, event chains and incident-response records. Telemetry that lets the underwriter assess your risk profile objectively.
- **Defined processes and policies:** Documented access rules, user-management workflows and escalation paths in case of an incident – proving organizational maturity, not just technical tooling.
- **Data and access protection:** Demonstrated **Zero Trust, MFA, DLP and encryption** across endpoints, cloud and email. Insurers increasingly treat the absence of these as automatic disqualification.
- **NIS2-aligned incident response:** A documented incident-response process that meets the **NIS2 24h / 72h / 1-month** reporting cadence. Insurers see this as evidence of operational maturity – and it is increasingly a precondition for coverage in regulated sectors.

An integrated platform delivers all three at once. The result for SME executives is twofold: **better terms and lower premiums** today, and the ability to **stay insurable** as the market continues to harden. Cyber insurance is no longer a hedge against the unimaginable; it is a normal part of doing business – and the controls described in Parts II and III are what make it accessible.

The dual benefit: the same platform that prevents incidents also reduces the cost of insuring against them – and ensures that, if the worst happens, the policy will actually pay out.

Partner with AQ SECURE

AQ SECURE specializes in helping small and medium-sized enterprises modernize cybersecurity and adopt generative and agentic AI safely – without the budget or headcount of a Fortune 500 security team. We bring **enterprise-grade rigor packaged for SME realities**: pragmatic scope, transparent pricing, fast time-to-value, and a clear path from "assessment" to "operational." Our approach is technology-agnostic and consultative – **visibility, control and cybersecurity in balance**.

How we help SME executives move forward

- **Cybersecurity & AI Exposure Assessment** – a 2-week diagnostic of your current security posture, shadow AI footprint and quick-win opportunities
- **Integrated SASE platform** – EDR/XDR, email, browser, ZTNA, CASB, NGFW, DSPM and DLP from a proven specialist vendor, right-sized for SMEs
- **Compliance acceleration** – GDPR, NIS2, DORA, ISO 42001 and the EU AI Act addressed in one coordinated program
- **Agentic AI security** – securing Microsoft Copilot, custom agents, MCP integrations, AI-SPM and LLM firewalls
- **Optional 24×7 SOC service** – outsourced monitoring and incident response for SMEs without dedicated security teams
- **Transparent consultation** – no black-box solutions; you keep full control and full visibility, always

Your next step. Book a 30-minute executive briefing with our team. You will leave with a clear view of your current security posture and AI risk exposure, the two or three highest-impact actions for your organization, and a realistic budget range to address them.

Visibility, control and cybersecurity in balance. Modern security as the foundation for safe AI adoption.

Book your executive briefing

AQ SECURE GmbH

info@aqsecure.de

www.aqsecure.de