axians Microsoft

Modern SecOps
in the Microsoft Ecosystem

2026

How Swiss companies turn existing security capabilities into long-term cyber resilience





01

From security capabilities **to operational resilience**

Swiss companies already using Microsoft's security solutions face a dilemma: there is a gap between the many available capabilities and truly effective cyber resilience.

This gap arises because security capabilities operate in isolation, signals are not brought together, IT teams assess alerts manually and data is not clearly classified. This increases complexity for IT and security leaders. At the same time, regulatory requirements, cyber risks and management expectations for comprehensive security are increasing.

Modern SecOps closes this gap. It combines protection, detection, response, data control and continuous improvement in a clear operating model. Microsoft provides the integrated platform. Axians Somnitec makes it effective in day-to-day Swiss business through architecture, governance, implementation, operations and continuous optimisation.

This turns Microsoft's security solutions into more than a set of tools. Companies gain transparency into their risks, prioritise measures by impact, make better use of existing licences and relieve internal teams. They respond faster to threats, manage their security posture measurably and strengthen resilience step by step.

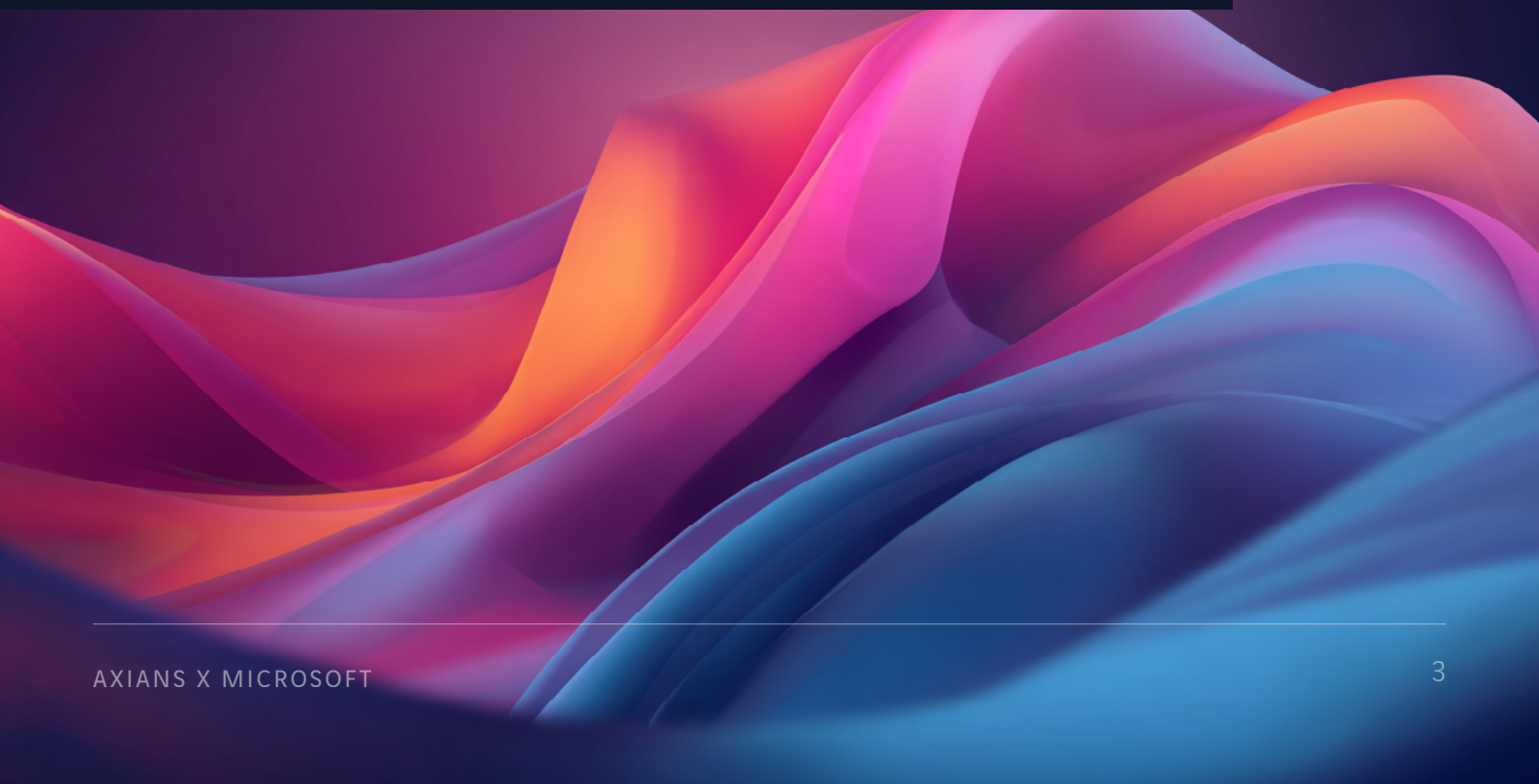
This guide shows how security leaders can evolve their Microsoft security environment into an operational security model. The goal is not only to secure systems technically, but to develop cybersecurity into a manageable contribution to stability, compliance and trust.

02

Security complexity despite investment in Microsoft

In practice, the security level of Swiss companies often falls short of what their purchased Microsoft solutions can offer on paper.

What is missing is a unifying operating model. Security capabilities run alongside one another rather than together. Even with a proven provider and extensive functionality, complexity arises and ultimately security is reduced.



The most common causes

01

Licences are available, but not fully utilised.

Companies often pay for capabilities they use only partially. This is especially true for Microsoft 365 E5, Defender, Entra, Purview or Sentinel. Without a clear roadmap, it remains unclear which capabilities are already available and what impact they could have.

02

Security tools do not work as one.

Even in the Microsoft ecosystem, security operations do not happen automatically. Only when signals, policies, roles and processes work together does a clear situational picture emerge.

03

Alerts erzeugen Aufwand statt Orientierung.

Security teams receive many indicators, but not always clear priorities. Without correlation and defined response paths, every alert becomes an individual review.

04

Data remains difficult to control.

Companies do not know exactly where sensitive information resides, who has access and how data is protected. With growing use of AI, Copilot and cloud services, this question becomes business-critical.

05

Assessments remain point-in-time.

A Secure Score or audit shows a state at one moment. Cyber resilience emerges only when companies continuously measure, prioritise and reduce risks.

What this means for Swiss companies

In Switzerland, these challenges meet a particularly demanding environment. Companies must ensure availability, data protection, compliance and trust, often across multiple sites, language regions and regulatory contexts. At the same time, management, customers and partners expect robust answers to cyber risks.



03

Modern SecOps: Security as an Operational State



Companies often respond to this development with additional tools, new policies or individual projects. However, technology alone does not reduce complexity. On the contrary, without clear integration, operational effort continues to grow.

Modern SecOps therefore takes a different approach.

The focus is not on individual security products, but on end-to-end security operations. The goal is to identify risks early, assess threats faster and continuously improve security measures across identities, endpoints, cloud environments, applications and data. Security is therefore no longer viewed as a collection of individual measures, but as a continuous, centrally orchestrated process.

What Modern SecOps Changes

Modern SecOps brings together prevention, detection, response and governance in an integrated model. Security-relevant signals are centralised, risks can be prioritised, and teams gain more context with less operational friction.

This shifts the focus:

» Away from isolated tools

» Away from manual correlation

» Away from reactive incident handling

Towards:

» Continuous transparency

» Automated prioritisation

» Faster response

» Measurable improvement of the security posture

For companies, this means one thing above all: **greater control.**

Security leaders gain a clearer view of risks, attack paths and vulnerabilities. At the same time, operational pressure on internal teams decreases as processes are standardised, signals are consolidated and recurring tasks are automated.

The **four core areas** of Modern SecOps

A modern security model combines four core capabilities:

Continuously optimise the SOC

Security Operations continuously evolve. Companies continuously improve their detection rules, response processes and security policies, rather than only after audits or incidents.

Make attack paths visible

Modern security platforms analyse relationships between identities, devices, cloud resources and permissions. This allows risks to be identified earlier and prioritised more effectively.

Detect threats holistically

Attacks rarely originate from a single point. Modern SecOps brings together signals from different areas to create a unified view across the entire environment.

Respond faster and more intelligently

Automation and AI help security teams assess incidents, prioritise actions and accelerate response processes.

The Key Difference

Modern SecOps does not replace an existing security strategy. Instead, it brings existing capabilities together into an integrated operational model. For many Swiss companies, this represents the next stage of development: moving beyond the technical use of existing Microsoft Security capabilities and turning them into resilient, continuously managed security operations.



The **Microsoft Unified Security** Platform

04

To achieve this, companies need a security architecture that brings information together rather than keeping it separate. This is precisely what Microsoft has designed its security solutions to do as an integrated platform.

Identities, endpoints, email, cloud services, applications and data continuously generate security-relevant signals. The Microsoft Unified Security Platform connects these layers into a shared security model.

Connect security across all layers

Microsoft Defender XDR provides the operational foundation for detection and response. The platform brings together signals from different areas and creates a shared security context.

Microsoft Sentinel extends this model with centralised analytics and automation capabilities.

With **Microsoft Entra**, identity becomes central to the security strategy. Access, permissions and user contexts are continuously evaluated to identify risks early and implement Zero Trust principles.

Microsoft Purview adds the data perspective to the platform. Companies gain greater transparency into where sensitive information is stored, how it is used and how data can be better protected.

Security Copilot uses AI to help security teams classify information faster, better understand relationships and make response processes more efficient.

From individual signals to operational control

The strength of this platform lies in orchestration. A suspicious login, for example, does not remain an isolated signal. It can be linked to device information, data access, user behaviour or cloud activities. This context is crucial to the effectiveness of Security Operations today.

Companies benefit from:

- greater transparency into risks
- less operational friction
- faster prioritisation
- more consistent security processes
- a stronger foundation for governance and compliance

05

Data Security as the Foundation for the Secure Use of AI

As the use of AI increases, the role of cybersecurity is also changing. Companies are no longer protecting only devices, user accounts or applications. Increasingly, data itself is at the centre. AI systems work with the very information that companies create, store and share every day. The more deeply AI is integrated into business processes, the more important one question becomes:

What data is a system actually allowed to see, process or share?

This brings Data Security to the centre of modern security strategies.



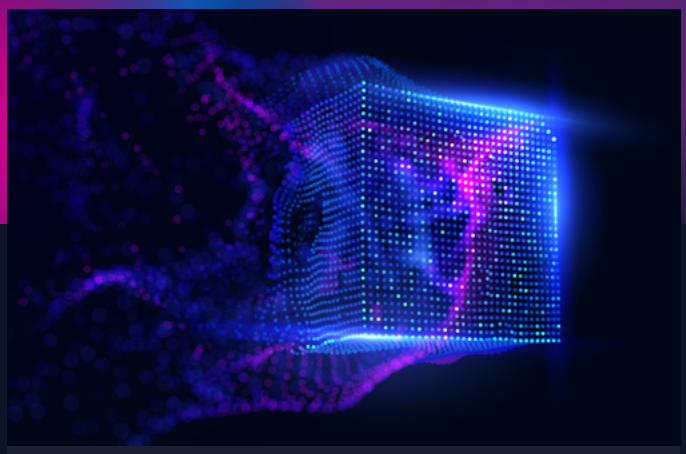


AI Increases the Pressure on Governance and Transparency

This creates new challenges:

- Sensitive data becomes too widely accessible
- Permissions grow over time without sufficient control
- Information is incorrectly classified or not protected at all
- Data leaves defined security contexts
- Compliance and data protection requirements become more difficult to manage

The introduction of AI makes existing vulnerabilities more visible and, in many cases, more critical.



Data Security Needs Context

This is precisely why traditional perimeter security is no longer enough. Companies need to understand:

- where sensitive data is located
- who can access it
- how information is used
- what risks arise from sharing, cloud services or the use of AI

Microsoft Purview adds exactly this perspective to the security architecture. Data can be classified, protection policies defined and access better controlled.

Microsoft Purview adds exactly this perspective to the security architecture. Data can be classified, protection policies defined and access better controlled.

This approach is particularly important in the Swiss context. Data protection, regulatory requirements and the trusted handling of information play a central role for companies, customers and partners.

06

From Point-in-Time Security to Continuous Resilience

Data protection, governance and Data Security can no longer be viewed in isolation. They are directly linked to how resilient a company truly is to cyber risks.

That is precisely why assessing security only at specific points in time is no longer enough. Security is created through continuous operations. A modern security model evolves constantly. Risks change, attack patterns adapt and digital environments continue to grow. Companies therefore need an approach that continuously improves security.

This is where modern platform capabilities such as Secure Score, Exposure Management and Attack Path Analysis come in. They help companies to:

01 Identify security gaps early

02 Prioritise risks based on actual relevance

03 Identify critical attack paths

04 Track progress measurably

05 Continuously improve security measures

Instead of isolated measures, this creates a continuous cycle of assessment, prioritisation, implementation and optimisation.

From Point-in-Time Security to Continuous Resilience

It is particularly important to understand the connections between risks. A single risk often appears harmless until it is combined with other vulnerabilities.

An overlooked device access point, overly broad permissions or unprotected sensitive data can together create critical attack paths. Modern security platforms help make exactly these connections visible.

This also changes how priorities are set in day-to-day security operations. Teams no longer focus solely on the number of alerts or vulnerabilities, but on their actual impact on the company's risk exposure.



07

From the Platform to Secure Operations with Axians Somnitec

Even powerful platforms only deliver their full value when companies not only identify risks in context, but also translate them into clear processes, responsibilities and actions.

The key is how consistently security is integrated into day-to-day operations. True cyber resilience only emerges when security is operationally embedded in processes, roles and workflows. This is where Axians Somnitec comes in. Axians Somnitec helps companies turn existing Microsoft security capabilities into an integrated security model aligned with the organisation, risk profile and existing IT structures.

The focus is on continuously manageable security operations. This includes:

01 Defining a robust security baseline

02 Integrating key Microsoft security components

03 Developing clear operational and response processes

04 Continuously optimising the security posture

05 Reducing the burden on internal teams through standardised Security Operations

Axians combines technical implementation with governance, operations and continuous strategic development.

A Model That Fits the Swiss Reality

For Swiss companies, reliability, transparency and governance play a central role alongside technology. Security must not only be effective, but also remain transparently manageable for management, customers, partners and regulatory requirements.

Axians Somnitec combines Microsoft Security with local operational expertise, clear responsibilities and a structured Modern SecOps approach.

This turns individual security capabilities into security operations that reduce risks, relieve internal teams and strengthen cyber resilience over the long term.



08

Where Do You Stand? **The Path to Modern SecOps**

The goal is not to redesign the entire security system at once. Companies develop their security organisation step by step, depending on their risk profile, resources, regulatory requirements and existing IT landscape. The following maturity model shows how companies typically progress towards Modern SecOps.

01

REIFEGRAD 1

Tool-basierte Security

Microsoft security capabilities are available, but largely operate in isolation.

Typical characteristics:
- Many manual processes
- High alert volume
- Limited transparency
- Security is primarily managed as a technical function

02

REIFEGRAD 2

Integrated Security Platform

Security signals from identities, devices, cloud environments and data are increasingly consolidated.

Typical characteristics:
- Greater transparency into risks
- Initial automation
- Security baselines and policies
- Measurable security posture

03

REIFEGRAD 3

Operational Modern SecOps

Security is embedded within the organisation and continuously managed.

Typical characteristics:
- Defined operational and response processes
- Continuous monitoring and reporting
- Clearer prioritisation
- Reduced workload for internal teams

04

REIFEGRAD 4

Resilient Security Organisation

Security evolves into a continuously optimised operating model.

Typical characteristics:
- Proactive risk analysis
- Integrated Data Security and governance
- AI-supported workflows
- High transparency and control



Get in **Touch**

Would you like to know where you stand today? A Modern SecOps Readiness Assessment with Axians Somnitec shows you what potential already exists within your Microsoft Security solutions.

Together, we then identify the measures that will have the greatest security and business impact, aligned with your requirements and resources. Get in touch!