Special Edition
Cybersecurity
Summit

United Innovations

Survey of Tools for

Secure Infrastructures and Processes

Release 2026

www.united-innovations.eu

CYBERSECURITY SUMMIT

Join the Cybersecurity Summit 2026 on March 17th in Duesseldorf, where industry leaders and innovators will explore the latest advancements in cybersecurity and witness the exciting finals of the German Startup-Cup.

17/03/2029
9:00 AM

VODAFONE SKY LOUNGE
FERDINAND-BRAUN-PLATZ 1
40549 DÜSSELDORF

Event Website

EDITORIAL

Security as the foundation of our digital future: A call for responsibility

Dear colleagues, distinguished guests,

It is a great honour for me and – as many of you know – a matter close to my heart to welcome you here today at the Security Summit. As former CIO of Vodafone Germany, I look back on a time when we set the course for digital transformation. Today, in 2026, we can see more clearly than ever that the digital world has changed rapidly. Technologies such as artificial intelligence, cloud computing and the Internet of Things open up unprecedented opportunities for us. Our meeting today has a clear focus: we must radically prioritise the importance of cyber security in order to ensure the digital sovereignty of all our customers. But how can we achieve this at a time when cyber attacks and vulnerabilities in software systems are part of everyday life? The answer lies in two inseparable pillars that also form the core of today's agenda: security by design and a vibrant security culture.

From reacting to acting: the philosophy of security by design: We have learned that traditional, reactive approaches are no longer sufficient. Adding security after development runs the risk of overlooking vulnerabilities and can result in immense financial damage and a massive loss of trust. That is why the concept of "security by design" has established itself as an indispensable standard. It is more than a method; it is a philosophy that integrates security into the architecture of our systems as an integral part from the outset. Since the Cyber Resilience Act (EU 2024/2847) at the latest, we have been morally and legally obliged to implement proactive security measures. We must create systems that operate according to principles such as minimising the attack surface, "defence in depth" and "least privilege". In concrete terms, this means that every process and every user is only granted the minimum necessary rights – a fundamental concept for drastically reducing the attack surface. But technical implementation – whether through threat modelling using frameworks such as STRIDE, the use of SAST and DAST tools, or cryptographic mechanisms – is only one side of the coin. We know that technological hurdles and a lack of expertise often act as a brake. But we must not view security as an "add-on". Security by design is a promise of quality to our customers.

The human factor: security culture as resilience: Technology alone will not save us. Establishing a culture of security within the company is a fundamental prerequisite for truly improving resilience against attacks.

Security begins with people. And here I hold us all accountable, especially those at management level. Creating a culture of security starts at the top. We as leaders must treat IT security as a strategic priority and lead by example. It is not enough to write policies; we must demonstrate through our behavior and decisions that security is embedded in our values. This includes providing sufficient resources for training and infrastructure. We must move away from the "fear of change" towards an organisation that seamlessly integrates security practices into everyday work. This requires regular, interactive training that goes beyond mere lectures. Workshops, security incident simulations and gamification approaches are essential to maintain awareness of issues such as phishing and password security. One particularly important aspect that is close to my heart is the establishment of a positive error culture. We must create an environment in which mistakes are not punished but are seen as valuable learning opportunities. If employees are afraid to report security incidents, we lose the opportunity to respond quickly. Companies such as Google and Ikea show us that psychological safety is the key to both innovation and security.

Our promise: trust and confidence: Why are we doing all this? Because the consequences of poor security practices – data leaks, system failures, loss of reputation – are devastating in our interconnected world. By incorporating security considerations into the development process from the outset, while empowering every single employee to be part of the solution, we are strengthening consumer confidence. Let's use this summit to learn from each other and seek exchange – even across company boundaries. Security is not a state, but a continuous improvement process (CIP) that requires agility and constant adaptation to new threats. I wish us all an inspiring day full of insights. Let us work together to understand security not as a compulsory exercise, but as the foundation of our digital sovereignty.

Yours sincerely, Ulrich Irnich, Former CIO Vodafone Germany

DEUTSCHER STARTUP-POKAL

Calling all innovators - New Season of Startup Cup !

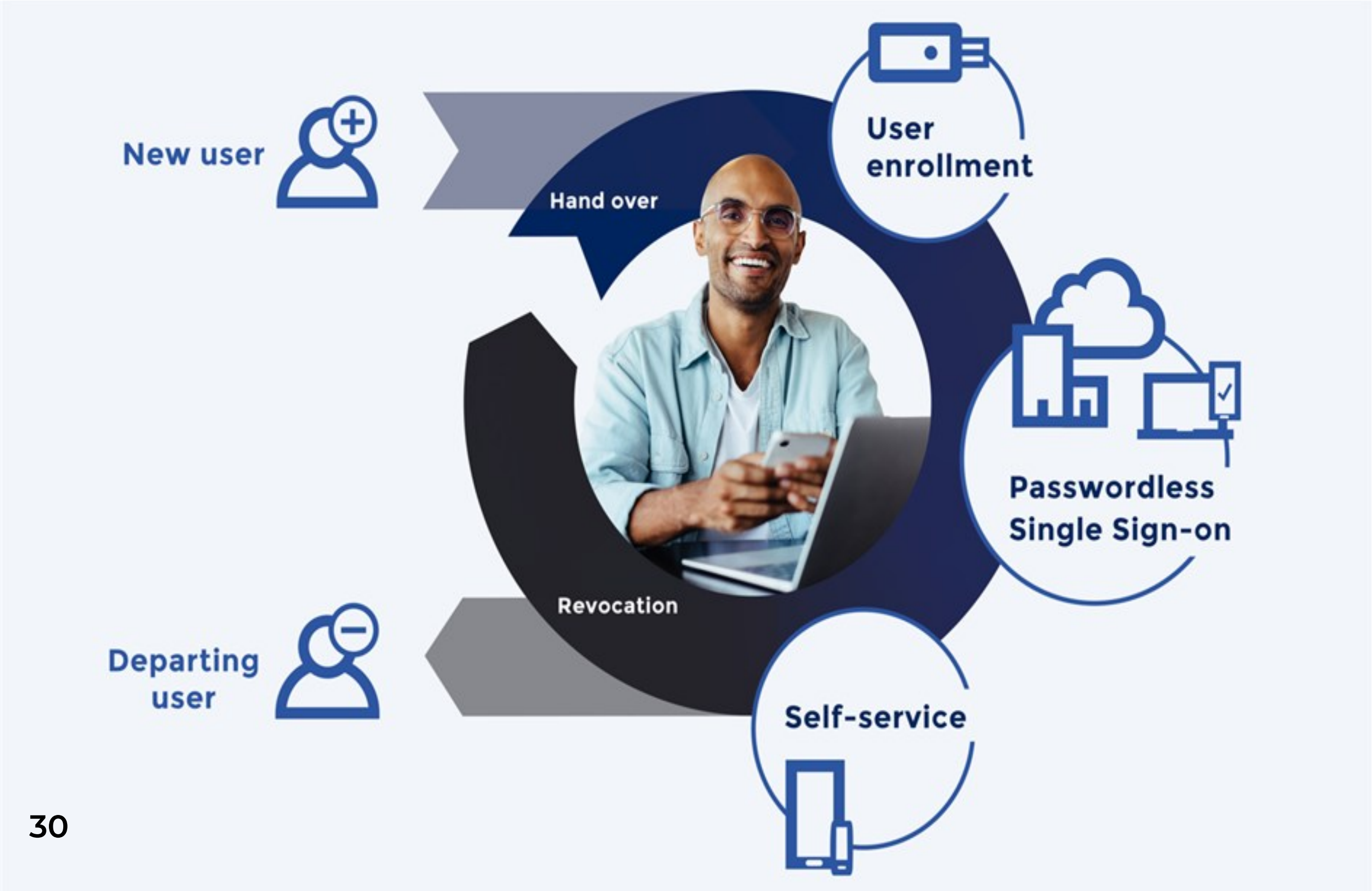
Get ready for an exciting new season of the Startup Cup! Every year, a large number of start-ups enter the new season of the German Start-up Cup and throw their hats into the ring to pitch for the cup. The live final events are held in partnership with companies such as BASF Coatings, PwC, KfW, Vodafone and Nord LB. There, the German Startup Cup is awarded during a summit in front of industry and science representatives and a jury of experts.

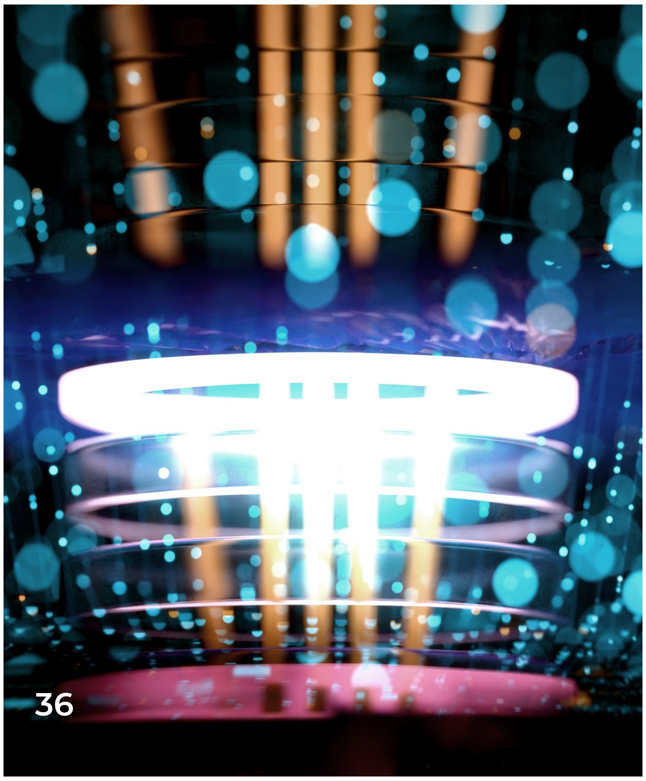
Apply now:

» https://www.united-innovations.eu/deutscher-startup-pokal-bewerbung/

Screen17's Sustainability Driver Framework
SCREEN
#pwcexperience
United
JOIN OUR INNOVATION NETWORK

GFFT
United Innovations
PHOENIX group
DEUTSCHER STARTUP-POKAL
UNITED INNOVATIONS AWARDS
USE CASE AWARD
UNITED INNOVATIONS AWARDS
Herzlich Willkommen!
Finale Deutscher Startup-Pokal & Use Case Award
Cybersecurity / KI & Software


New user
Hand over
User enrollment
Passwordless Single Sign-on
Self-service
Revocation
Departing user
30


36

AI
38

CONTENT

United Innovations

Driving European Innovation Forward

United Innovations (UI) is a dynamic force reshaping Europe's innovation landscape. Our mission is to enhance efficiency in large corporations and promote the adoption of cutting-edge methods and technologies. UI focuses on increasing the success rate of new technologies in Europe, bolstering the continent's reputation as a leading innovation hub.

At UI, we emphasize collaboration through our innovation network, enhancing efficiency, quality, and reducing costs. Our partnerships expedite innovation cycles, facilitating the successful launch of new advancements.

Our innovation strategy revolves around identifying innovation needs, assessing current methods and technologies, and establishing effective innovation processes, including the development and implementation of new solutions.

United Innovations invites you to be part of this vibrant evolution in Europe's innovation sector. For more information, visit www.united-innovations.eu or follow UI on LinkedIn.

Contact

info@united-innovations.eu
+49 6101 95498-10

Our vision

GFFT
Gemeinnützige Gesellschaft zur Förderung des Forschungstransfers e.V.
United Innovations
pwc
DEUTSCHER STARTUP-POKAL
UNITED INNOVATIONS AWARDS
Paneldiskussion
#pwcexpe

Social Media

www.linkedin.com/company/gfft-ev/

Imprint

GFFT Innovationsförderung GmbH
Dr. Gerd Große
Niddastraße 6
61118 Bad Vilbel

Web

www.united-innovations.eu

Beyond Shift Left and Shift Right: The Role of Runtime Evidence

Security leaders have spent the last decade professionalising “shift left”. Better engineering practices, faster feedback loops, automated testing, software composition analysis, and security gates in CI have raised the baseline. This work matters as it reduces avoidable exposure and improves overall software quality.

An article by Contrast Security

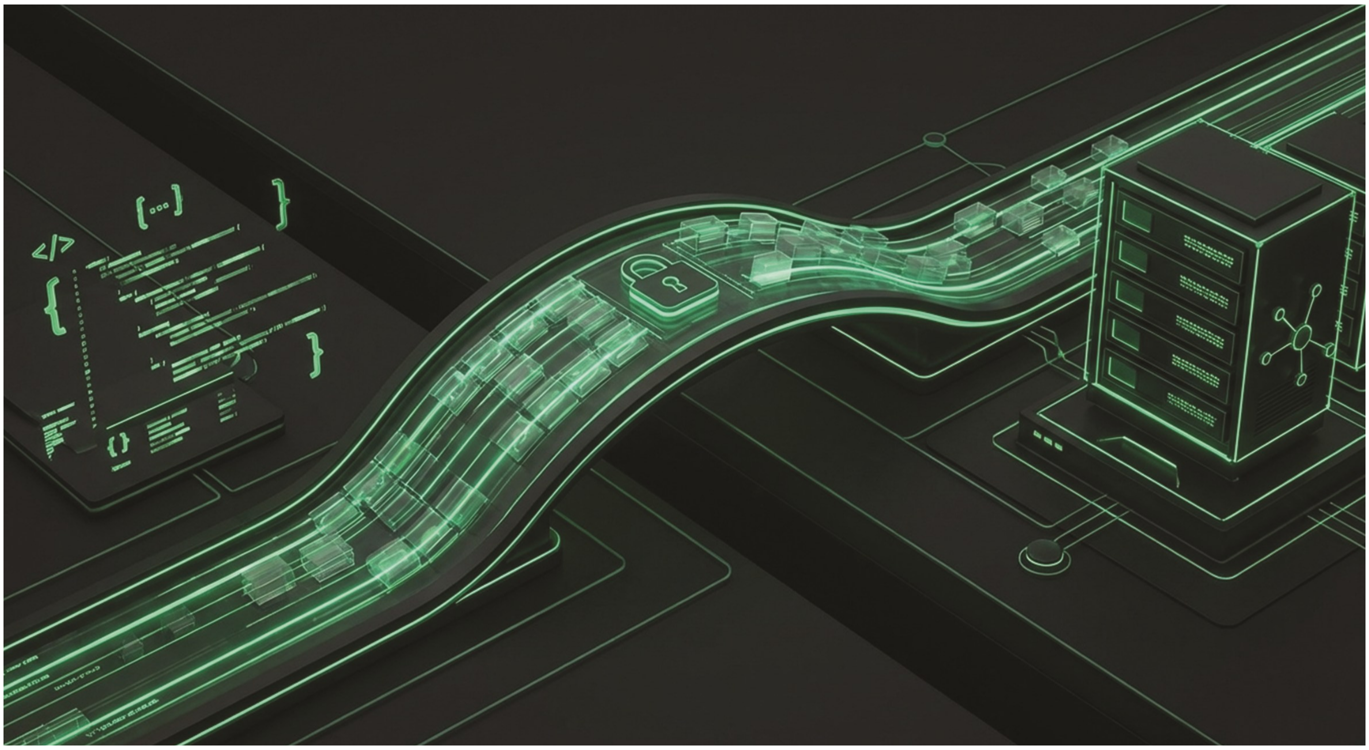


Image source: © Contrast Security

However, it has also created an assumption: that if enough controls are placed in the pipeline, application resilience in production can be reliably predicted.

In practice, it cannot.

Attacks do not occur in backlogs, design reviews, or build stages. They occur against running applications, live APIs, and real user journeys. Production is where intent meets execution. It is also where security teams are often least informed, because the application itself remains the least observed layer in many environments.

This is the core issue behind the “shift left versus shift right” discussion. It is often framed as a trade-off, when in reality it is a dependency chain. Shift left reduces the number of defects that are deployed. Shift right determines which of those defects actually matter, which are being exploited, and what action is required.

Without runtime evidence, organisations tend to fall into one of two positions.

The first is assumption. Controls in the pipeline are trusted to be sufficient, and incidents in production are treated as exceptions. Investigations rely on inference - logs, network indicators, correlations, and judgement calls about whether an alert represents a real threat.

The second is volume. Uncertainty is compensated for with more rules, more alerts, and more dashboards. Over time, this increases operational cost and places sustained pressure on security teams without necessarily improving outcomes.
Neither approach scales under three pressures that have become increasingly visible.

First, application environments are heterogeneous. Most organisations operate a combination of modern services and older tier two and tier three applications that still process sensitive data and still have some form of external exposure. These systems are often business-critical, sparsely documented, and rarely changed - but still exposed.

Second, software itself is changing. Machine-generated code is becoming more common in both development and maintenance. While this accelerates delivery, it also introduces code paths that are not always fully understood by the teams operating the systems. At the same time, attackers are increasingly using automation to discover and exploit weaknesses at scale. In this context, slow detection and ambiguous evidence represent a structural disadvantage.

Third, security budgets are being evaluated based on outcomes. Boards and executive management are asking for clear proof that controls work in practice, not only in design. After an incident, organisations are expected to explain not just what was detected, but what was actually happening inside the affected systems.

This is where runtime becomes a practical requirement rather than a conceptual one.
Runtime visibility provides direct insight into how applications behave during execution. It shows which code paths are used, whether user input reaches a vulnerable function, and whether a known weakness is actually being exercised. This replaces assumptions with verifiable information.

Application Detection and Response (ADR) is designed to address this operational gap. It instruments applications during execution and identifies attacks based on real behaviour inside the application, not solely on external indicators. For security operations, the effects are tangible: fewer alerts due to higher confidence signals, faster triage through explicit exploit context, and more targeted response options that focus on the vulnerable behaviour rather than broad, disruptive controls.

This is not a question of choosing shift right instead of shift left. Shift left defines the prevention strategy. Shift right provides the evidence, measurement, and operational feedback loop that makes prevention accountable.

For most organisations, the practical question is not which approach to adopt, but whether they have sufficient visibility to understand what is actually happening inside their most important applications when it matters.

John Wood

Sales Director Europe
Contrast Security

From compliance to genuine security

An article by Bugshell

Why new regulations are forcing a rethink of cyber resilience

Cybersecurity has changed fundamentally in recent years. Not only due to technological advances or increasing threats, but also due to an expanding regulatory framework. Initiatives such as NIS2, DORA and increasing requirements along the supply chain make it clear that security is no longer an optional IT discipline, but a central prerequisite for economic cooperation.

Compliance is thus becoming the focus of attention. Certifications, evidence and regulatory audits are increasingly determining whether business relationships are established or continued. Cybersecurity is becoming a prerequisite for market access and trust.

When regulatory compliance becomes the target

Implementing new requirements is complex, resource-intensive and time-critical. Accordingly, organisations focus on fulfilling the required evidence in a structured, efficient and audit-proof manner. This prioritisation is understandable – after all, delivery capability, contractual relationships and corporate stability depend directly on it.

At the same time, an area of tension arises: Regulatory compliance primarily describes the degree to which defined requirements are met, not the actual resilience to real attacks. While audits provide snapshots, attack strategies evolve dynamically and exploit technical vulnerabilities, organisational gaps and dependencies between companies. This can lead to a situation where formal compliance is achieved, but real cyber resilience remains unclear.

Regulation has a systemic effect – across industries

Current developments clearly show that cyber security can no longer be viewed in isolation. Whether critical infrastructure, the financial sector or industry – regulatory requirements are increasingly taking an ecosystemic approach. Security levels are passed on along supply chains and responsibilities are anchored at management level. This also changes the requirements for companies:

- Risks must be continuously assessed.
- Security decisions become a management task.
- Evidence must reflect real effectiveness.

Cybersecurity is thus developing into a permanent control and governance issue.

From proof of compliance to robust resilience

Against this backdrop, it is no longer sufficient to simply document security measures. The ability to test the effectiveness of protective measures under realistic conditions and to continuously develop them further is becoming crucial.

Key components include:

- Practical security reviews
- Clear prioritisation of business-critical risks
- Close integration of IT, processes and organisation

Only this combination creates a security foundation that not only meets regulatory requirements but also creates business stability and capacity to act.

Image credit: © canva/anyaberkut/Getty Images

Compliance as the starting point for strategic security

The multitude of current regulations is not a temporary trend, but rather a structural change. Compliance is becoming a necessary ticket to digital value creation, but resilience is becoming the real differentiating factor.

Organisations that use regulatory requirements as a structured starting point and continuously review security build lasting trust with customers, partners and regulatory authorities. Specialised partners can support this transition by combining regulatory understanding with technical assessment and translating risks into clear priorities. The key is an approach that goes beyond formal evidence and makes real resilience measurable.

Outlook

Cybersecurity is thus becoming an integral part of corporate responsibility – comparable to financial or quality management. NIS2, DORA and other initiatives do not mark the beginning of a short-term adjustment phase, but rather a permanent transformation process. The focus is not on whether compliance is being met, but on how this can be used to create robust security. Companies that shape this change at an early stage are securing their future viability in a networked, digital economy.

Jakob Semmler

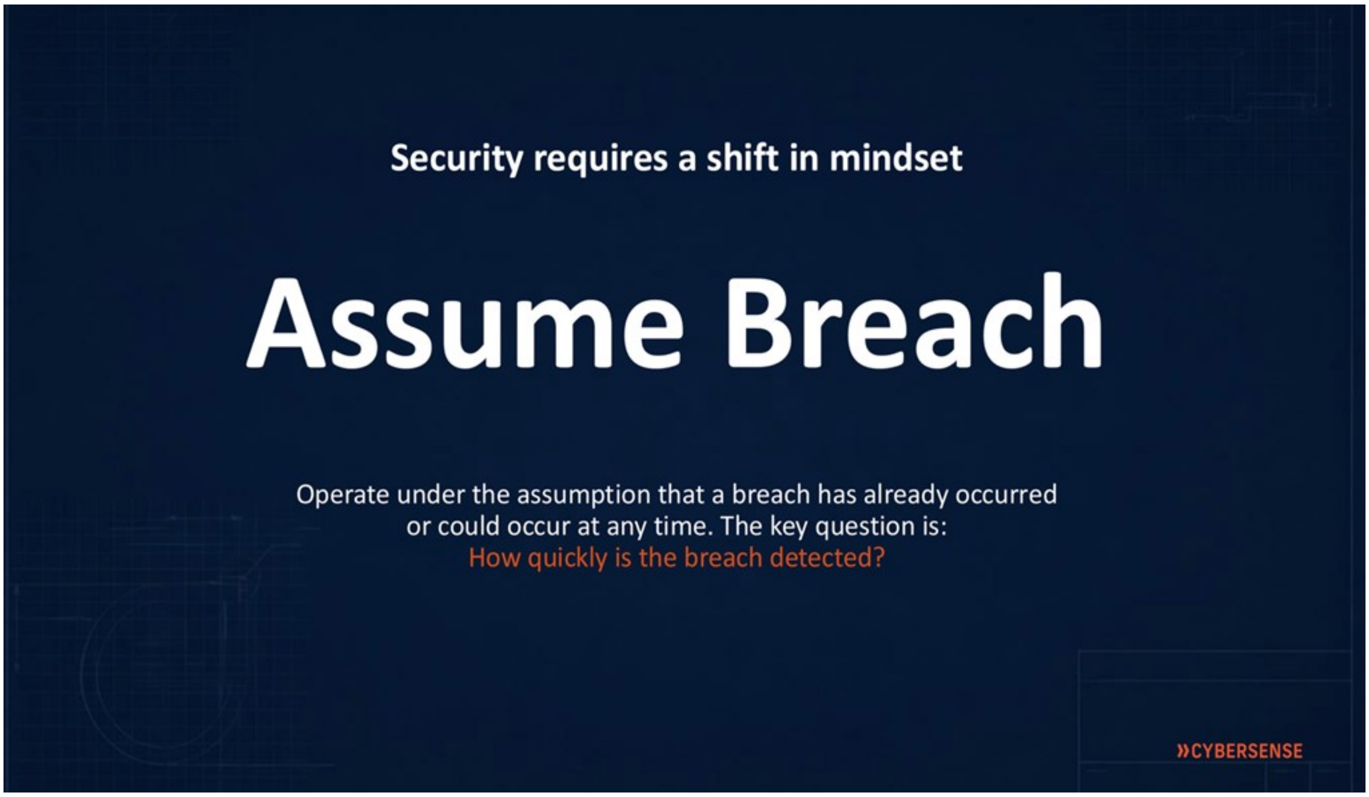
Co-Founder
BugShell GmbH

Detailed information in the techL profile:
Bugshell

Hard Shell, Soft Core

Where modern security architectures still fall short: why organisations continue to pass security tests while attackers operate undetected once they are inside the network?

An article by Cybersense



Security requires a shift in mindset

Assume Breach

Operate under the assumption that a breach has already occurred or could occur at any time. The key question is: How quickly is the breach detected?

»CYBERSENSE

Image credit: © Cybersense GmbH

Hardly any organisation today refrains from investing significantly in the protection of its IT perimeter. Firewalls, email security, web gateways and endpoint protection are part of the standard security toolkit and generally pass audits, penetration tests and compliance checks with solid results. Paradoxically, however, real-world experience shows a recurring pattern: in almost all successful cyber attacks, these very measures failed to prevent the incident.

This contradiction is not an indication of technical weakness. The "hard shell" works – it blocks a large proportion of unspecific attacks and fulfils its intended role within the security architecture. The structural problem lies elsewhere: inside the infrastructure. Modern IT environments are complex, hybrid and heavily identity-driven. Attackers increasingly rely on legitimate access paths such as phishing, compromised credentials or third-party service providers. Once initial access has been obtained, traditional protective mechanisms offer only limited effectiveness.

As a result, modern attacks rarely fail at the perimeter. What matters instead is the phase after the breach: the attacker's undetected movement within the network. This so-called dwell time often spans several weeks in European organisations. During this period, attackers analyse internal structures, extract directory information, move laterally and prepare targeted attacks against business-critical systems. For IT managers and decision-makers alike, the implication is clear: the primary risk is not initial access, but the lack of visibility inside the environment – the "soft core".

Against this backdrop, deception technology is gaining relevance. Rather than continuously evaluating all network activity for anomalies, organisations deliberately integrate decoy systems and intentionally placed access information into their infrastructure. These assets serve no productive purpose, yet are difficult for attackers to distinguish from genuine target systems. Any interaction with them therefore constitutes a highly reliable indicator of unauthorised activity.

This approach shifts detection away from statistical interpretation towards clearly attributable signals. Attackers become visible as soon as they begin to explore the environment or move laterally, regardless of whether traditional perimeter controls have already been bypassed. Deception thus addresses precisely the phase of an attack in which the inner part of the infrastructure has traditionally remained insufficiently monitored.

Building on this technological principle, some providers focus specifically on attack detection within the internal network. Cybersense, a German cybersecurity software provider, for example, uses intrusion detection based on deception technology to identify unauthorised activities at an early stage and to direct security operations towards events of genuine relevance. The objective is to reliably distinguish real intrusion attempts from legitimate activity and thereby close the gap that classical perimeter and monitoring solutions leave open inside complex infrastructures.

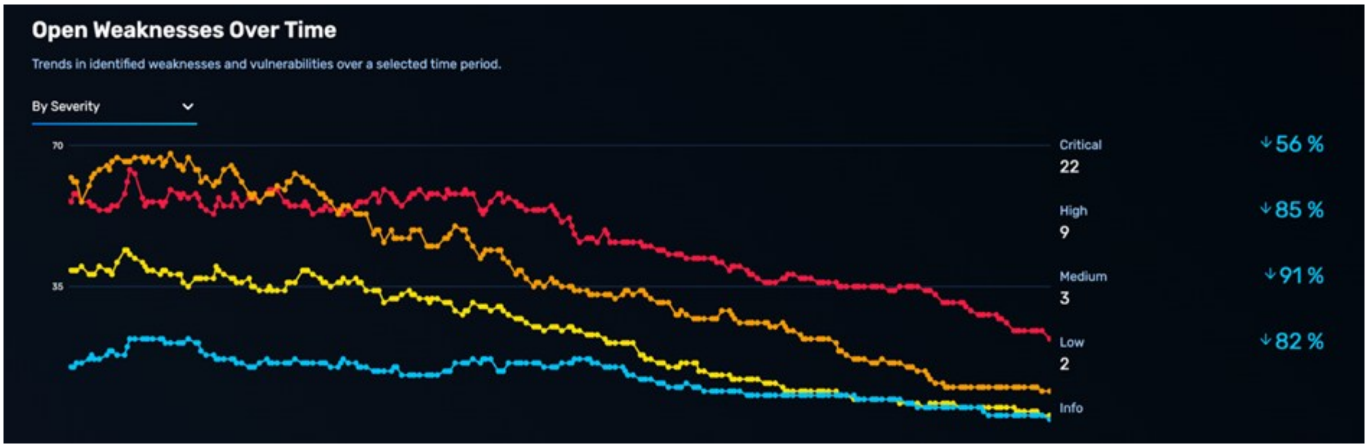
A strong perimeter remains essential. Without an equally robust core, however, it is incomplete. Sustainable cybersecurity emerges where successful test results are not confused with actual security – and where attack detection is treated as a strategic capability rather than a by-product of technical shielding.

Ralf Sturhan
Managing Director
Cybersense GmbH

Eight criteria for an effective cybersecurity solution

Cyberattacks are constantly on the rise and increasingly targeting medium-sized companies. An effective cybersecurity solution is considered the gold standard for identifying and reducing real attack risks — but only if it is scalable, continuous, and practical. The following eight criteria help to realistically evaluate cyber security solutions

An article by DEFENDERBOX



DEFENDERBOX customer: Development of open security vulnerabilities over the course of a year. © defenderbox

The following eight criteria provide a framework for evaluating cybersecurity solutions realistically and thoroughly.

1. Scalability of tests

The cybersecurity solution must be able to monitor a company's entire IP address space – even in productive environments. Attackers view organizations as a whole. Systems that only analyze sub-segments leave relevant attack surfaces undetected. Modern approaches cover 10,000 to over 100,000 IPs in a single run, ensuring coverage that mirrors an attacker’s perspective. Large-scale testing is particularly important for companies with complex IT environments, including multiple sites, remote offices, and diverse hardware and software ecosystems.

2. Coverage of hybrid IT environments

Many organizations today operate hybrid infrastructures, combining on-premises servers, private clouds, and multiple public cloud platforms. A robust cybersecurity solution must seamlessly navigate these environments, identifying risks across all layers. Tools that operate solely within a single cloud instance or data center can leave dangerous blind spots, allowing attackers to exploit less-monitored areas. For example, an effective solution should detect exposed cloud credentials stored on file shares or misconfigurations in multi-cloud environments—exactly the way an attacker would explore weaknesses.

3. Autonomy instead of static processes

Effective solutions respond dynamically to newly discovered security information. Static workflows are not sufficient to detect complex attack paths. Autonomous systems analyze context, move laterally within the network, and link multiple vulnerabilities—similar to real attackers.

4. Verifiable evidence instead of assumptions

Vulnerability scanners often deliver false positives. Without concrete, verifiable proof of exploitation, IT teams struggle to order risks effectively. Verifiable evidence of successful security incidents, including logs of the steps taken, is crucial. This is the only way to correctly prioritize risks and communicate them internally.

5. Concrete recommendations for action

Identifying a vulnerability is only the first step. Good solutions provide understandable, actionable instructions for remediation—even for IT teams without in-depth security expertise. Clear guidance reduces human error, accelerates mitigation, and ensures that the organization's security posture improves after each test.

6. Rapid verification of corrections

Once vulnerabilities are addressed, it is essential to confirm that remediation efforts were successful. Efficient cybersecurity solutions offer targeted retests that verify fixes within minutes, not days. This capability not only improves risk management but also frees up IT resources, allowing teams to focus on proactive measures rather than repeating lengthy testing cycles.

7. Responsiveness to new threats

Known exploited vulnerabilities (KEVs), such as those tracked by CISA, are prime targets for attackers. Security solutions must quickly integrate new exploits, allowing organizations to assess zero-day and n-day risks without delay. Timely updates, combined with continuous monitoring, ensure that the organization remains protected even as threats evolve. Rapid threat adaptation is essential for staying ahead of attackers and minimizing exposure to emerging vulnerabilities.

8. Centralized evaluation and trend analysis

Individual test results are only part of the picture. A comprehensive solution provides an organization-wide view of risk trends, progress, and recurring vulnerabilities. Consolidated dashboards, historical trend analysis, and standardized reporting enable executives and security teams to make informed strategic decisions, allocate resources efficiently, and track improvements over time.

Conclusion

Cybersecurity solutions only reduce risks sustainably when they operate at scale, continuously monitor the environment, and provide clear, actionable guidance. Coupled with rapid retesting, verifiable evidence, and comprehensive trend analysis, they create a reliable foundation for decision-making not only in medium-sized enterprises.

The DEFENDERBOX delivers this holistic, autonomous approach, combining monitoring, real-world exploit testing, actionable remediation, and centralized analytics in a single platform tailored specifically to the needs of the medium-sized business sector.

Markus Schulte
CEO
DEFENDERBOX

Next-Level Attack Surface Assessment

The Internet Is Your New Perimeter – But Who Owns the Risks? Why CISOs, boards, and operators are rethinking external exposure

An article by Graydaxe Cybersecurity

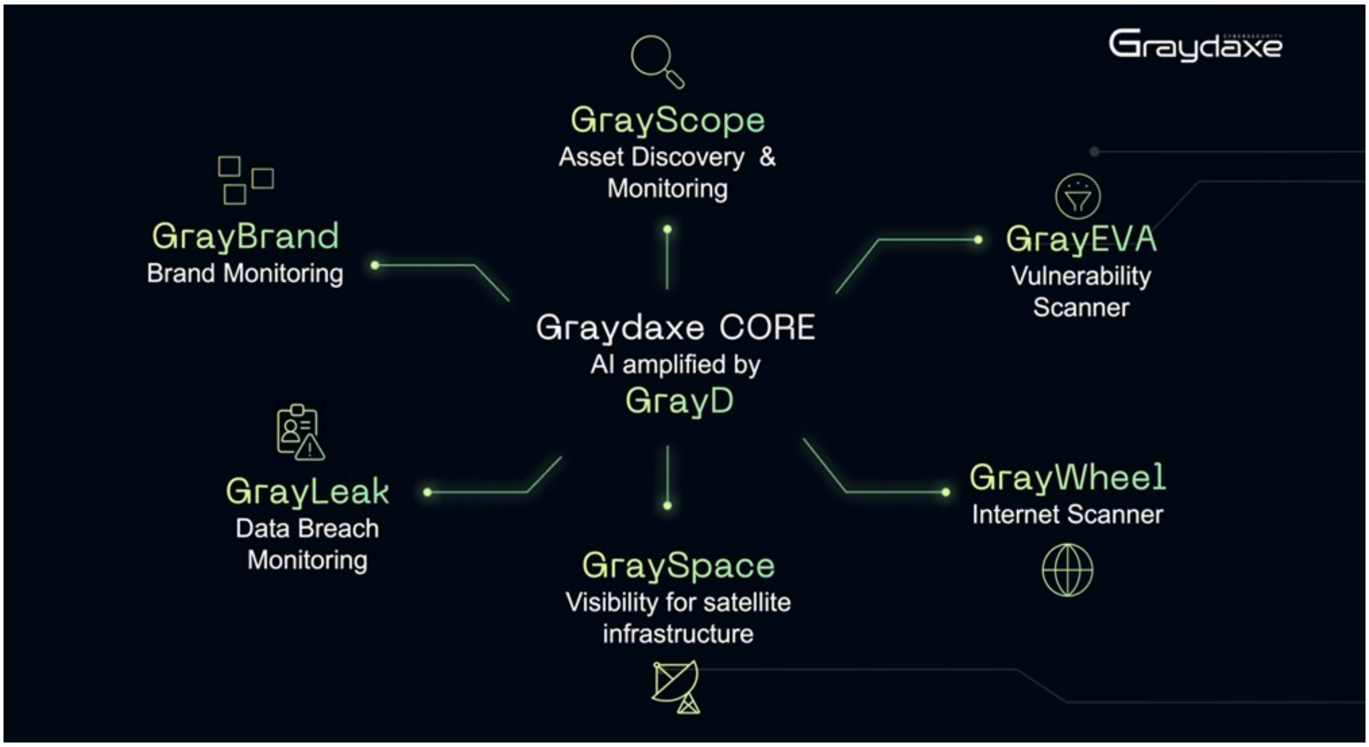


Image credit: Graydaxe Cybersecurity GmbH

For years, organizations secured clearly defined internal environments. Networks, systems, and assets were known and controlled. This model no longer reflects today's reality.

Cloud services, APIs, third-party platforms, and connected devices have moved the security perimeter onto the public internet. Every day, new digital assets go online — often without anyone knowing. Domains are registered, cloud services are spun up, test systems are exposed, APIs are published, and integrations are connected.
At the same time, attackers continuously scan the internet, searching for weak points long before defenders do.
Security tooling has traditionally focused on internal environments, while external exposure extends beyond traditional visibility models. As a result, the perimeter is no longer fixed but increasingly dynamic and difficult to define.

When exposure becomes invisible

Externally exposed assets often remain invisible until it is too late. These include forgotten domains, legacy servers, test environments, misconfigured cloud storage, impersonated brand identities, leaked credentials, or publicly accessible APIs.

While organizations often lack awareness of these assets, attackers can find and exploit them with ease. Shadow IT is widespread. Cloud environments change constantly. There is often no central inventory of externally exposed systems. Public-facing services are frequently misconfigured. Most organizations do not actively monitor their own external exposure, and leaked credentials or brand abuse often go unnoticed.

The impact is measurable. A significant share of cyber incidents originates from vulnerabilities in external systems. Yet many organizations still do not systematically include external assets in their security strategy.

When detection does not lead to action

Even when external risks are identified, many organizations struggle to act. Security teams are small or overstretched. Findings lack prioritization. False positives consume time. There is often no clear security architecture defining what "secure" actually means for internet-facing systems. IT teams balance operations, availability, and security, while investigations remain manual and fragmented.

As a result, risks are detected but not resolved. Findings remain isolated. Decisions are delayed. Exposure silently increases. This gap between visibility and action is one of the central challenges of modern cybersecurity.

Rethinking external security

This challenge cannot be solved by extending internal security tools to the internet. External Attack Assessment starts from a different premise: what is actually visible, reachable, and exploitable from the public internet — independent of internal assumptions or static inventories. Graydaxe was built around this approach. Using multi-stage discovery and automated asset validation, externally exposed attack surfaces become visible with high accuracy. Active and passive analysis methods are combined to evaluate risks based on technical exposure, exploitability indicators, and real-world threat intelligence. An independent risk methodology helps establish clear priorities instead of overwhelming teams with raw findings. This approach is industry-agnostic: everything that communicates via TCP/IP can be assessed, including complex and sensitive environments such as aerospace and satellite infrastructure.

From assumptions to resilience

As external attack surfaces continue to grow, cybersecurity can no longer rely on assumptions or static inventories. Organizations need continuous visibility, clear priorities, and the ability to act before hackers can exploit vulnerabilities and cause damage.

Managing external attack surfaces is therefore not an additional layer of security, but a fundamental capability for modern cyber resilience.

André Beran
Co-Founder & CEO
Graydaxe Cybersecurity GmbH

Rethinking Access Security: Why Traditional Password Managers Fail Most Teams

An article by heylogin

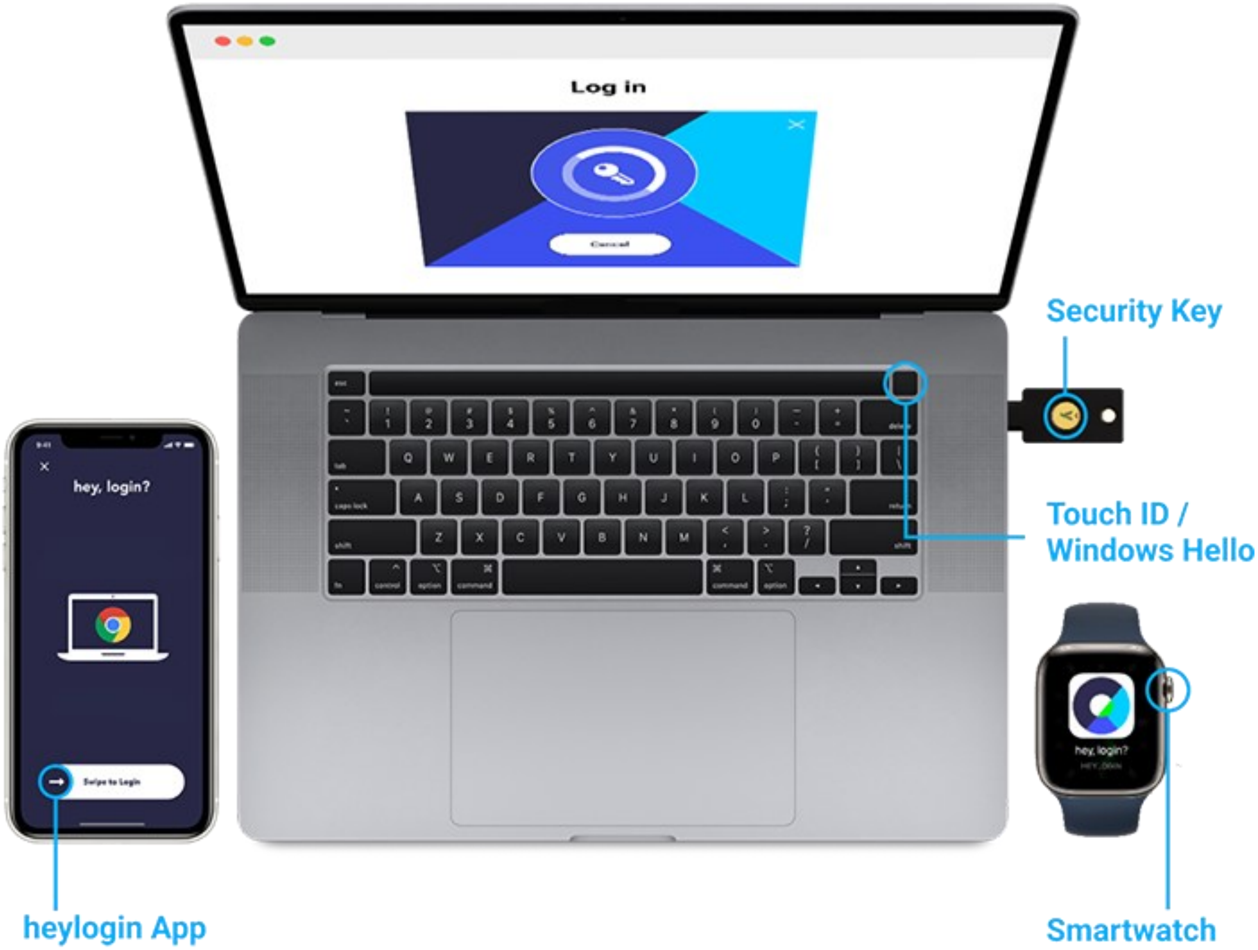


Image credit: © heylogin GmbH

Credentials are still the most common entry point for attackers - and the tools meant to protect them aren't keeping up. Phishing, password reuse, MFA fatigue, and credential stuffing are all still on the rise. A big part of the problem?

Most employees never adopt password managers. Why? Because traditional password managers weren't built for normal people. They're clunky, require training, and introduce friction into daily So people default to insecure habits: sticky notes, Excel lists, reused passwords, or messaging login credentials to colleagues.

This isn't just a user issue - it's a UX issue. Even in companies that roll out password managers, usage is often limited to tech teams. The rest of the organization is left behind, still vulnerable, still unprotected.

Shift towards passwordless intuitive access

There's a clear shift away from legacy tools and toward passwordless, intuitive access. FIDO2, biometric logins, and access orchestration are replacing the old "vault" model. Organizations are recognizing that real security starts with usability - if people don't adopt a tool, it can't protect anything.

At the same time, security and IT teams are demanding more control: automated onboarding and offboarding, audit logs, and zero shared secrets. The idea isn't just to lock down access, but to make it manageable, scalable, and invisible in daily workflows.

Security solutions are also becoming more people-centric. Not everyone is a tech expert - and they shouldn't have to be. Tools need to work out of the box for support staff, sales reps, external contractors - anyone who needs secure access, without needing a security briefing.

How heylogin solves these challenges today

Unlike traditional password managers, heylogin offers a unique login experience:
Just one click in the browser, and confirmation via Face Unlock, fingerprint, or PIN on your phone.

No master password. No typing. And 2FA is built-in by design - not bolted on as an extra layer. This makes heylogin radically easier to adopt across your entire team - especially for non-tech users. It feels more like using Apple Pay than using a password manager.

Fast, secure, and seamless or IT, heylogin gives full visibility and control. You can assign, revoke, and monitor access instantly - with no shared credentials and no risky workarounds. Shared logins can be managed with proper audit trails. Offboarding someone is just one click. And because heylogin runs via a browser extension, it integrates cleanly into everyday workflows without disrupting how people work.

In short: where password managers store secrets, heylogin manages access - the way it should be.

Dr. Dominik Schürmann
CEO & Co-Founder
heylogin GmbH

Why the Modern Threat Landscape Demands a Defense-in-Depth Approach

Are your employees and devices truly protected against today's sophisticated cyber threats?

An article by Jamf

Image resource: Jamf

Rapid workplace mobility, sophisticated cyberattacks, and the growing use of connected devices are creating new security challenges for businesses. Jamf helps organizations meet these challenges by combining device management, endpoint security, and identity controls in a comprehensive defense-in-depth approach.

Welcome to the Modern Landscape

Employees now work from anywhere, accessing corporate resources from smartphones, tablets, and wearables over wireless networks. While this mobility enhances productivity, it also increases exposure to cyber threats. Attackers are leveraging AI-driven deepfakes, phishing, and sophisticated malware to exploit vulnerabilities across endpoints. Traditional perimeter defenses are no longer sufficient. Organizations need a strategy that protects every user, device, and connection—this is the essence of defense-in-depth.

Holistic Approach to Cybersecurity: Defense-in-Depth

Defense-in-depth is a layered security philosophy, combining device management, endpoint protection, identity and access controls, and continuous monitoring. This approach reduces single points of failure and creates multiple barriers to potential attacks. Mobile devices, often the most vulnerable, are secured alongside desktops and cloud resources. By integrating human behavior considerations with technology, organizations can better protect against both AI-driven and human-targeted threats.

One Step Closer with Our Guide

Standalone tools and perimeter-based defenses are no longer enough. Jamf's guide to defense-in-depth demonstrates how an integrated security framework strengthens enterprise resilience, secures Macs and other devices, and adapts policies to modern work patterns. By monitoring activity, enforcing controls, and safeguarding endpoints, IT and security teams can move from reactive defense to proactive protection—keeping organizations secure in a rapidly evolving threat landscape.

Adam Boynton
Enterprise Strategy
Manager
Jamf

Save the Date

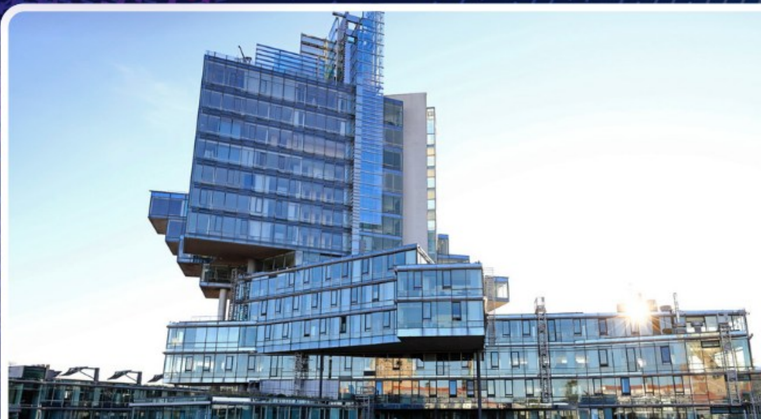
AI & SOFTWARE SUMMIT

Join us on June 18, 2026, at Nord/LB in Hanover for the AI & Software Summit 2026, where industry leaders, researchers, and startups will explore the future of artificial intelligence, software development, and regulation. Discover innovative insights, groundbreaking technologies, and the exciting finale of the German Startup Cup for AI & Software.

17/06/2026

9:00 AM

Norddeutsche Landesbank
Friedrichswall 10
30159 Hannover



Reduce cyber risk in your digital supply chain

Take control of supplier risk and secure your business success

An Article by LocateRisk

Image credit: © LocateRisk

AI-driven cyberattacks are now escalating faster than security teams can react. This is precisely where LocateRisk GmbH steps in with Cyber Vendor Risk Management (C-VRM), transforming cyber risk assessment within the supply chain. The result is a new level of quality in vendor assessments and time savings of up to 70 percent.

"Threats are becoming faster and more complex—often posing the greatest risk within the supply chain. Our goal is to reduce the attack surface across the entire ecosystem so that attacks fail. That's exactly why Cyber Vendor Risk Management (C-VRM) was developed," explains Marc Linman, Director of Business Development*.*

"The solution checks the IT compliance of suppliers, reports anomalies, and optimizes communication. It takes the pressure off IT and procurement managers while ensuring the security of the digital supply chain."

80 percent of all cyberattacks target small and medium-sized enterprises. Attackers exploit the weakest links in the supply chain as an entry point—an overlooked server at a supplier or a forgotten interface in the partner network is sufficient to bypass even strong security systems. Therefore, effective security means: continuously minimizing the attack surface across the entire digital ecosystem.

Catching Up in Strategic Risk Management

While US companies have long established the monitoring of assets and third-party relationships, German companies often show significant deficits in Cyber Vendor Risk Management (C-VRM). Less than one-third of German companies continuously monitor third-party relationships for cyber risks—lagging significantly behind competitors in the UK and US, for example. For good reason, EU regulations are now making IT security a C-level priority. Responsibility now lies directly with the board and executive management. Security gaps are no longer minor operational errors, but a strategic risk for the entire company.

From "Point-in-Time" Compliance to "Continuous Assurance"

A wide range of regulations and standards—such as NIS-2, TISAX, DORA, ISO 27001, etc. —mandate the continuous monitoring of both internal and third-party IT attack surfaces as part of Vendor Risk Management (VRM). This approach is essential for identifying ecosystem anomalies in real-time and mitigating risks. But what does this look like in practice?

"Security must not be a bureaucratic night-mare. That is why we have maximally automated and digitalized the risk assessment process. LocateRisk enables results that are three times more insightful than conventional methods, saves an extreme amount of time, and provides audit-proof evidence at any time," says Lukas Baumann, Chief Executive Officer at LocateRisk.
"Furthermore, the solution is easily scalable to hundreds of suppliers."

The value is created through intelligent data aggregation and contextualization: automatically identified systems undergo security checks for outdated applications, Shadow IT, misconfigurations, and open ports, among other vectors. Identified risks are cross-referenced with regulatory frameworks, prioritized as technical vulnerabilities, and clearly documented with actionable recommendations in compliance status reports. Combined with digitalized questionnaires, these automated analyses reduce audit effort by up to 70 percent compared to manual assessment procedures.

Technology as an Enabler: Cyber Vendor Risk Management "Made in Germany"

The complexity of digital supply chains continues to increase—but with the right technology, Vendor Risk Management becomes transparent and controllable. LocateRisk combines automated IT risk scans, digital compliance questionnaires, and powerful benchmarking functions into a scalable platform for preventive cybersecurity.

The central performance dashboard visualizes the IT security posture of business partners at a glance: criticality, IT risk scores, compliance status, and changes are continuously recorded and clearly displayed. This allows companies to keep their supply chain in view, recognize critical developments early, and act proactively.

Kristina Breuer
Corporate
Communications
LocateRisk GmbH
press@locaterisk.com

Detailed information in the techL profile:
LocateRisk

Cyber insurance as an essential part of risk management

Ongoing digitalization and the rapid development of artificial intelligence are creating new opportunities across all industries. At the same time, technological progress is giving rise to new risks that organizations have to address proactively. Alongside a robust IT infrastructure, security measures and employee awareness, cyber insurance has become a key component of a comprehensive cyber risk management strategy.

An Article by CyberDirekt

Image credit: © canva/ Getty Images

What is cyber insurance?

Cyber insurance is a specialized insurance solution that protects companies and organizations against financial losses resulting from cyber attacks, cyber fraud, or IT security incidents. Coverage typically includes both first-party losses and damages suffered by third parties.

Cyber insurance policies cover a wide range of digital risks, including data loss, system outages, ransomware attacks, data protection violations, and cyber extortion. Insured costs may include expenses for restoring data and IT systems, crisis management services including PR consulting and legal support, liability claims from customers or business partners, and—depending on the policy—ransom payments in the event of extortion.

Beyond financial protection, many cyber insurance policies also offer preventive services. These include risk assessments, vulnerability scans, advisory services to improve IT security, and access to specialized security experts who provide professional incident response support in the event of an attack.

What does cyber insurance cover?

Hackers and organized criminal groups are becoming increasingly professional, and their attack methods more sophisticated. As a result, companies of all sizes and across all industries are increasingly targeted by cybercriminals. The resulting damage can be substantial and, in extreme cases, pose an existential threat to an organization.

Cyber insurance primarily protects against the financial consequences of a cyber incident. These include revenue losses caused by business interruption, costs for restoring IT systems and data, as well as expenses for legal advice, potential regulatory fines resulting from data protection violations, and other liability claims.

In addition, cyber insurance provides companies with rapid and professional support in the event of an incident. A structured incident response is essential to contain attacks, close security gaps, and restore business operations as quickly as possible. Policyholders gain access to a network of IT security, forensic, and crisis management experts who assist in managing and mitigating the incident.

Protecting corporate reputation is another critical aspect. The loss of sensitive customer data in particular can severely and long-term damage the trust of customers and business partners. Cyber insurance helps limit reputational damage by providing professional crisis management, communication support, and PR consulting. Transparent and well-controlled communication can be crucial in restoring public trust and minimizing long-term reputational harm.

Why cyber insurance benefits all types of business

Cyber attacks on large corporations often attract media attention. However, small and medium-sized enterprises are increasingly targeted by cybercriminals, as they typically have fewer security resources and are perceived as easier targets.

Cyber insurance is therefore a sensible investment in security for nearly all companies—including those with well-developed IT infrastructures. No system is completely secure. In an increasingly interconnected world, cyber risks can never be entirely eliminated. Cyber insurance protects against difficult-to-calculate consequential losses that can quickly become existential threats in the event of an attack.

Hanno Pingsmann
Founder & Managing Director
CyberDirekt GmbH

Cyber Resilience Becomes Mandatory: EU Regulation Accelerates Industrial Security

From 2027 onwards, connected machines and devices will only be permitted to operate within the EU if they can demonstrate cyber resilience. Organizations that underestimate the new Cyber Resilience Act risk multimillion-euro fines, personal liability for executives, and ultimately, a loss of competitiveness in European and global markets.

An Article by ONEKEY

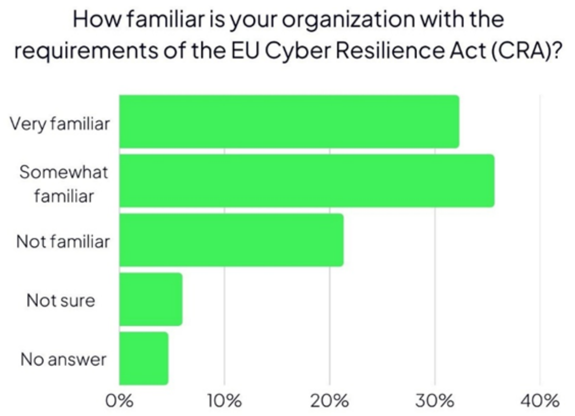


Image credit: IoT & OT Cybersecurity Report 2025, powered by ONEKEY I n=300

With the EU Cyber Resilience Act (CRA), Brussels is tightening the security screws considerably. From fall 2026, the first binding requirements will apply; from 2027 onward, connected devices, machines, and systems may only be used if they comply with the CRA. For machinery and plant manufacturers, this means end-to-end product security from development and assembly through operation and remote maintenance – backed by documented processes, evidence, and clearly defined responsibilities.

The sanctions are tough. Violations can result in fines of up to 15 million euros or 2.5 percent of global annual revenue, whichever is higher. In addition, managing directors and board members can be held personally liable. In practice, this means that projects, approvals, and market access can stall if CRA compliance cannot be demonstrated.

The 'IoT & OT Cybersecurity Report 2025' by security provider ONEKEY illustrates the current state of the industry. Of the 300 German industrial companies surveyed, 32 percent are thoroughly familiar with the CRA requirements. 36 percent have looked into them while 27 percent have not dealt with them. 14 percent have launched comprehensive implementation programs, 38 percent have taken initial steps and an equal proportion has done nothing so far. Still, the report shows tangible movement: more than 40 percent have set up cross-functional working groups or dedicated CRA teams, and 44 percent are engaged with the SBOM topic. The message for machinery manufacturers is clear: establish CRA roadmaps through to 2027, schedule testing and documentation, and involve suppliers early on—especially given typical development cycles of two to three years.

At the heart of the CRA lies the principle of 'security by design and by default', meaning that products must be designed securely from the outset and protected throughout their entire life cycle. This includes access control, data integrity, availability preservation, and mandatory security updates. Any exploited vulnerabilities or serious incidents must be reported within 24 hours, and all security-relevant information must be consolidated in traceable documentation.

A critical building block is the Software Bill of Materials (SBOM). It provides transparency regarding all software components and their vulnerabilities and is therefore central to both security and compliance. The report shows that SBOM adoption is underway: 44 percent of companies are engaged with SBOM, and 32 percent have already created one for some connected devices, machines, and systems. Full coverage is still limited—12 percent have SBOMs across all affected products, while about a quarter have not created one yet, often due to legacy systems, proprietary components, and complex supply chains. At the same time, pressure is rising: in 2025, more than 48,000 new vulnerabilities were reported. The implication is clear: SBOMs are not a one-off deliverable, but an ongoing responsibility—because not knowing about a vulnerability does not remove liability.

The report also indicates that standards alignment must be expanded further. Only 27 percent of companies consider IEC 62443-4-2, a core foundation for CRA compliance in industrial environments that defines security requirements for industrial automation and control components. About a quarter rely on the harmonized IoT standard ETSI EN 303 645, which sets 13 requirements and can support CE marking and CRA conformity. RED (EN 18031) is factored in by 16 percent, despite being essential for connected radio modules in machines, sensors, and tools.

Organizationally, the picture is equally diverse. 46 percent of respondents assign responsibility for CRA implementation to IT security, with further shares distributed across compliance, executive management, legal, and product development—underscoring how broadly the CRA cuts across technical, operational, and governance tasks. Team sizes range from small units to double-digit headcounts. To avoid gaps between departments, companies should establish clear end-to-end ownership and escalation paths so that requirements are executed consistently across all affected products.

Training is another area in which many companies are currently lacking. Fewer than one in three organizations trains its employees on the CRA at least once a year, while another 28 percent consider intervals of one to two years to be sufficient. Given the technical and legal complexity of the regulation, regular training is essential to ensure clean processes, complete documentation and consistency across the board.

One thing is certain: the industry is moving in the right direction, but time is running out. The CRA is an EU regulation, not a directive, so it becomes directly applicable law without the delay of a national transposition process, as was seen with NIS2. Meanwhile, the real impact of cybercrime continues to grow. In Germany alone, cyber incidents caused an estimated €178.6 billion in damages in 2024. Companies that accelerate their efforts now, embed CRA requirements systematically into development, production, and service, and actively involve their supply chain will secure market access from 2027 onward and strengthen their long-term cyber resilience.

Jan Wendenburg
CEO
ONEKEY GmbH

How increased security with passkeys also works as your compliance driver

Is it possible to combine phishing-resistant security with user-friendliness while adapting to new regulations? Implementing passkeys at an enterprise scale could be the silver bullet, solving all three in one go.

An article by Pointsharp

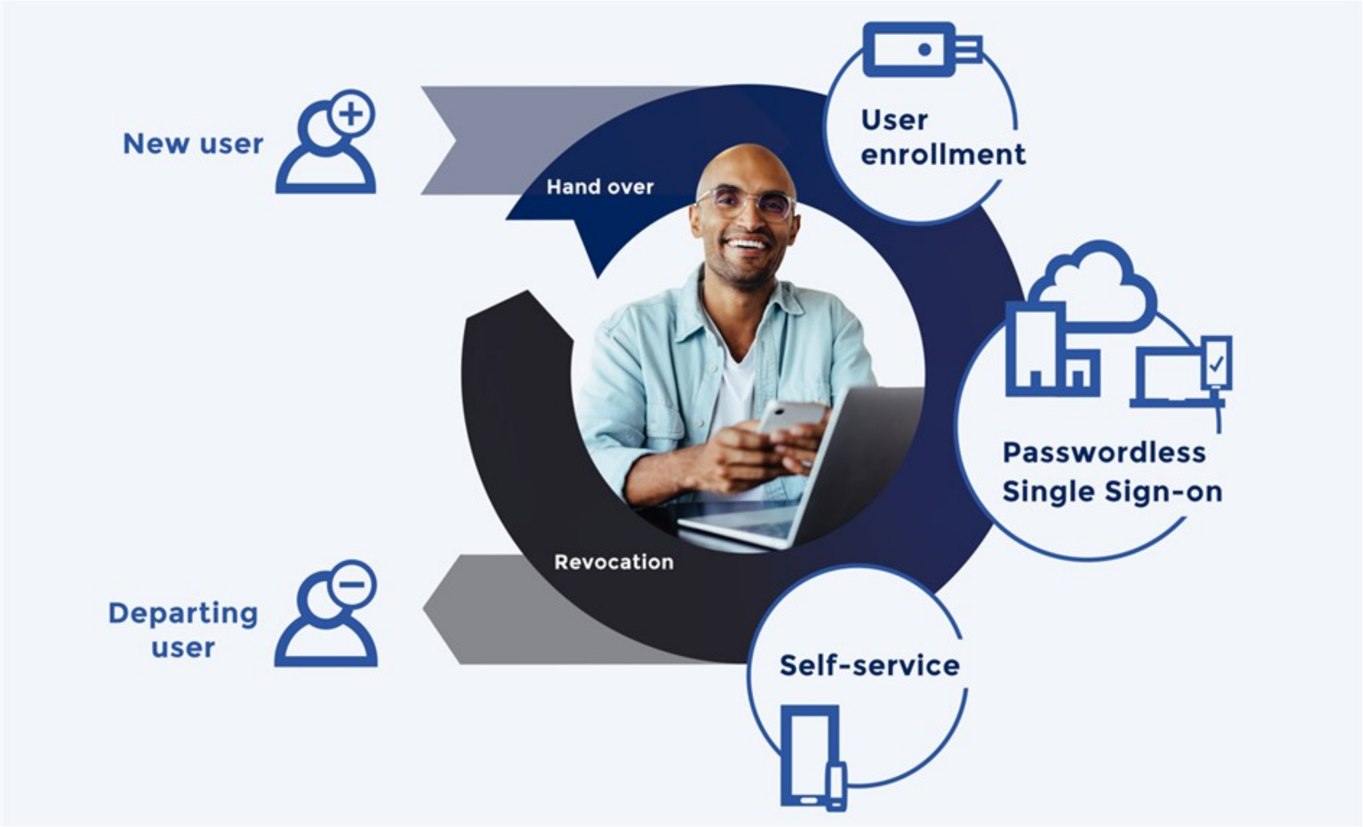


Image source: © Pointsharp

NIS2, DORA, and other upcoming regulations, such as the Cyber Resilience Act, have raised the bar for what organizations are expected to do in terms of security measures, risk management, and resilience. These measures are very much needed, especially as phishing attacks continue to grow in scale and number each year.

An effective measure for becoming phishing-resistant is FIDO2-based passkeys. Implementing passkey authentication measurably decreases credential-based incidents wherever it is implemented. However, passkeys are designed primarily for personal use. Adopting passkeys for your personal accounts can be done with just a few clicks. While this is great, it does not apply to enterprise use.

Turning passkeys from personal to organizational

As an organization, it would not be wise to allow your users to connect their personal passkeys to company resources. However, passkeys can be deployed within an organization using modern access management solutions, combining enterprise control with the security and simplicity of private passkey use. As a welcome side effect, compliance with strong authentication, audit trails, and risk management comes included.

If we look at passkeys from a business-need perspective, there are a few things that need to be in place in an access management solution to create organizational IDs secured by passkeys.

- Register-and-enroll-on-behalf features simplify migration to passkeys for organizations with many users, while users receive keys that work out of the box.
- Pre-registration further simplifies the migration and onboarding of new users by registering specific keys with a user ID. This is especially important for remote users, as the key remains inactive until the right user activates it.
- Time-limited keys and tokens increase the security of the entire setup. All keys have a set time limit and will be deactivated unless regularly recertified.

The ability to set allowed tokens, down to specific security key models if needed, will further ensure that no rogue keys are circulating. Because all of these features are logged in the access management system, auditability for compliance purposes becomes much easier.

Take passkeys to the next level

Implementing passkey lifecycle management is just one part of the process. The next step is, of course, what the user can actually unlock with the passkey. Here, the answer really should be everything. Security is like a chain, only as strong as the weakest link. It is here that a modern access management solution turns from a great security measure and a tool for great user acceptance into a compliance driver for the entire organization.

By connecting the access management solution to every application, service, file server, and so on, you can have it serve as the connective tissue for the whole organization and use passkey authentication for everything.

For users, that means using only one easy authentication method for everything, creating familiarity and a sense of doing things the correct way.

For the organization, it means that every login, every granted access, and every connection has the same security level. It is also fully logged and auditable, and with an easy overview to see whether a user has excessive access rights and to automatically revoke access during offboarding.
Depending on your choice of access management solution and your infrastructure in general, you can easily extend this passkey support to on-premises resources, legacy applications without MFA support, and even Windows login, creating a fully unified login environment.

Enterprise passkeys are the fast track to compliance

Organizational changes never happen in a vacuum. Instead, changes in one area create ripple effects everywhere. That is especially true of enterprise passkey adoption through a modern access management solution. What might have started as a compliance project ends up simplifying the daily lives of admins and users alike. Or what might have started as a need for better security can take great strides toward regulatory compliance.

Matthias Kess
Head of Product Management
Pointsharp

Together, but secure. Secure, but together.

02:14 a.m. An incident alert pops up – who decides true positive or false alarm, and triggers containment before lateral movement begins? Why a partnership-based SOC makes organisations faster, safer, and more resilient.

An article by Proact Deutschland

Image source: ©Proact

Why a partnership-based SOC makes organisations faster, safer, and more resilient

Security isn't a slide, an audit, or a 9-to-5 task – it's a 24/7 responsibility. So here's the question: at 02:14 a.m., who is watching your SIEM, EDR, and XDR, deciding whether a signal is noise or an active compromise, locking a suspicious account before lateral movement begins, and making sure your posture improves week after week as attackers evolve? For too many teams, the honest answer is somewhere between "no one" and "we do our best." That's the real problem: tools don't secure environments – operations do. A Security Operations Center (SOC) exists to close that gap.

Build vs. buy: why neither is enough

Building your own SOC looks great on paper – full control, full visibility, unlimited customisation. In practice it needs six to nine FTE for 24/7 coverage, rare, costly skills, ongoing use-case development and tuning, log hygiene, and daily care of connectors, parsers, normalisation and enrichment – plus a cultural shift across IT. Timelines get long, costs get high, and the operational load is heavy.

Traditional MSSP models promise the opposite: quick onboarding, fixed pricing, predefined processes. You often get shallow context, generic detections that miss what matters, inconsistent escalations and slow, opaque feedback loops. You don't feel like a partner – you feel like a ticket in a queue. Blind spots grow, dependency deepens, and internal maturity stalls.

A partnership SOC: operated for you – built with you

There is a third way. Our model blends 24/7 monitoring and incident response with your business context and decision rights. We run operations – triage, investigation, response and use -case management – while you retain risk ownership and architectural control. No black boxes, no hand-offs into the void: just a clear, auditable interface where action is fast, precise and accountable.

Because we bring platform, engineering and experience, we get you secure and operational in weeks, not years. Yet nothing is one-size-fits-all: detections, playbooks and escalation paths are tailored to your tenant, risk posture and processes. You gain speed without losing control.

Most importantly, capability grows on your side, not ours alone. We co-engineer use cases, review detections together, share playbooks openly and run improvement sessions that turn lessons into better coverage. Your teams learn to interpret and act on findings; expertise accumulates in-house. We don't replace your team – we elevate it.

This approach avoids the outsourcing trap. The people watching your signals are the same people who understand your architecture, crown-jewel processes and what "normal" looks like at 02:14 a.m. That continuity turns speed into accuracy – and accuracy into trust. It also scales at your pace and budget: start focused, prove value quickly, then add sources and automation where risk justifies it. Security becomes a living process – detect, learn, improve – measured by fewer false positives, faster containment, clearer accountability and a posture that strengthens every week.

Security isn't bought – it's built together. A SOC isn't something you unbox or a dashboard you glance at; it's an operating model and a shared responsibility that turns tools into outcomes. Side by side, we turn detection into decisions, incidents into improvements and pressure into resilience.

Together, but secure. Secure, but together.

Anja Hünnekes
IT Solution Architect
Security
Proact Deutschland
GmbH

Secure contact management as a critical factor in cybersecurity

Why companies will no longer be able to do without SECURE CONTACTS APP in 2026

At a time when cyberattacks, data misuse, and regulatory requirements are constantly increasing, companies face an often underestimated threat: the insecure management of business contacts on smartphones. BYOD and COPE models in particular increase the risk of confidential contact data unintentionally flowing into external systems – such as Apple, Google, WhatsApp, or rental car synchronization services. This is exactly where the Secure Contacts app comes in, providing a comprehensive, GDPR-compliant solution for the secure handling of business contacts.

An article by Provectus Software

The problem: contact management as a security vulnerability

Smartphones automatically synchronize contacts with commercial platforms. According to the GDPR, this is highly problematic for business contacts, as unwanted data leakage can cause legal and economic damage. Traditional contact apps offer little control over where data is transferred to, thus opening up an often overlooked point of entry into the corporate network.

The solution: Secure Contacts – data protection and usability in one app

The Secure Contacts app brings together all business contacts from Outlook, Microsoft Teams, CRM systems, company address books, and other sources in a single, encrypted, and isolated environment. The data is never synchronized with third-party platforms.

Key security features

GDPR-compliant storage of all contacts

No unauthorized synchronization with Apple, Google, WhatsApp, or other platforms.

256-bit AES encryption & access protection

Secure with PIN, Face ID, or Touch ID.

No data collection, no tracking

The app itself does not collect any user data.

Serverless architecture & full integration with Microsoft Azure / Intune

Manageable with Intune, including remote deletion and centralized rights management.

Efficiency and convenience without compromise

Cybersecurity should not be an obstacle to everyday work. Secure Contacts therefore combines security with a noticeable increase in efficiency.

Key productivity features

- Automatic synchronization & data maintenance
- No more manual contact maintenance.
- Caller ID via Outlook, Teams & CRM
- Increases security and productivity for incoming calls.
- Siri, CarPlay & Android Auto integration
- Safe to use – even on the go.

Image source: © Provectus Software GmbH

- vCard & QR scan for new contacts
- Fast and secure contact management.
- Vacation/absence function
- Only calls from favorites are allowed – real protection against social engineering.

Protection against social engineering & data leakage
In 2026, social engineering will continue to be one of the biggest threats. Hackers use contact information to fake identities or target specific employees.

Secure Contacts prevents this by:
isolated data storage, no transfer to messenger services, anonymous calls directly from the app, support for secure company policies through MDM systems.

Microsoft-Integration als strategischer Vorteil
Secure Contacts is fully embedded in the Microsoft 365/Azure environment. Companies that rely on Microsoft benefit from:

- Single sign-on (Entra ID),
- Intune-based policy control,
- Teams status display directly in the app.

Conclusion: Contact management is becoming the number one cybersecurity issue
While many companies implement firewalls, endpoint security, and zero trust models, one critical aspect often remains unprotected: their employees' contacts. Secure Contacts closes this gap.

The app offers:

- Maximum security,
- Full GDPR compliance,
- High efficiency and user-friendliness,
- Seamless integration into existing Microsoft infrastructures.

This makes it an indispensable component of modern cybersecurity strategies.

Jan Gombert
Channel Manager
Provectus Software GmbH

Post-Quantum Cryptography in Industry: Why Acting Now Matters

An article by secunet

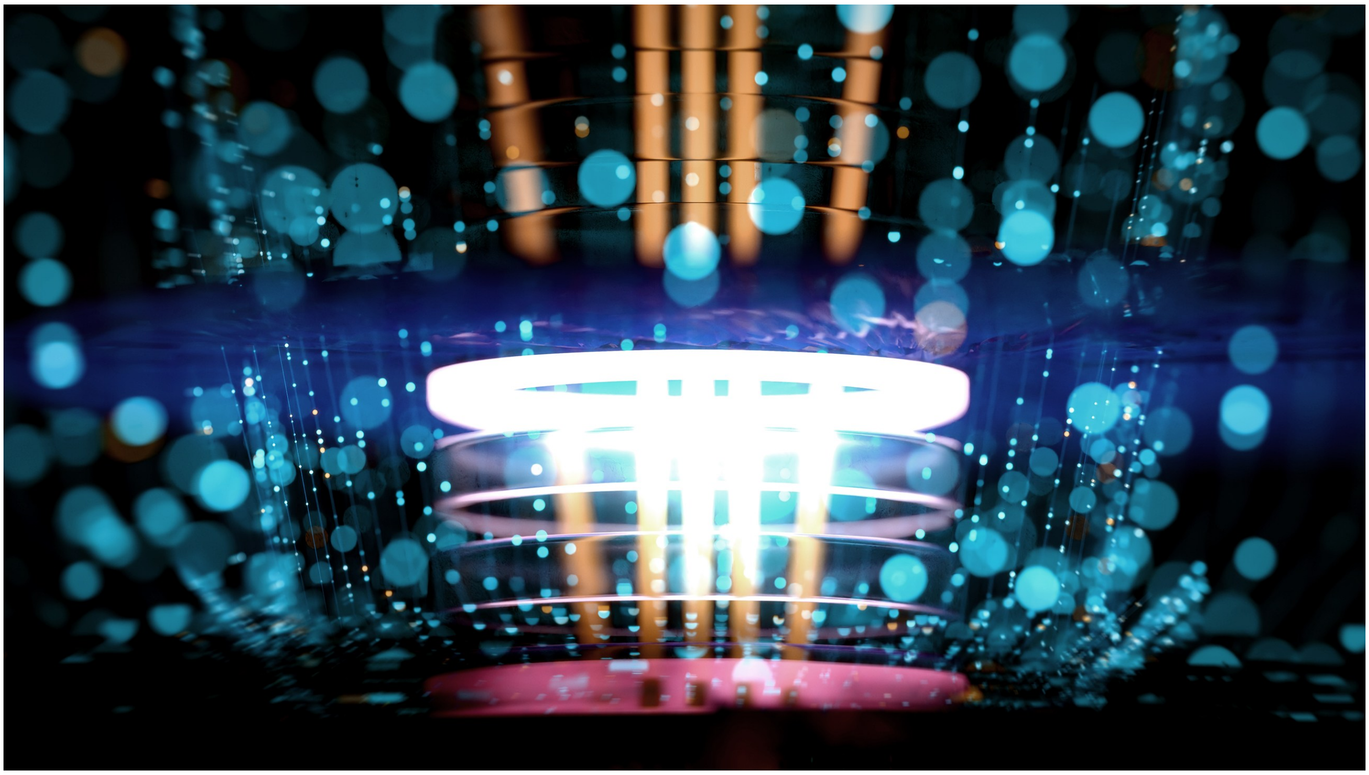


Image credit: ©Getty Images/koto_feja

Last summer, the European Union took a further step by publishing the “Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography,” bringing the potential threat of quantum computing to the attention of business leaders and CISOs. Developed collaboratively under the auspices of the NIS Cooperation Group, authorities from several EU Member States and their national cybersecurity agencies (e.g., Germany’s Federal Office for Information Security and France’s National Agency for the Security of Information Systems) set out a high-level path toward a future in which IT systems can be considered quantum-safe.

The roadmap outlines a transition timeline, “first steps” and “next steps,” and an approach for assessing risks posed by a sufficiently capable quantum computer. For high-risk use cases, it proposes completing the transition to postquantum cryptography by the end of 2030, while aiming to transition all feasible systems no later than 2035. Importantly, the roadmap addresses not only public authorities, but also enterprises, particularly operators classified as critical infrastructure.

Another major development in the regulatory landscape is the Cyber Resilience Act (CRA). It requires appropriate measures for products with digital elements to ensure authenticity, integrity, and (where applicable) confidentiality for example, for secure firmware updates from the end of 2027 onward.

Taken together, these recommendations, requirements, and timelines create regulatory pressure and push companies to start post-quantum migration now rather than later. In the industrial sector, common challenges arise from product characteristics and lifecycle constraints. Unlike typical IT environments, where systems are usually online, centrally managed, and equipped with ample compute resources, industrial devices are often deployed in the field, bound to hardware chosen at production time, and not always designed to support smooth upgrades to new cryptographic standards. In addition, post-quantum (or hybrid) algorithms can introduce practical overheads that matter acutely in embedded and real-time contexts: larger message sizes, increased handshake latency, higher memory footprint (RAM/flash), and limited availability of hardware acceleration for the new primitives. These constraints may be unacceptable for low-latency and high-throughput industrial use cases, even if they are manageable for common web workloads.

Public key infrastructures (PKIs) require particularly careful planning and early action. They often rely on long-lived certificates (e.g., 10 to 20 years), which can make it difficult to complete a PQC transition in time. The situation is further complicated when devices and firmware are not yet prepared for certificate re-enrollment or large-scale credential rotation. Compounding the problem, many companies do not have full visibility into their cryptographic toolset and lack continuous monitoring of their PKI and cryptographic dependencies.

This is why many recommendations start with establishing a cryptographic inventory across IT and OT networks, including deployed products and their software components. While there are many tools and approaches to build such an inventory, visibility is only the starting point. Because cryptographic mechanisms are often deeply embedded and highly interdependent, defining a safe and practical migration order remains challenging. Finally, the effort required to prepare products for migration- i.e., to make them truly crypto-agile, is often underestimated.

The EU has outlined an ambitious roadmap for the transition to post-quantum cryptography. Industry should use this window to prioritize crypto inventories, establish crypto-agility, and plan phased migrations for the most critical and long-lived.

Dr. Nils Abeling
Senior Consultant
secunet Security Networks AG

The backup paradox – why perceived security could be your biggest vulnerability

An article by Rubrik

Today, companies need to think beyond traditional backup strategies and ensure that their data remains secure and available, regardless of the circumstances. Attacks on SaaS applications in particular have increased significantly, driving a shift towards cloud-based data protection. Gartner predicts that by 2028, 75 per cent of large enterprises will prioritize SaaS backups, compared to only 15 per cent today. This reflects a growing awareness that traditional backup solutions alone are not sufficient against modern cyber threats.

1. Thinking beyond backups

Cyber resilience means not only being able to defend against attacks but also being able to quickly return to full operational capacity during and after an incident and maintain critical business processes. After all, it is not a question of 'if' but 'when' an attack will occur. That is why a holistic approach to cybersecurity is crucial. By identifying and protecting key business processes, detecting threats early and implementing rapid response mechanisms, you can ensure that your organization remains operational even in the event of an attack.

2. Integration of artificial intelligence (AI)

AI plays a crucial role in improving cybersecurity – but it also brings new challenges. While AI-powered security systems can automate threat detection and defense, cyber criminals are also using AI to develop sophisticated attacks – such as automated phishing or adaptive malware. To effectively counter these threats, organizations should not only use AI for defense, but also to predict, counter and neutralize AI-based attacks in real time. This proactive strategy can strengthen overall cyber resilience and ensure that organizations are always one step ahead of both human and AI-driven attackers.

3. Zero Trust approach

Another key element of cyber resilience is the introduction of a Zero Trust security model, which operates on the principle of 'never trust, always verify'. Essentially, this means that every user, every device and every application is initially regarded as a potential threat, regardless of its origin. This approach can drastically reduce the risk of internal attacks and ensures that only authenticated and authorized entities gain access to critical data and systems.

A cyber resilience strategy to resolve the paradox

At Rubrik, too, backups were only the starting point on the journey from start-up to NASDAQ-listed company. Evolving attack patterns quickly made it clear that data backups alone are not enough and that a comprehensive approach to cyber resilience is essential to reliably protect data and effectively leverage today's AI transformation. After all, a strong cyber resilience strategy goes beyond backup and recovery – it includes

Image credit: © Getty Images

continuous testing, real-time threat detection and a proactive approach to security. Backup systems must be tested and validated regularly to ensure that they function reliably in an emergency.

It is not enough to simply back up data – it is important to evaluate the integrity of backups and recovery processes through continuous simulation of real cyber attacks. This is the only way to ensure that the organization is truly prepared for the worst-case scenario. To counter modern, increasingly sophisticated cyber threats, companies must implement AI-driven monitoring systems that are capable of detecting threats in real time. Such systems can identify unusual behavior patterns, highlight vulnerabilities and respond to attacks faster than would be possible manually. Real-time monitoring ensures that threats are detected and neutralized before they cause serious damage.

How can we resolve the paradox of a false sense of security? Looking ahead, it is clear that companies can no longer afford to view backups as their sole data security strategy. To effectively counter the rapidly changing threat landscape, a comprehensive cyber resilience strategy is required – with a focus on prevention, detection and rapid recovery. Cyber resilience is not just a strategic advantage – it is a necessity for survival in today's threat landscape. That's why we should not rely solely on backups, but actively embrace resilience and take the necessary steps to protect what really matters: our data, our business and our future.

Frank Schwaak
Field CTO EMEA
Rubrik

Building Resilient Cyber Defenses With Zero Trust

An article by ThreatLocker

Image source: GETTY

When Forrester developed its Zero Trust model in 2009, it didn't take off overnight. According to Okta, in 2021, less than a quarter (24%) of all organizations had a Zero Trust framework in place. But just two years later in 2023, that number had grown to 61%. I've seen more and more organizations view Zero Trust as a necessity, especially with government mandates pushing its adoption forward.

However, it's important to understand that Zero Trust isn't about eliminating all trust; it's about adopting a 'least privilege' mindset. Zero Trust means granting access only when necessary, to minimize the attack surfaces in an organization.

But why and how should organizations start thinking about Zero Trust implementation today?

The Evolution Of Zero Trust

In the high-profile SolarWinds breach of 2019, attackers compromised the SolarWinds software, infiltrating numerous governmental and private organizations. This case brought the importance of Zero Trust back to the public sphere, nearly 10 years after the term was invented. If organizations had restricted SolarWinds' access to only necessary resources, like preventing it from reaching the internet, it would have greatly limited the attack's impact.

Instead of trusting everything by default, access in a Zero Trust framework is limited to only what users and applications require to perform their jobs. This goes beyond controlling network traffic.

It includes managing who and what can access applications, files, and data.

Reflecting on the early days of the internet, it's astonishing to me how open our systems were. Computers had all ports accessible, making them a playground for hackers. Then, firewalls were introduced to block unnecessary access by restricting inbound traffic. Similarly, early mail servers were open relays, which led to rampant spam. Closing these relays made email communication safer and more reliable. These historical shifts underscore the trend of moving from open access to more controlled environments.

Following the devastating Colonial Pipeline ransomware attack in May 2021, the U.S. administration recognized the urgent need to strengthen the nation's cybersecurity infrastructure by issuing an executive order in May 2021 titled "Improving the Nation's Cybersecurity." This executive order mandates that all federal agencies advance towards Zero Trust architectures by adopting strict access controls, continuous monitoring and robust authentication measures.

Successful Zero Trust Adoption

Today, Zero Trust solutions require about the same effort as traditional cybersecurity to get started. The major difference is Zero Trust requires a mindset shift. Instead of security running in the background, organizations must limit individual access and the pathways applications are allowed to take. Take a simple password manager, for example. It might need to interact with the command prompt to function correctly. While these exceptions are necessary, they must be as narrow as possible in the event that the individual's device is compromised. Blocking any unwanted access before a threat occurs is the best and fastest way to reduce an organization's risks. Better yet, these risks are mitigated without the company having to invest in detection technologies upfront.

We recently helped a financial firm implement a Zero Trust approach to securing their systems. By segmenting their network and strictly controlling access to sensitive financial data, they quickly isolated the malware. This fast action prevented it from spreading to critical systems and avoiding significant financial loss.

To put it in clear terms, I see Zero Trust adoption involving the following key strategies:

- **Take Proactive Measures To Limit User Access**

Allowlisting policies can stop malicious software or unwanted software from running in the first place, this can stop legitimate tools such as Teamviewer which are often used by cybercriminals. When untrusted applications are denied, attackers may try to turn to the features of permitted tools such as PowerShell, but organizations can limit those tools' access with restrictions, such as internet access or access to data on your systems, halting the attack before it spreads further.

- **Give Permissions Based On Roles**

When organizations can't deploy proactive measures to limit user access, they should implement role-based access control (RBAC) to assign permissions based on user roles. Only the payroll staff should access the payroll system, not everyone in the company. Additionally, software on your computers should access only the data it needs. If an application has a backdoor or vulnerability, its strictly controlled permissions prevent it from becoming an entry point into your environment.

- **Reduce Any Broad Exceptions**

Avoid broad exceptions by using tools that allow for specific, narrow exceptions. This prevents attackers from exploiting overly broad permissions and keeps your security robust even when exceptions are necessary. Each exception should be justified and closely monitored to maintain the integrity of your security framework. Broad exceptions can undermine the entire security framework, creating loopholes that attackers can exploit.

- **Layer Security Measures**

Using methods like application separation, Endpoint Detection and Response (EDR) and dynamic access controls create multiple barriers against intruders. If one security layer is breached, others remain to protect the system, providing comprehensive defense against new and emerging threats.

- **Ongoing Vigilance And Training**

Zero Trust isn't a set-and-forget solution; it's an ongoing process. Regularly review and adjust access controls to keep up with emerging threats and organizational changes. Continuous monitoring and regular audits are vital to ensure that your security measures evolve alongside the threat landscape.

Overcoming The Challenges Of Zero Trust Implementation

One challenge I’ve observed over the years in helping organizations transition towards Zero Trust is setting up precise access controls for various applications and data.

This is most apparent with legacy companies, because it requires a larger cultural change to drive adoption. Employees who are used to having broad access may struggle to adjust to more restrictive protocols. This shift requires comprehensive training and a fundamental change in mindset across the organization.

Moreover, the variety of cyber threats adds another layer of complexity. Nation-state attacks, unlike typical ransomware incidents, aim to gather intelligence and maintain long-term access rather than just extort money. This demands strategies that are resilient and able to effectively counter diverse and evolving threats.

Adopting Zero Trust requires a cultural shift within the organization. Organizations can foster a security-first mindset and educate employees about the importance of Zero Trust and how it protects both the organization and their personal data. Ensuring the user understands the importance of the new procedures will help employees adapt to new security protocols, reducing resistance and ensuring smooth implementation.

Building a resilient security framework is essential. By restricting trust and rigorously managing access, organizations can protect their systems from all threats, whether known or unknown.

Danny Jenkins
CEO and Co-Founder
ThreatLocker

United
Innovations

Survey of technologies

We regularly consult experts on their current needs, with tool research being a frequent request. This chapter highlights key technologies we find noteworthy, providing brief product summaries and links to detailed datasheets and contacts in our techL database.

All innovations be found in the technology database

techL

www.techl.eu

United
Innovations

www.united-innovations.eu