
Solvinity
Secure Managed Cloud
NIST & ZERO TRUST
FOUNDATIONS FOR CYBER RESILIENCE
WHITEPAPER

Content

Introduction

Cybersecurity is no longer just a matter for the IT department, especially now that cyber threats pose a direct business risk. Cybersecurity has become a strategic issue. The impact of an incident goes beyond simply blocking or damaging systems. There is a good chance that a cyberattack will have a serious impact on your services, reputation, and continuity. Moreover, the security landscape is more complex than ever. Digital dependency is increasing, laws and regulations are becoming stricter, and attacks are increasingly sophisticated.

Many organisations have the basics reasonably well in order. Still, the question remains: how vulnerable are you really, and how do you continue to improve your cyber resilience? Frameworks, such as the NIST Cybersecurity Framework (CSF), provide guidance. More important, however, is how you translate these guidelines into your own practice. In addition, it is now a requirement that your approach is sustainable and demonstrable, due to inspections and compliance requirements.

In this whitepaper, we demonstrate how the NIST Framework and a Zero Trust approach can help you gain control over your security. Using Solvinity's practical experience as a starting point, you will discover how your organisation can create oversight, make targeted security improvements, and work demonstrably towards cyber resilience.

Gain **control of your security** with the NIST framework and a Zero Trust approach

NIST as a backbone for cybersecurity

At many organisations, security has developed organically, with separate measures and solutions often introduced in response to incidents or regulatory requirements. For example, firewalls from supplier A, a monitoring tool from party B, and a SOC via partner C. These components are very valuable, but without cohesion, there is a lack of oversight.

The NIST Cybersecurity Framework (CSF) provides structure and embeds cybersecurity into policy, technology, and behaviour. Measures are grouped into five interconnected functions: Identify, Protect, Detect, Respond, and Recover. Together, these form a continuous process that enables you to manage risks effectively. This way, you gain insight into your infrastructure, systems, networks, applications, and processes. It also highlights potential risks the organisation faces, such as missing or duplicate security measures.

At Solvinity, we use this framework both internally and for our clients. We support clients with risk assessments, improving monitoring, and streamlining access management. By incorporating everything into the NIST model, a logical whole emerges, providing a structure for compliance and audits.

One of the strengths of the NIST Framework is that it serves as a common frame of reference for both CISOs and executives. While good security is essential for everyone, each organisation has its own areas of focus. With NIST, you can determine the maturity level for each component: from ad hoc and reactive to demonstrably controlled and strategically embedded.

NIST is not a checklist or an end goal, but a practical tool for providing structure, maturity, and demonstrability in complex environments such as the (semi-)public sector, financial sector, and vital infrastructure.

NIST Framework

Zero Trust: not a model, but a mindset

Zero Trust is a logical step if you want to move beyond a purely reactive approach to cybersecurity and instead aim for continuous improvement. It is not a product or a project; it is a way of thinking and working. The principle is clear: do not trust by location, rank, or role, but always verify behaviour, context, and identity to achieve complete visibility. This approach focuses security on both external threats and internal networks.

It is important to realise that Zero Trust is not a technology. It is an architectural principle that helps you design your IT landscape in a secure and considered way. At Solvinity, Zero Trust is central to our design and management. Our infrastructure is based on the 'secure-by-design' principle. This means: thinking carefully before building anything. We ensure that everything is protected by default and only becomes accessible when absolutely necessary, based on the ‘least privilege’ principle. Security measures such as network segmentation, authentication, hardening, and multi-factor authentication form the foundation for Zero Trust. In addition, essential elements such as continuous pentesting/red teaming and 24/7 security monitoring (Managed Detection & Response, MDR) are what make a Zero Trust approach workable. Zero Trust stands for ‘never trust, always verify’, so continuous pentesting and security monitoring are an inseparable part of our Zero Trust approach.

In our infrastructure, access is closed by default and we use segmentation, strict access management, continuous monitoring, and automated detection. This approach is firmly embedded in Solvinity’s daily practice. You can see this reflected in the design of our secure managed clouds and in our collaboration with partners such as Securify. This prevents the use of ad hoc solutions and makes deviations quickly visible.

The link with NIST

Zero Trust aligns seamlessly with the NIST Framework. Full visibility, a core principle of Zero Trust, is directly reflected in the Identify and Detect phases of NIST. Continuous verification and strict access control also fall under the Protect function. Incident response and recovery procedures correspond with Respond and Recover. In this way, Zero Trust becomes not an abstract strategy, but a concrete working method. The guideline published by NIST, SP 800-207, provides practical, step-by-step instructions for implementing Zero Trust. This enables you to translate the abstract Zero Trust principles into a workable approach that fits your infrastructure and risk profile.

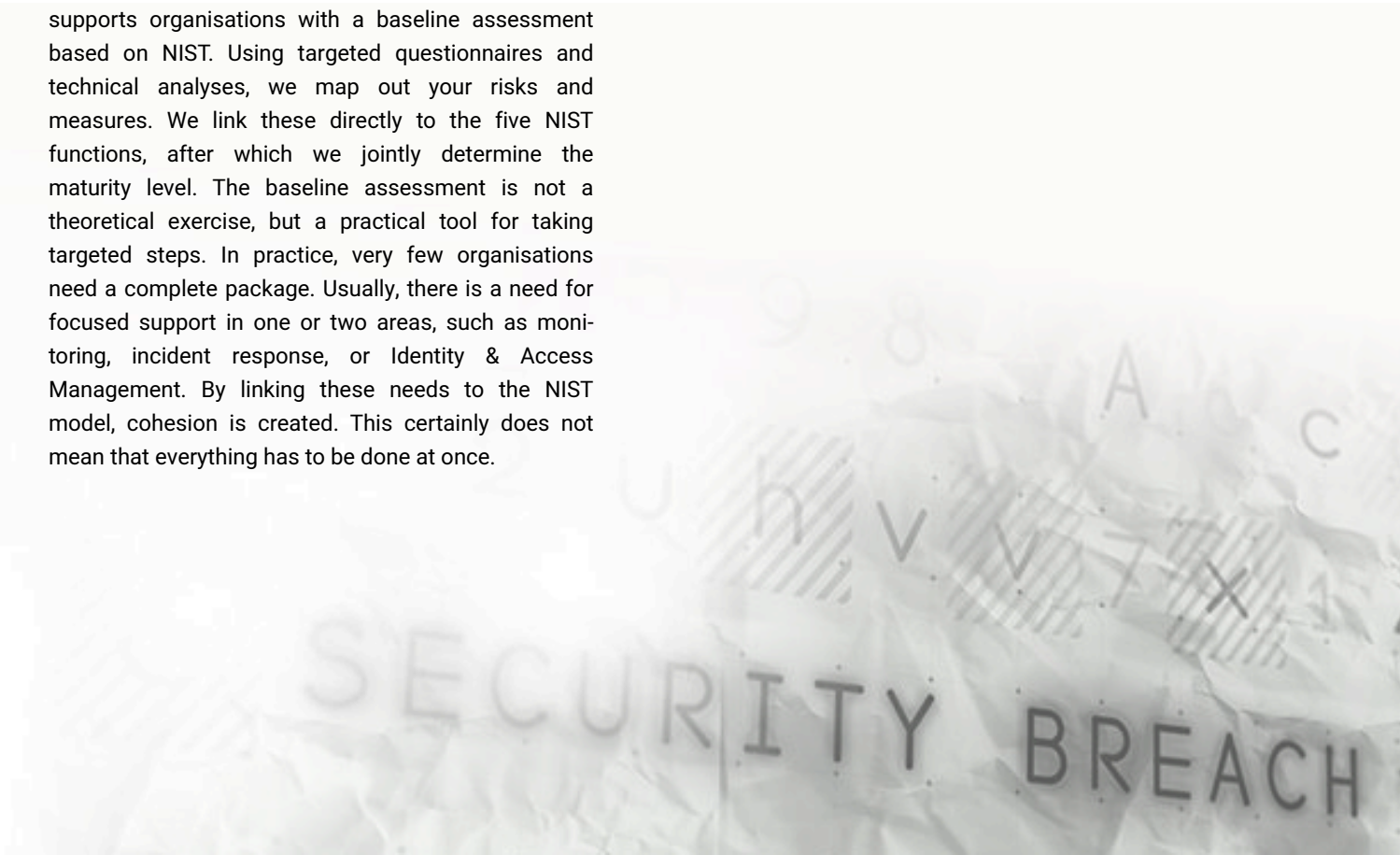
However, Zero Trust is not a solution that you can simply roll out as a 'product'. It is a way of looking at your infrastructure and processes. For many organisations, it means a cultural shift: from implicit trust and assumptions to explicit control and measurable measures. This requires a continuous process of awareness, implementation, and evaluation. It helps you respond more quickly, reduce risks, and make compliance easier to demonstrate.

Where do you stand? Everything starts with insight

But at many organisations, security measures accumulate over time. Different suppliers, ad hoc solutions, and internal processes do not always align with each other. There is often a lack of cohesion and oversight. Measures are spread across departments and suppliers, processes are not coordinated, and vulnerabilities remain unclear.

A structured approach starts with insight. Solvinity supports organisations with a baseline assessment based on NIST. Using targeted questionnaires and technical analyses, we map out your risks and measures. We link these directly to the five NIST functions, after which we jointly determine the maturity level. The baseline assessment is not a theoretical exercise, but a practical tool for taking targeted steps. In practice, very few organisations need a complete package. Usually, there is a need for focused support in one or two areas, such as monitoring, incident response, or Identity & Access Management. By linking these needs to the NIST model, cohesion is created. This certainly does not mean that everything has to be done at once.

For organisations seeking greater depth, we collaborate with Securify. Through a pentest or red team approach, we provide a realistic picture of vulnerabilities — sometimes even without employees being aware that testing is taking place. This gives a true reflection of actual resilience.



Shared Ownership

Demonstrable security is not optional. This is not only due to legislation and regulations such as DORA or NIS2. Supervisors, auditors, and chain partners not only expect measures to be in place, but also require evidence. Is there logging? Is patch management demonstrably effective? Are incidents recorded and followed up? You must be able to demonstrate that security measures are considered, effective, and up to date.

The NIST model provides a structured approach to demonstrate this. Each component can be linked to concrete measures, tools, and procedures. This makes it easier to provide evidence. Moreover, this insight promotes shared understanding between IT, CISOs, and the board. At the same time, compliance remains a shared responsibility. Just like with the 'shared responsibility model' in the cloud, basic security lies with the platform or service provider, but as an organisation you are responsible for configuration, usage, and control. Solvinity supports you in this, but does not take over that responsibility.

Continuous improvement

No one starts from zero when it comes to security. At the same time, few organisations are truly 'secure'. Cybersecurity is not a destination, but an ongoing process. New threats, such as AI, accelerate attacks and increase the attack surface—for example through spear phishing or automated exploits. At the same time, AI also helps with defence, such as analysing log files or detecting abnormal behaviour.

Solvinity has been using AI for monitoring for years, but we too continue to learn. We closely follow developments in quantum computing, data sovereignty, and new regulations, and continuously adapt our approach. This is only possible with a solid foundation. NIST and Zero Trust provide that basis. This way, your organisation remains secure and agile, even as technology changes. In this way, you are not working reactively, but strategically on digital security.

Cybersecurity is not a destination; it is a **continuous process**

From awareness to a demonstrably secure approach

Cybersecurity is about managing risks that could threaten the continuity of your organisation. However, it goes beyond just risk management. A well-secured environment requires insight, structure, and discipline. The NIST Cybersecurity Framework provides a solid and recognisable foundation. Zero Trust helps you make the right choices when it comes to the design of systems, access, and monitoring. Together, they form the backbone of a secure, future-proof IT strategy.

If you want to get a grip on risks, compliance, and continuity, you need to start with insight. The baseline assessment acts as a thermometer: how cyber resilient are you, where are you performing well, and what needs improvement? This requires awareness and context—otherwise, you will simply be putting out fires. That's why we believe in an approach that starts with an overview and ends with demonstrable improvement. 24/7 monitoring, secure-by-design, segmentation, and MFA are not separate elements, but together form one whole: a Zero Trust approach that works in practice.

In short: map out what you have, determine where reinforcement is needed, and work step by step towards a demonstrably secure environment — before risks or attacks catch up with you.

Curious how Zero Trust can contribute to the digital security of your organisation?

Discover it with a baseline assessment based on the NIST Framework. This will give you immediate insight into risks, areas for improvement, and concrete next steps. Get in touch with us:

+31(0)20 364 3600

info@solvinity.com

Solvinity
Secure Managed Cloud

Solvinity B.V.
Postbus 23673
1100 ED Amsterdam

T +31(0)20 364 3600
E info@solvinity.com
www.solvinity.com

With secure managed cloud services, Solvinity supports and advises organisations with high security requirements in their digital transformation.

	Public Cloud Private Cloud Security Services Workspace
	Solvinity distinguishes itself in the field of cybersecurity with an extensive portfolio of security services and solutions, and, through its majority stake in Securify, offers additional services in the areas of pentesting, red teaming, and agile security.
	Certifications according to (inter)national standards such as ISO 27001, ISO 14001, ISO 9001, ISAE3402 Type I and II, and PCI DSS. As the first Managed Service Provider in the Netherlands to provide SOC 1 & 2 compliance reports for the entire management environment, not only for the private cloud but also for Azure cloud.
	Solvinity provides services to central government, municipalities, and leading organisations in the financial and business services sectors, such as the Ministry of Justice and Security, the Dutch Police, Translink (OV-chip card), ING, and Klaverblad.

300+

Amsterdam, Assen
Amersfoort, Den Bosch