RAPID7

DATA SHEET

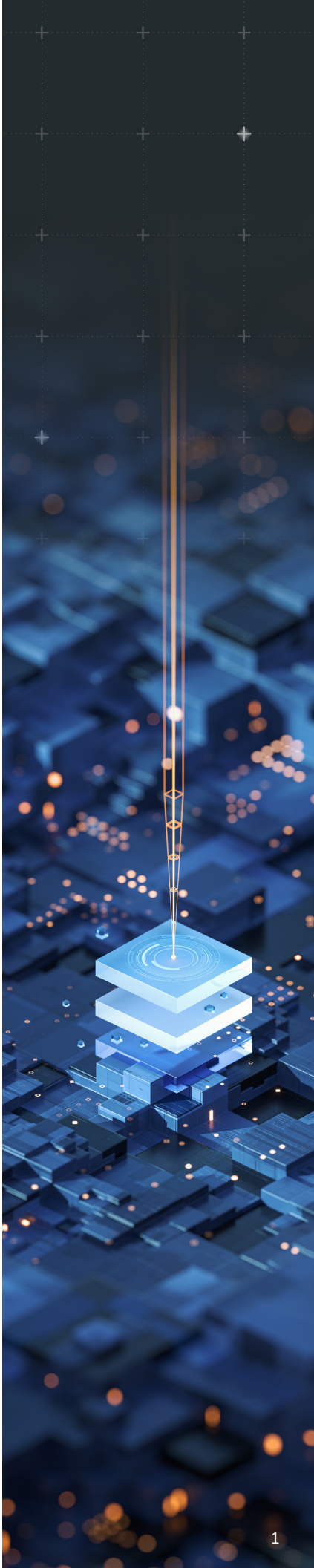
SUPPORTING NIST CSF 2.0 COMPLIANCE WITH RAPID7

Governments globally are increasingly establishing guidance and regulations for cybersecurity best practice. The NIST Cybersecurity Framework (CSF) 2.0, released in February 2024, provides voluntary guidance to help organizations manage and reduce their cybersecurity risks. NIST's cybersecurity framework and standards are widely used and recognized around the world, designed for use by organizations of all sizes and sectors, including industry, government, academia, and nonprofit organizations, regardless of the maturity level of their cybersecurity programs.

In the EU, the Digital Operational Resilience Act (DORA) and NIS2 have recently been introduced which go beyond the voluntary nature of NIST CSF 2.0 and add stricter regulation and mandates to the management of cybersecurity by critical sectors. The background and reasons for these guidelines and directives are similar. Government institutions, critical industries and individuals are now so dependent on IT services that any threats to those services pose a significant problem both to individuals and the wider economy.

The NIST Cybersecurity Framework (CSF) has evolved from Version 1.1 to Version 2.0, introducing several key changes to enhance its applicability and effectiveness across all sectors. Changes include:

- **Expanded Scope**: CSF no longer targets only critical infrastructure but applies to all organizations, regardless of size or industry, broadening its relevance and utility.
- **Introduction of the 'Govern' Function**: A sixth pillar, "Govern," has been added to the existing five pillars (Identify, Protect, Detect, Respond, Recover) to emphasise that a programmatic approach is required to the delivery of cybersecurity.
- **Implementation Examples**: CSF 2.0 includes more guidance and implementation examples for organizations looking to improve their cybersecurity posture.



The NIST CSF 2.0 Functions

NIST CSF 2.0 now has six functions. These functions are the foundation of a successful cybersecurity program and provided a comprehensive approach to managing cybersecurity risk.

- **Identify:** Identify critical business processes and assets. Consider which of your organization's activities absolutely must continue to be viable.
- **Protect:** Establish safeguards to manage the organization's cybersecurity risks and help contain the potential impact of a cybersecurity breach.
- **Detect:** Monitor networks, systems, and facilities continuously to find potentially adverse events. Develop and test processes and procedures for detecting indicators of a cybersecurity incident on the network and in the physical environment.
- **Respond:** Establish and execute an incident response plan once an incident is declared, in coordination with relevant third parties. Respond quickly to a detected breach.
- **Recover:** Restore any assets and operations affected by a cybersecurity incident. Recover any data that might have been lost as a result of a breach or attack.
- **Govern:** This new pillar emphasizes the importance of governance in cybersecurity risk management, highlighting the need for organizational oversight and decision-making in cybersecurity strategies. Ensure that the organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

How Rapid7 supports NIST CSF 2.0 Compliance

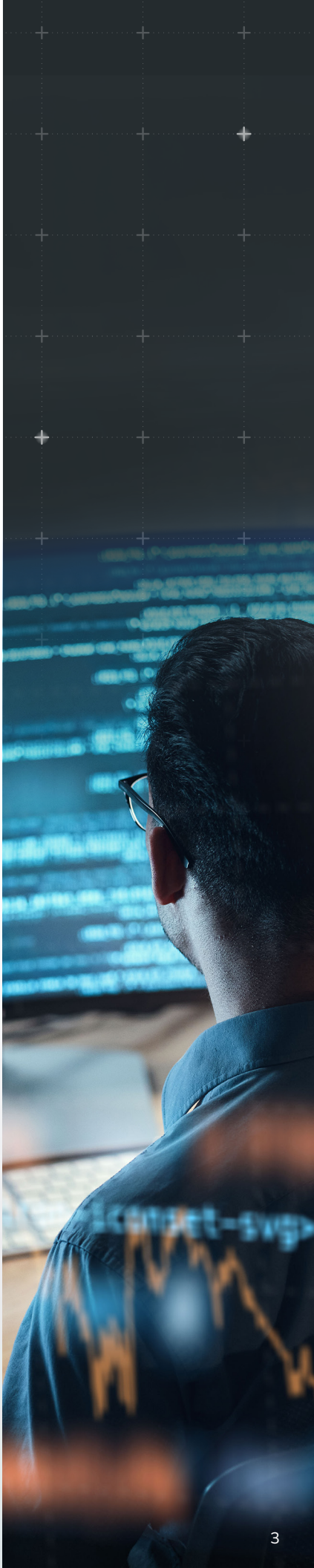
As per DORA and NIS2 compliance, it is likely that multiple cybersecurity and other solutions will be required to support an organisation's overall compliance with NIST CSF. At Rapid7, our solutions can be used to help support the requirements contained in all six pillars of the framework.

The table illustrates how the Rapid7 Command Platform can support your NIST CSF compliance.

NIST CSF Pillar	Rapid7 Solution
Identify	• Surface Command • Exposure Command • Managed Threat Complete • Vector Command
Protect	• Exposure Command • Managed Threat Complete
Detect	• Exposure Command • Managed Threat Complete • Vector Command
Respond	• Exposure Command • Managed Threat Complete
Recover	• Partner

Next Steps

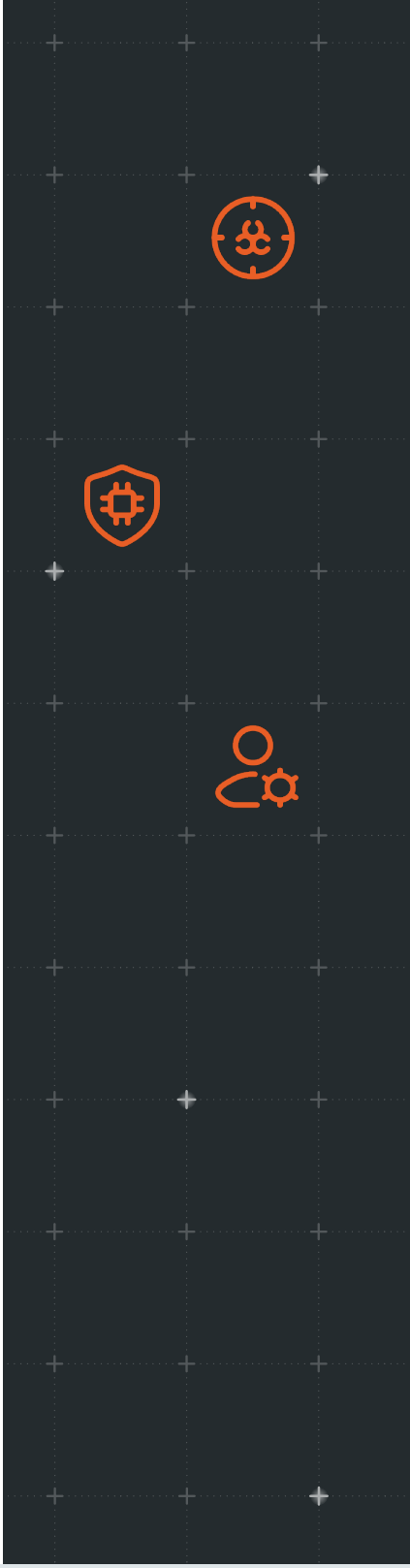
NIST is not a regulatory agency so compliance with its frameworks is usually voluntary. However companies working with the US government, especially those handling Controlled Unclassified Information (CUI), often need to comply with NIST standards to be eligible as suppliers. In addition many companies may ask their suppliers to demonstrate adherence to NIST guidelines as part of their overall cybersecurity risk management practices. Following NIST frameworks can be a way for suppliers to show potential clients that they have robust cybersecurity practices in place.



As an organisation, Rapid7 continues to monitor and contribute to the development of emerging industry and regulatory cybersecurity standards and requirements. Within our portfolio of products we offer and continue to extend our compliance solutions that either map to or partially support standards and emerging regulatory requirements. Leveraging our suite of compliance packs and policy tools for both cloud and on-prem scenarios can enable you to tailor your compliance requirements and achieve optimal visibility into your assets, speeding up both regulatory compliance and ROI.

IF YOU WOULD LIKE TO FIND OUT MORE ON HOW RAPID7 CAN SUPPORT YOUR NIST CSF 2.0 COMPLIANCE PLEASE VISIT:

https://www.rapid7.com/products/command/exposure-management/ or contact your local Rapid7 representative or partner.



About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/trial/insight