NIST Cybersecurity Framework 2.0

Take the Path to Stronger Cybersecurity with the RSA Unified Identity Platform

Originally focused on securing critical infrastructure, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) has been expanded to help organizations of all types and sizes across all industries adopt a risk-based approach to strengthening cybersecurity. CSF 2.0 builds on the original framework of CSF 1.0 by responding to the evolution of cybersecurity threats, reinforcing the central role of identity in cybersecurity, and reflecting the importance of zero trust and other fundamental principles of security in today's digital world.

As a framework for building defenses in a growing and changing threat landscape, CSF 2.0 incorporates the same approach to cybersecurity that underlies RSA's response to today's threats. Just as CSF 2.0 has broadened the scope of the initial CSF framework over the past decade, so too has RSA broadened its approach to identity security, consolidating multiple capabilities in a single platform to help prevent risks, detect threats, and evolve beyond authentication.

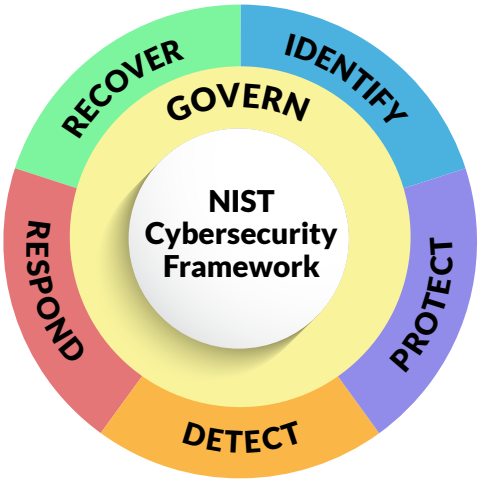
This brief highlights the main changes to the framework and why they're important, as well as explaining how RSA technology and solutions are aligned with the principles of CSF 2.0.

NIST CSF 2.0: What's New, and Why Does It Matter?

- **Broader scope:** CSF 1.0 focused primarily on protecting critical infrastructure. The original document's title, "Framework for Improving Critical Infrastructure Cybersecurity," clarifies the primary audience that NIST had in mind in 2014. Recognizing that cyber threats affect organizations beyond critical infrastructure and the interconnected threat landscape, CSF 2.0 takes a different stance and a broader scope. Noting that the 2014 title "is not used for CSF 2.0," NIST updated the guidance to include all organizations of every type and size. Expanding CSF 2.0 beyond critical infrastructure will prevent threats from spreading in our interconnected digital world, and ensure that all organizations have a more advanced cybersecurity standard.

- **Additional guidance and resources:** To help all types of organizations adopt the framework, including smaller organizations that may be more pressed for time and resources, CSF 2.0 includes resources such as quick start guides, reference tools, and other items designed to make it easier to put the principles of the framework into action.

- **Expanded functions:** CSF 2.0 is organized around six key areas of functionality, having added "govern" as a function. The term in this context refers broadly to the need for involvement of senior management as well as IT when putting in place a process to address the risk associated with cybersecurity threats. In this way, it brings to the forefront the need for cybersecurity to be integrated with the larger organization and with overall enterprise risk management.



The Cybersecurity Framework core functions organize cybersecurity outcomes at their highest level. "Govern" was added in CSF 2.0 to emphasize the importance of senior management engagement in addressing cybersecurity risk.

Realizing the CSF 2.0 Vision: The Outsize Role of Identity

Since the publication of NIST CSF 1.0 in 2014, identity has become central to cybersecurity for several reasons.

- **A vanishing perimeter and an extended threat landscape:** Identity has become more critical than ever to establishing and protecting access, with the attack surface going beyond any defined perimeter, and with the base of users growing to include not just internal employees but also customers, partners, contractors, and even devices.
- **More dangerous threats:** The threat landscape has long been dominated by identity-driven threats, but today's threats are more sophisticated and dangerous than ever. That makes them more difficult to detect and defeat, and more damaging when they succeed.
- **The rise of advanced persistent threats:** Threat actors today often count on the ability to exploit weak credential enrollment and recovery processes to compromise low-level accounts—and then stealthily gain additional privileges over time by taking advantage of poor governance and lifecycle practices.

RSA Unified Identity Platform: Uniquely Equipped to Support CSF 2.0

In today's rapidly evolving digital landscape, organizations are challenged with securing their environments against sophisticated threats while ensuring seamless access for users. The RSA Unified Identity Platform is a security-first, intelligent platform that replaces multiple point solutions with a platform that brings together everything secure environments require—including the authentication and identity governance capabilities needed to establish zero trust.

The RSA Unified Identity Platform delivers:

Trusted Security

For decades, RSA has secured the most secure organizations, working with leaders in government, finance, energy, and more to defend their operations. That pedigree drives the development of new security-first RSA solutions, including comprehensive authentication, access, and governance capabilities that provide visibility into who has access, what they have access to, and why they need it. A broad range of authentication methods—including phishing-resistant and passwordless options—support today's hybrid/remote workforce and maintain security amid a growing population of external users.

Actionable
Intelligence

Driven by AI and machine learning, RSA identity intelligence provides the threat awareness and insights needed to defend against today's advanced identity threats. At the point of authentication, RSA Risk AI intuitively determines user risk before granting access, keeping bad actors out and letting trusted users in. In mobile environments, RSA Mobile Lock's threat-intelligence capability detects critical threats to a device and restricts the user's ability to authenticate until it's resolved. RSA Governance & Lifecycle provides a dynamic identity governance and administration (IGA) dashboarding framework that provides insights to uncover access risks.

Continuous
Compliance

Combining traditional governance capabilities with a robust risk engine, the RSA Governance & Lifecycle component of our platform offers advanced dashboards to swiftly detect and resolve excess entitlements, inactive accounts, and unusual access patterns. These capabilities help mitigate compliance failures and reduce the risk of identity breaches. Additionally, our innovative gamification features incentivize timely access reviews, fostering a culture of compliance and enhancing risk discovery.

Maximum
Flexibility

In a constantly changing threat environment, the RSA Unified Identity Platform is expressly designed with the flexibility to withstand modern attacks and adapt to future dangers. It's the result of constant innovation, with solutions that leverage AI to detect threats and automate responses, provide secure, flexible access, maintain compliance, and work securely across cloud and hybrid environments. We also leverage open standards, APIs, and solution-specific connectors that allow RSA to integrate with thousands of applications, increasing customer flexibility and choice.

Realize the Vision of CSF 2.0 with RSA

At RSA, we look forward to working with organizations in a variety of sectors to build strong, risk-based identity programs based on the principles that shape the NIST CSF 2.0 framework. Our long history of helping establish identity security for government agencies and other security-first organizations and our robust authentication, access, and governance capabilities make RSA uniquely prepared to help lead efforts to meet this challenge

Watch our video to learn more about the RSA Unified Identity Platform.

About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organizations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments.
For more information, go to RSA.com.

RSA