WHITE PAPER

oxsecurity

NIST Cybersecurity Framework 2.0:

Improve Application Security in Today's Threat Landscape

Contents

In today's dynamic cybersecurity landscape, staying ahead requires a proactive and well-governed approach. The NIST Cybersecurity Framework (CSF) 2.0 is a highly respected resource that offers a robust structure for organizations to secure their digital assets, especially their applications.

OX Security's Application Security Posture Management (ASPM) platform is indispensable in this journey; OX provides the essential visibility, risk prioritization, and automation needed to align with NIST CSF 2.0 across the entire software development lifecycle (SDLC).

This white paper will explore the significant impact of NIST CSF 2.0 on application security (AppSec) and demonstrate how OX empowers companies to achieve and maintain compliance.

Introduction: The Evolving Landscape of Cybersecurity and the Role of NIST CSF 2.0 in Application Security

The digital world is under constant siege, with cyberattacks regularly targeting software applications. As these attacks become more frequent and sophisticated, serious consequences like data breaches, financial losses, and reputational damage are more likely. To effectively counter these threats, organizations need strong, adaptable cybersecurity strategies built on comprehensive frameworks. The NIST Cybersecurity Framework (CSF) has become a globally recognized standard, providing a structured way to manage and reduce cybersecurity risks for organizations of all types and sizes.

In February 2024, NIST released Version 2.0 of the CSF. This update broadens the framework's reach to include all organizations, regardless of size, sector, or cybersecurity maturity level — a significant shift from its initial focus on critical infrastructure. This expansion reflects the widespread recognition that cybersecurity is a universal concern in our interconnected world.

Within this landscape, application security is paramount. Applications are often the primary way businesses operate and handle sensitive data, making their security crucial for protecting assets and ensuring resilience.

This white paper offers a detailed look at NIST CSF 2.0, specifically focusing on what it means for application security (AppSec). We'll break down the key changes in this updated version, explain how it addresses the evolving challenges of securing modern applications, and guide organizations on how to align their application security practices with CSF 2.0. We'll also highlight the tangible benefits of adopting this framework for building a more secure and resilient application environment.

Understanding the Foundations: NIST Cybersecurity Framework 2.0

NIST CStF 2.0 provides a structured yet flexible approach to cybersecurity risk management, built on three core components:

The Framework Core

The Framework Core is central, offering a taxonomy of high-level cybersecurity outcomes organized into six key functions.

Organizational Profiles

Organizational Profiles allow organizations to describe their current and desired cybersecurity posture about these outcomes.

Framework Tiers

Framework Tiers characterize the level of sophistication in an organization's cybersecurity risk management practices.

Core Functions: Govern, Identify, Protect, Detect, Respond, Recover

At its heart, NIST CSF 2.0 organizes cybersecurity outcomes into six core Functions: Govern, Identify, Protect, Detect, Respond, and Recover — Functions well known to anyone who's used CSF previously.

Each function represents a critical stage in managing cybersecurity risk throughout its lifecycle.

A significant addition to CSF 2.0 is the **Govern (GV)** function. This function focuses on establishing, communicating, and monitoring an organization's cybersecurity risk management strategy, expectations, and policies. It emphasizes the importance of integrating cybersecurity into the broader enterprise risk management (ERM) strategy and ensures that cybersecurity decisions align with the organization's mission and stakeholder expectations. The Govern function provides the necessary context for how an organization approaches and prioritizes the outcomes of the other five functions:

- **The Identify (ID)** function helps organizations identify cybersecurity risks by providing guidelines for evaluating critical business processes and assets, and understanding potential threats and vulnerabilities to the organization's environment.
- **The Protect (PR)** function details the safeguards that help security teams manage identified cybersecurity risks. These include deployed security controls and practices that prevent or reduce the likelihood and impact of cyber incidents.
- **The Detect (DE)** function covers the types of activities required to identify cybersecurity events, such as continuous monitoring of systems and networks to identify potential security breaches or anomalies.
- **The Respond (RS)** function defines how to plan for an incident and the actions to take when a cybersecurity incident is detected, including analysis, containment, eradication, and recovery.
- **The Recover (RC)** function focuses on the steps to restore organizational capabilities and services impacted by an incident, including recovery planning, system and data restoration, and stakeholder communication.

Categories and Subcategories: A Detailed Look

Each of the six Core Functions is further broken down into Categories, representing groups of cybersecurity outcomes. For instance, within the Protect Function, categories like "Access Control," "Awareness and Training," and "Data Security" group related security outcomes. These Categories are then further divided into Subcategories, which describe specific, detailed outcomes that support achieving each Category.

NIST CSF 2.0 includes 22 Categories and 106 Subcategories and supplies a granular and actionable framework for managing cybersecurity risk.

Organizational Profiles and Tiers: Tailoring the Framework

Organizational Profiles allow organizations to describe their current cybersecurity posture ("Current Profile") and their desired future state ("Target Profile") in terms of the CSF Core outcomes. This helps organizations understand, tailor, assess, prioritize, and effectively communicate their cybersecurity efforts. Framework Tiers characterize the rigor of an organization's cybersecurity risk governance and management practices. These Tiers range from Tier 1 (Partial), which indicates reactive practices, to Tier 4 (Adaptive), which represents sophisticated and proactive approaches.

Key Updates and Their Significance for Application Security

NIST CSF 2.0 includes several key updates that build on the strengths of version 1.1. These changes reflect the evolving cybersecurity landscape and help provide more relevant and actionable guidance.

The Introduction of the Govern Function and its Impact on Application Security Strategy

The most significant update in CSF 2.0 is the introduction of the Govern function, as noted above. The addition highlights the critical role of governance in a strong cybersecurity risk management program, including application security programs. The Govern function emphasizes aligning cybersecurity strategy with business objectives and integrating it into the broader enterprise risk management framework. For application security, this means that decisions about security policies, resource allocation, and accountability for applications are driven by overall business goals and risk tolerance, and ensures that executive teams are actively involved in cybersecurity decisions.

Enhanced Focus on Supply Chain Risk Management and Implications for Third-Party Application Components

CSF 2.0 significantly strengthens its focus on Cybersecurity Supply Chain Risk Management (C-SCRM), an inherent element in every software development program. C-SCRM is particularly relevant for AppSec given the widespread use of third-party components, libraries, and services used to build software today. In the current iteration of the CSF, the Govern function now includes a dedicated category, GV.SC, for C-SCRM. This category now requires organizations to thoroughly assess the cybersecurity practices of suppliers and implement comprehensive risk management strategies that extend beyond their internal operations. This means that organizations must now set and follow security requirements for software component suppliers, conduct due diligence, and continuously monitor risks associated with their products and services used in applications. While this might seem like an arduous task, it is one that will demonstrably reduce the risk of supply chain issues and improve overall cybersecurity and business risk posture.

Broader Scope and Applicability to Diverse Organizations

While earlier versions of the CSF primarily targeted critical infrastructure (CI), CSF 2.0 explicitly broadens its scope to include all organizations, regardless of size, industry, or cybersecurity maturity. This change acknowledges the widespread adoption of the CSF beyond CI and recognizes the universal need for robust cybersecurity practices. The language in CSF 2.0 has been generalized to be more adaptable to the diverse needs of myriad organizations and business units, including application security and software development teams.

Emphasis on Measuring Cybersecurity Outcomes in AppSec

CSF 2.0 places a greater emphasis on the importance of measuring cybersecurity outcomes. In this new version, organizations are encouraged to develop and use metrics and benchmarks to evaluate the effectiveness of their cybersecurity practices, including those related to AppSec and software supply chain security (SSCS). This focus on measurable outcomes allows organizations to adopt a data-driven approach to security and arrive at better-informed decisions related to cyber risk management.

Addressing Modern Application Security Challenges with NIST CSF 2.0

NIST CSF 2.0 is a valuable framework for tackling the complex and evolving challenges of securing modern applications. Its principles and functions can be applied to effectively mitigate risks associated with modern application architectures and development methodologies.

Securing Cloud-Native Applications

The elements of CSF 2.0 are highly relevant for securing cloud-native applications, which often utilize technologies like containers, microservices, and serverless computing, often indispensable components of the software development lifecycle (SDLC). The framework's core functions, especially Identify, Protect, Detect, Respond, and Recover, can guide organizations' implementations of security controls tailored to ephemeral environments, including but not limited to managing container security, securing communication between microservices, and ensuring the integrity of serverless deployments. Further, the new Govern function plays a crucial part in establishing policies and providing oversight for cloud security practices related to applications.

Integrating Security into DevSecOps Pipelines

CSF 2.0 strongly supports the integration of security practices throughout the entire SDLC using a DevSecOps approach. The framework's functions align with DevSecOps principles, emphasizing the need to "shift left" by embedding security considerations early and continuously within the development pipeline when they are easier and less costly to address.

The Identify function helps AppSec teams understand security risks associated with an application. The Protect function guides the implementation of secure coding practices and security testing. The Detect function focuses on identifying vulnerabilities and threats within the pipeline. Respond and Recover address incident response and remediation during development and through deployment. The Govern function ensures that security becomes a shared responsibility across DevOps, AppSec, and operations teams.

Protecting APIs and Microservices

As API-driven architectures and microservices gain greater adoption, CSF 2.0 provides guidance for securing APIs. The Identify function helps catalog and classify APIs and microservices based on their sensitivity and risks. The Protect function guides the implementation of security controls like authentication, authorization, encryption, and input validation. The Detect function focuses on monitoring API traffic for malicious activity. Respond and Recover address incident handling specific to API security breaches. Last but not least, the Govern function ensures API security is integrated into the overall AppSec strategy with appropriate policies and enforcement capabilities.

The Impact of CSF 2.0 on Application Development Practices

The adoption of NIST CSF 2.0 positively impacts how organizations approach application development and maintenance, helping teams build, distribute, and use more secure and resilient software.

Shift Left: Embedding Security Early in the SDLC

CSF 2.0 strongly encourages the "shift left" approach in application development, meaning, software development teams integrate security considerations from the initial design stages all the way through testing, deployment, and runtime.

The ability to proactively identify and address potential security risks early in the development process allows organizations to prevent costly fixes to code later on. The Identify function helps organizations with threat modeling and defining security requirements that can be used during initial software development phases, leading to more secure applications that require less effort and reduced cost.

Secure Coding Standards and Practices

The Protect function helps DevOps teams establish secure coding standards. Organizations adopting CSF 2.0 are encouraged to define and enforce coding guidelines that minimize common software vulnerabilities like SQL injection and cross-site scripting (XSS).

Vulnerability Management and Remediation

The Framework's Identify and Detect functions guide vulnerability management and remediation processes, which are essential in application development. AppSec teams must regularly scan their software and environments using a combination of vulnerability assessment tools like SAST, SCA, Git posture, and secrets scanning to identify known vulnerabilities.

The Respond function then helps teams prioritize and remediate high-fidelity issues that would substantively impact that business's security posture if compromised. A continuous cycle of vulnerability identification and remediation is vital for maintaining a strong application security state throughout the SDLC.

Enhancing Application Security Posture Throughout the Application Lifecycle

NIST CSF 2.0 is a comprehensive framework that allows organizations to secure software at every stage of an application's lifecycle, from initial design through runtime.

Secure-by-Design Principles

The Framework promotes secure-by-design principles from the onset, which means that security requirements are baked into software development processes and potential threats are addressed as they are identified (i.e., at every stage). The Identify function details how to conduct threat modeling to anticipate attack vectors and design secure architectures that minimize vulnerabilities. Doing so is more effective and cost-efficient than adding security measures after an application is built.

Secure Deployment and Configuration

The Protect function guides the secure deployment and configuration of applications in production environments. This section covers hardening application servers and infrastructure, adhering to the principle of least privilege for access controls, and securely managing configuration settings. Proper deployment and configuration are also critical for preventing vulnerabilities from misconfigured systems or overly permissive access.

Continuous Monitoring and Threat Detection for Applications

The Detect function emphasizes the need for continuous monitoring and threat detection. Proper detection requires AppSec teams to implement mechanisms to log application activity, monitor for suspicious behavior, and leverage threat intelligence to identify potential attacks in real time. ASPMs, SIEMs, and application performance monitoring tools are vital for achieving continuous visibility.

Incident Response and Recovery for Application Security Breaches

Despite preventative measures, application security breaches can still happen. The Respond and Recover functions help organizations prepare for and respond to security events and incidents. To achieve appropriate preparedness, organizations must:

- Develop and test incident response plans specific to their AppSec programs and business operations
- Establish clear communication protocols (within development/security teams and more broadly throughout the organization)
- Build procedures for quickly recovering affected applications and data.
- Conduct feedback and "lessons learned" from past incidents, incorporating learnings into future security practices

New and Modified AppSec Controls and Recommendations

The NIST CSF 2.0 introduces several new and modified subcategories with direct implications for enhancing application security. Understanding these changes is essential for organizations that want to align their application security practices with the current framework.

Table 1: Key CSF 2.0 Updates Relevant to Application Security

Function	Category	Subcategory	Change from CSF 1.1	Impact on Application Security
Govern	Cybersecurity Supply Chain Risk Management	**GV.SC-09** Supply chain security practices integrated into cybersecurity programs	New	Emphasizes integrating secure software development practices across the supply chain, impacting the selection and management of third-party components, libraries, and APIs used in applications. Organizations should ensure their suppliers follow robust security practices throughout their development lifecycle.
Protect	Platform Security	**PR.PS-01** Hardware, software, and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	New Category	Highlights the critical importance of securing the underlying platforms hosting applications, including operating systems, web servers, application servers, and cloud services. This requires implementing security measures like hardening, patching, and secure configuration management for these platforms.
Identify	Improvement	**ID.IM-01** Cybersecurity risk management processes and activities are improved based on lessons learned, trends, and emerging threats	New Category	Encourages a culture of continuous improvement in cybersecurity practices, including application security. Organizations should regularly analyze security incidents, emerging threats, and lessons learned to refine their application security policies, procedures, and controls.
Protect	Identity Management, Authentication, and Access Control	**PR.AA-05** Logical access to assets and associated facilities is managed, administered, and reviewed	Revised and Re-sequenced from PR.AC-04	While the concept existed in 1.1, its placement and emphasis in 2.0 within the refined Identity Management category underscore the importance of robust access controls for applications and their associated data and infrastructure. This includes implementing strong authentication mechanisms, role-based access control, and regular reviews of access privileges.
Protect	Data Security	**PR.DS-01** Data at rest is protected **PR.DS-02** Data in transit is protected	Existing Categories with Refined Subcategories	These categories continue to emphasize the need for protecting sensitive application data both when stored and when transmitted. This includes implementing encryption, data masking, and other data protection techniques relevant to application data handling.

Steps for Organizations to Align Application Security Practices with NIST CSF 2.0

As with any effective security process, aligning AppSec and SSCS practices with NIST CSF 2.0 is systematic, ongoing, and involves numerous steps.

Assess Current Application Security Posture

Organizations should start by thoroughly assessing their existing application security policies, procedures, and controls and consider implementing a best-of-breed ASPM platform.

Define a Target Profile

Based on unique business objectives, risk appetite, and specific security needs, organizations should define a Target Profile using NIST CSF 2.0. Doing so involves selecting relevant Functions, Categories, and Subcategories from the CSF Core that align with their desired future state of application security.

Conduct a Gap Analysis

Once both Current and Target Profiles are defined, a comprehensive gap analysis should be performed to identify the differences between current application security practices and the desired state in the Target Profile.

Develop and Implement an Action Plan

Based on the gap analysis, organizations should develop a prioritized action plan to address the identified gaps. This plan should include specific tasks, responsibilities, resources, and timelines for implementing necessary changes to application security policies, procedures, and controls.

Continuous Monitoring and Improvement

Aligning with CSF 2.0 is an ongoing process. Organizations should establish mechanisms for continuously monitoring the effectiveness of their AppSec controls and action plans. Lessons learned from security incidents, emerging threats, and evolving business requirements should be incorporated to drive continuous improvement.

Benefits of Adopting NIST CSF 2.0 for AppSec

Adopting NIST CSF 2.0 for application security offers numerous significant benefits, including:

- Improved governance and oversight
- Enhanced risk management
- Better communication and collaboration
- Alignment with industry best practices
- Increased business resilience to cyberattacks

Conclusion: Embrace NIST CSF 2.0 for a More Secure Application Future

The NIST Cybersecurity Framework 2.0 is a crucial step forward in cybersecurity guidance, providing a comprehensive and adaptable approach to managing risks, especially in application security. By embracing its principles and functions, organizations can build a more robust and resilient application security program aligned with their business goals. This updated framework effectively addresses the evolving threat landscape and fosters a culture of continuous improvement. Key enhancements like the Govern function and the stronger focus on supply chain risk management highlight the need for a holistic security strategy for all applications.

The OX Security ASPM Platform is vital for companies aiming for NIST CSF 2.0 compliance — and ultimately, a more secure process to build, test, deploy, and use software. OX offers a unified view of application security posture across the SDLC by consolidating data from ten native AppSec tools and hundreds of integrations; prioritizing risks based on context, exposure, and business impact; and automating both workflows and remediation.

OX directly supports the framework's Identify, Protect, Detect, Respond, and Recover functions and offers comprehensive insight into the software supply chain, aligns with CSF 2.0's increased emphasis on C-SCRM, and enables effective management of third-party component risks. The OX Platform streamlines security and development efforts, allowing organizations to meet NIST CSF 2.0 requirements and achieve more secure and compliant applications and software development practices.

About OX Security

For AppSec and development teams that struggle with wasted resources caused by generic prioritization of security issues, OX Security is the only unified application security posture management (ASPM) platform that leverages **proprietary Code Projection technology**. Code projection dynamically and accurately prioritizes risks based on reachability, exploitability, and real-world impact.

Unlike traditional tools that rely on static data and generic prioritization, OX Security projects code into runtime context, enabling deep, evidence-based insights from design to runtime. This ensures teams focus only on the critical 5% of risks that matter, eliminating 95% of irrelevant issues, improving collaboration, and reducing costly runtime fixes.

oxsecurity