DATASHEET

Enterprise Access: The Third-Party Remote Access Solution for the NIST Cybersecurity Framework

The Cybersecurity Framework consists of five overarching components:

The Cybersecurity Framework from NIST for Critical Remote Access

The National Institute of Standards and Technology, or NIST, focuses on helping organizations better understand and improve their management of cybersecurity risk. One of the key tools they use to equip organizations is their Cybersecurity Framework — recommended standards, guidelines, and best practices that organizations can implement to manage their cybersecurity risk and resilience.

Organizations, while not required to implement these cybersecurity recommendations, will be better prepared, protected, and responsive to cyber threats and attacks with these best practices in place. The Framework is purposely flexible, allowing organizations of different industries and sizes to decide how they can best apply the guidelines to achieve business outcomes and reduce overall cybersecurity risk.

Let’s look at two components specifically: protect and detect.

> The **protect** function outlines the safeguards that organizations should develop and implement to ensure delivery of critical infrastructure services.
>
> In the next “stage”, the **detect** function outlines the appropriate activities organizations should implement to identify and detect any cybersecurity events.

While there is flexibility in how to implement these safeguards, organizations are better positioned to mitigate the risks of an attack, protect their data and networks, and identify and contain an in-progress event when meeting these standards. Imprivata can help accomplish this.

Cost of a Data Breach: The average cost of a data breach for a U.S. organization is

$9.05 million.

Third parties and their remote access need to be key considerations when evaluating overall cybersecurity risk. Third parties are highly targeted by attackers as easier entry points into an organization's critical systems. In fact, 49% of organizations experienced a breach caused by a third party in the past year alone, and most attribute the breach to granting too much privileged access. Traditional remote access tools, such as VPNs or desktop sharing, do not meet the security standards that NIST recommends. They are not designed to restrict access to only authorized users, and they don’t provide visibility through recordings of access activity for review and examination.

Third Parties Are Your Weakest Attack Vector:

56% of organizations have experienced one or more data breaches caused by a third party.

SecureLink Enterprise Access provides the means to meet NIST’s security recommendations with regards to your third parties’ access. With individual identity management, granular control over vendor access, and detailed audit trails that log all activity, Imprivata will be a valued partner in helping you mitigate the risks of third-party access and meet the recommendations in the Cybersecurity Framework.

How SecureLink Enterprise Access enables organizations to meet NIST's cybersecurity recommendations

NIST function	NIST category	Recommendations	How Enterprise Access helps
Identify	Governance	Information security roles and responsibilities are aligned with internal roles and external partners	• Defines access policies and enforces least privileged access for third-party remote access and internal users
	Risk Assessment	Asset vulnerabilities are identified and documented	• Best Practices and Compliance checklist provides security configuration recommendations and could be used to assist in risk mitigation steps
Protect	Access Control	Identities and credentials are managed for authorized devices and users	• User identities are verified with MFA and via defined IP ranges and an email authentication key • Credentials are secured and managed in a credential vault and injected directly into the session so users never see or know them • Users can be authorized locally, via Active Directory or SSO/SAML solutions.
		Remote access is managed	• Provides secure remote access to critical systems, with access defined down to the host, port and application level • Access is enforced on a least privileged model.
		Access permissions are managed, incorporating the principles of least privilege and separation of duties	• Provides granular access controls and permissions to enforce least privilege access • Access controls include approval workflows, time-based access, and access schedules
		Network integrity is protected, incorporating network segmentation where appropriate	• Can limit connectivity to segregated networks
	Data Security	Data-at-rest and data-in-transit is protected	• All audit and credentials are encrypted at rest • Data-in-transit is encrypted with AES-128, 192 or 256

NIST function	NIST category	Recommendations	How Enterprise Access helps
Protect	Maintenance	Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access	• Provides a variety of audit options for each session, including contextual audit logs, video recordings and text-based audit • Can be reviewed in accordance with the organization's policy
	Protective Technology	Audit / log records are determined, documented, implemented and reviewed in accordance with policy	• All remote access is logged with detailed audit trails and session recording • Supports remote access for only authorized users • Can require reason for access and approval before access is granted to authorized users
		Access to systems and assets is controlled incorporating the principle of least privilege	• Access for third-party users is provisioned on the principle of least privilege • Can control access with access schedules, approvals, and time-based access controls
Detect	Anomalies and Events	Event data is aggregated and correlated from multiple sources and sensors	• Audits all sessions with video recordings and text-based audit of all user actions by default • Can export audit and data to a SIEM solution for further analysis if needed

Risks and Consequences of Unsecured Third-Party Access

RISKS WITH THIRD PARTIES

49% of organizations have experienced one or more data breaches caused by a third party in the past year

46% of organizations have a comprehensive inventory of all third parties with access to their network

63% of organizations see third-party remote access to their network becoming their weakest attack surface

41% of organizations believe they are effective at controlling third-party access to their networks

37% of organizations have visibility into the level of access and permissions for both internal and external users

FREQUENCY AND COST OF ATTACKS

- The average cost of a data breach in the United States is $9.05 million
- By 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021
- The costs of a cyberattack last for 3 years on average, with 67% of the costs incurred in year one, 22% in year two, and 11% in year three

Unsecured third-party remote access can result in severe consequences, such as stolen sensitive information, loss of customers and revenue, downtime of critical systems, or even inability to operate. SecureLink Enterprise Access mitigates these risks. It secures your third-party remote access and enables you to implement security best practices to align with NIST's Cybersecurity Framework recommendations.

Contact us to learn more about how Enterprise Access can help.

CONTACT US

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com