LastPass

LastPass for NIST 2.0

Meeting the NIST Cybersecurity Framework 2.0 guidelines is increasingly important for businesses of all sizes globally, as well as for managed service providers (MSPs) who build and manage security programs for their clients. These guidelines offer a structured approach to managing cybersecurity risks, emphasizing data protection, threat detection, and effective incident response. While no single solution can fully address every aspect of the NIST 2.0 framework, tools like LastPass play a critical role in helping organizations meet specific requirements and strengthen their overall security strategy.

LastPass supports key functions within the NIST 2.0 framework across governance, identification, protection, and detection. The chart below highlights how the product capabilities map to these functions, providing detailed descriptions of how each feature aligns with category criteria—helping businesses and MSPs enhance security and streamline compliance efforts.

LastPass supports key functions within NIST 2.0 framework

Governance

Policy, Cybersecurity supply chain risk management

Identification

Asset management

Protection

Identity management, Authentication and Access control, Awareness and Training, Data security

Detection

Anomalies and events, Security continuous monitoring

Discover how LastPass aligns with key categories of the NIST 2.0 Framework to strengthen security and compliance:

NIST CSF function	Category	Subcategory	Product capability	Description
Govern	Policy	GV.PO	User management admin controls	Centralize credential management, enabling admins to standardize and enforce password security best practices, multi-factor authentication (MFA), and access control policies, including provisioning, de-provisioning, and secure sharing of credentials internally and externally, while governing shared access between privileged users and outside organizations.
	Cybersecurity supply chain risk management	GV.SC	Dark web monitoring	Dark Web Monitoring empowers organizations to proactively reduce supply chain risk by identifying leaked or stolen supplier credentials, enabling swift action to prevent unauthorized access and protect against downstream threats.
Identify	Asset management	ID.AM	SSO + SaaS monitoring	Provide visibility into unmanaged SaaS applications through saved credentials, helping organizations identify shadow IT and improve control over approved applications via SSO.
Protect	Identity management, authentication + access control	PR.AA	Password management + MFA + SSO + idP integrations	Enforce strong and unique credentials, enable secure sharing, and streamline access control to ensure only authorized users can access critical resources.
	Awareness + training	PR.AT	Digital security dashboard	Provide security teams with visibility into password and identity security health scores, enabling them to evaluate user behaviors, assess organizational security posture, identify opportunities for targeted training, and reinforce good practices by offering personal licenses that protect both employees and the organization from targeted attacks.
	Data security	PR.DS	Secure notes	LastPass Secure Notes let users securely encrypt, store, and access sensitive information instantly within their digital vault.
Detect	Anomalies and events	DE.AE	Dark web monitoring + email notification	Monitor the dark web for compromised credentials, tracks anomalous access patterns, and sends automated email notifications on access events. With SIEM integrations, LastPass empowers organizations to quickly detect and respond to potential security threats as part of their incident response strategy.
	Security continuous monitoring	DE.CM	Dark web monitoring	LastPass offers real-time dark web monitoring for compromised credentials, allowing for proactive identification of potential security threats and vulnerabilities within the organization. Admins are notified of any user who has an unresolved dark web alert.