

Automated Credential Stuffing Protection

When cyber defenders lack the automatic visibility of corporate and personal clear-text credentials exposed in the open, deep, and dark web, they leave the door open to initial access via valid credentials.

Picnic provides visibility and continuous monitoring of breach data to identify exposed corporate, personal, and third-party credentials, and automatically prevents their reuse within the organization.

Select Capabilities & Services

- Automated credential compromise protection
- Automated and unlimited password banning
- Integrates with any IdP via API
- Enables security workflows
- Logs are streamed to the SIEM
- Breach data monitoring



CISO

Safeguard digital identity assets, respect customer privacy, counter social engineering risks, and ensure business continuity.



CRO & General Counsel

The reputation of key employees is often synonymous with corporate reputation. Proactively protect hard-won reputational halos for your organization and your leadership.



Third-Party Risk Professionals

Get the tools to make informed risk management decisions quickly regarding the companies within your organization's supply chain.



Identity & Access Management Professionals

An intelligence-based approach to identity protection allows you to thwart adversaries before they can cause harm and provides the ability to prevent account takeover.



[Schedule a demo](#)