



Proactively protect hard-won reputational halos for your organization and your leadership

Reputations are hard to build and easy to destroy. An organization's reputation is its most valuable asset, creating trust with the market across customers, employees, partners, regulators, lenders, and shareholders.

The reputation of key employees is often synonymous with corporate reputation, making impersonation of key employees one of the most critical risks to identify and diffuse. Picnic detects these risks to proactively defend against new and emerging threats to your organization's reputation and that of your executive team.



Most organizations lack the capability to analyze and measure the risk posed by exposed data tied to the human element. It is not surprising that this is both the single largest source of breaches and the biggest security gap companies have. Picnic provides the automated monitoring, analysis, and proactive remediation required to fill the defense gap and allow companies to effectively address this problem.

Henry Ristuccia, Former Deloitte Governance, Risk and Compliance Leader



Select Platform Capabilities, Services, & Use Cases

High-Value Target protection

Protect the human attack surface for executives, board members and employees with access to sensitive data.



Automated credential stuffing protection

Prevent reuse throughout the organization of compromised corporate and personal passwords that could be used in credential stuffing attacks.



Human attack surface management

Prioritize and mitigate corporate and individual risk at scale by combining external threat intelligence with human risk mapping.



Impersonation attack prevention

Proactively prevent impersonation attacks against your employees and your company.



[Schedule a demo](#)