Improve your cybersecurity defenses to stay ahead of emerging threats and protect critical systems, networks, and data

Operational interruptions and reputational damage related to social engineering attacks tend to have a wide-ranging impact. Traditional security controls have failed to stop social engineering attacks that focus on gaining access to valid identities.

While new technologies like passwordless will help protect organizations, social engineers will continue to pivot to new techniques that coerce, trick, and manipulate humans. Picnic is solely focused on stopping social engineers from interrupting your operations and damaging your reputation by bypassing your existing technology investments.

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