Prevent payment fraud with proactive risk mitigation

Social engineering attacks are a growing threat to organizations that can result in significant financial losses. They exploit human vulnerabilities and use impersonation, deception, and manipulation to gain access to sensitive information, systems, and networks.

Defending against these attacks is important to protect critical systems, networks, and data and minimize financial and reputational damage to the organization. Picnic offers finance leaders tools to proactively mitigate the risk of fraudulent transactions, preventing them from occurring and resulting in measurable savings.

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