Proactively prevent identity fraud

As organizations confront an unparalleled wave of attacks aimed at their dynamic and remote ecosystem of employees, partners, and customers, robust identity authentication has never been more critical.

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

Infrastructure security has come a long way, threat actors have had to adapt, and the cybersecurity game has changed in today's environment, where there is no true network edge. Social engineers using our own data against us is a central issue. Picnic protects individuals and their families in office, home, and remote environments, creating an enterprise culture of safety, security, and privacy. It empowers their people and delivers a smart cost-effective layer of cybersecurity that modern security teams need.
Scott Goodhart, CISO, Emeritus

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.

Suspicious domains & accounts detection

Detect attacker infrastructure before it can be used in social engineering attacks against your digital VIPs, their immediate network, or an entire workforce.

Impersonation attack prevention

Proactively prevent impersonation attacks against your employees and your company.

Schedule a demo

www.getpicnic.com