Protect high-value targets by bridging the gap between cyber and physical risk

Keep high-value targets, their families, and their support staff safe by leveraging the same techniques threat actors use to hunt them in the digital and physical worlds. Automatically and continuously discover and remediate risk and easily share reports that inspire confidence in your program.

Actionable intelligence and automated protections mean spending more time with those you protect and less time sifting through digital footprints and websites knocking down false positives.

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.

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.

Spearphishing simulation & mitigation

Enhance spearphishing simulations by targeting HVTs and individuals most at risk, and by leveraging real-time risk assessments and remediation guidance.

Impersonation attack prevention

Proactively prevent impersonation attacks against your employees and your company.

Schedule a demo

www.getpicnic.com