Minimize supply chain risk

With third-party data breaches at an all-time high, traditional risk management methods are insufficient.

Picnic's Third-Party Intelligence offers security teams and business leaders the tools to make informed decisions quickly regarding the companies within their organization's supply chain, reducing the risk of data breaches and safeguarding reputation.

In today's threat environment, where human attack surface data is being leveraged to breach organizations and the majority of system intrusion incidents come through an organization's partner, having the capability to manage the human attack surface of third-parties is essential. Picnic's technology allows companies to do this by proactively monitoring and remediating exposed third-party data and providing an enterprise-wide layer of prediction and prevention against attacks that impersonate trusted partners or leverage supply chain contractors' personally identifiable information.
Matt Polak, CEO, Picnic

Select Platform Capabilities, Services, & Use Cases

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.

Exposed enterprise data search & neutralization

Deny attackers the opportunity to leverage exposed enterprise data by responding quickly to breach data, improving social media OPSEC, and hardening your external attack surface.

SMS attack & phishing risk neutralization

Tackle smishing and phishing risk comprehensively before attacks even happen by reducing the human attack surface and addressing exposed data.

Schedule a demo