PICNIC™

HUMAN ATTACK SURFACE PROTECTION SERVICES

REDUCE ORGANIZATIONAL RISK BY 65%

getpicnic.com

WHAT IS PICNIC

For decades, organizations have invested in layers of security controls that are continually defeated by modern cyber threats. Threat actors circumvent these traditional perimeter defenses by leveraging open-source intelligence (OSINT) and preying on human vulnerabilities to gain initial access to corporate infrastructure or defraud customers and supply chain contractors.

Picnic offers a frictionless cybersecurity solution delivered as a **managed service** that protects against social engineering attacks. Picnic proactively and continuously disrupts attacker reconnaissance and resource development, **quickly reducing organizational risk by 65%.**

NO HARDWARE. NO AGENTS. NO HEADACHES.

PICNIC AUTOMATES THREE CORE ACTIONS

ANALYZE

Automatically expose social engineering attack and compromise paths before they happen

RECON

Emulate hacker reconnaissance of your enterprise's entire OSINT footprint

REMEDIATE

Neutralize vulnerabilities, reduce attack surface, and automate continuous risk detection and reduction

CHRIS KEY
Former CPO at Mandiant & Founder of Verodin

"Everyone knows the human element is the single largest attack vector and security risk. Picnic is the first solution I've seen that prioritizes who inside the organization will be targeted and how based on human attack surface data. I believe Picnic changes the game for security teams."

WHY PICNIC?

AUTOMATED PROTECTION

We do all the work beyond your perimeter and integrate with your existing security stack to drive prioritized and automated protections against the most commonly observed social engineering attacks, such as spear phishing, phishing, smishing, impersonation, and credential stuffing.

OUTCOMES-DRIVEN

We reduce your operating costs associated with detection and response by reducing organizational risk and the number of cybersecurity incidents. We do it through prediction and prevention, delivering remediations that harden your human attack surface to prevent operational interruptions and security incidents that negatively impact your organization's brand, reputation, and bottom line.

HUMAN-CENTRIC

The human element is the source of most cybersecurity incidents. We identify high-value and highly accessible human targets and pathways to compromise, and we predict and break potential attack chains.

THREAT-INFORMED

We prioritize threat intelligence and remediations by mapping them to your industry, people, and connected infrastructure. We focus on the threat actor tactics, techniques, and procedures that exploit breach data and human vulnerabilities.

FORCE MULTIPLIER

We increase cyber awareness and drive employee engagement by enabling learning through private and personalized human risk assessments and recommendations based on actual corporate and personal risk data.

ROBERT M. LEE
CEO at Dragos Inc.

"Social engineering is a key and growing threat to industrial organizations and Picnic offers important innovations to help the community strengthen its defenses. Picnic's team understands how threats perform reconnaissance and initial targeting against companies and has built a privacy-forward platform for organizations looking to strengthen their cybersecurity."

WHAT PICINIC DOES FOR YOU

Picnic emulates threat actor reconnaissance on both your human and enterprise attack surface, identifies pathways to compromise, and delivers prioritized remediations that disrupt attackers.

Preempt the single largest source of breaches. Secure work and personal identities, disrupt attacker reconnaissance and resource development, and protect your human element, business processes, and infrastructure.

Safeguard your people. Protect your high-value targets, employees, and contractors from being targeted or exploited by threat actors.

Prioritize defenses. Fill a critical security gap with targeted remediations informed by relevant and timely threat intelligence mapped to your workforce.

Personalize security coaching. Tailor education to combat real-world threats with data-driven, risk-based social engineering training and advanced spear-phishing simulations.

Quantify and reduce human cyber risk. Know and communicate your progress with comparative scoring and reporting capabilities that facilitate sharing with stakeholders at all levels.

SECURITY OUTCOMES DELIVERED VIA MANAGED SERVICES

HUMAN ATTACK SURFACE PROTECTION (HASP)

HASP offers a set of technical capabilities and business processes to continually evaluate the accessibility, exposure, and exploitability of the human element by threat actors active in your industry and to prioritize and implement preventive measures that improve your organization's security posture.

Working in tandem with Enterprise Attack Surface Protection, HASP disrupts the pre-attack tactics, techniques & procedures that are used by threat actors to gain initial access to corporate assets.

ENTERPRISE ATTACK SURFACE PROTECTION (EASP)

EASP offers capabilities and business processes to continually identify and prioritize external infrastructure vulnerabilities more likely to be exploited alongside human vulnerabilities in an attack chain.

It complements and completes the coverage of HASP by identifying, monitoring, and securing internet-connected assets the threat actor will likely aim to exploit in an attack chain.

Picnic reduces the volume and efficacy of social engineering attacks while fortifying your existing security systems

HUMAN ATTACK SURFACE PROTECTION (HASP)

HIGH-VALUE TARGET DIGITAL RISK PROTECTION SERVICES

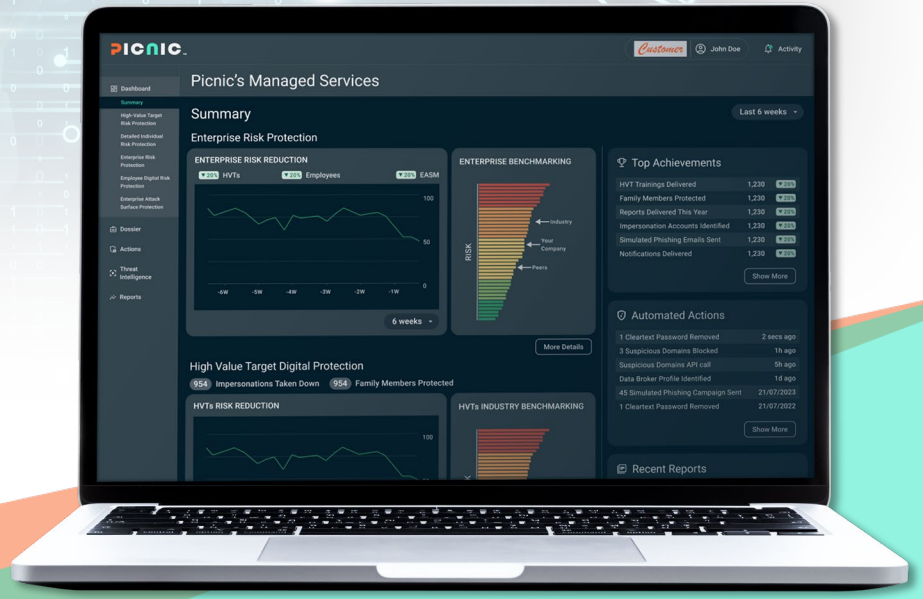
High-Value Targets (HVTs) are the most prominent figures in an organization and critical targets for social engineers. Picnic protects them and the enterprise from social engineering attacks by reducing the online human attack surface that fuels the campaigns that target them, their families, and extended support staff. HVTs may include executives, board members, and employees with privileged access to the organization's crown jewels.

Outcomes

- Continuous, automated monitoring and protection of personal and professional digital footprint
- 99% data broker removal
- 100% blocking of breached credentials associated with work and personal identities, as well as service accounts
- 100% risk identification for email spoofing (work email and personal email) with remediation support
- 100% identification and remediation of fraudulent social media accounts
- 90% smishing reduction, as reported by our HVTs
- Annual, personalized HVT risk report
- Real-time messaging about external footprint changes
- Extended protection to family members and support staff
- Personal EDR with ransomware, malware, and related threat protection
- Advanced red-teaming threat simulations

> We started protecting our top 50 executives and opted to extend coverage to 150 additional executives. Picnic not only cleans up their PII, but also reduces inbound attacks. Working with Picnic is easy with limited effort for my team.

Chief Information Security Officer
@ Fortune 100 Healthcare Company



HUMAN ATTACK SURFACE PROTECTION (HASP)

EMPLOYEE DIGITAL RISK PROTECTION SERVICES

Not all employees are considered High-Value Targets by threat actors, but many, if not most, are highly accessible online and easy targets. Attackers use them as a springboard to continue the reconnaissance of HVTs, moving laterally outside the traditional corporate perimeter. A highly-accessible employee can be tricked or coerced into performing actions that put the organization at high risk of compromise.

Outcomes

- Limit OSINT available to threat actors
- Increase the target's awareness of exposure and automated protections
- Extend protection to a family member

> After having Picnic for about six months, I no longer receive SMS-based scams. My employee-reported smishing incidents have decreased by 90%, too.

VP Information Security
@ Venture-backed Technology Firm

HUMAN ATTACK SURFACE PROTECTION (HASP)

BREACHED CREDENTIAL REUSE PROTECTION FOR WORK AND PERSONAL IDENTITIES

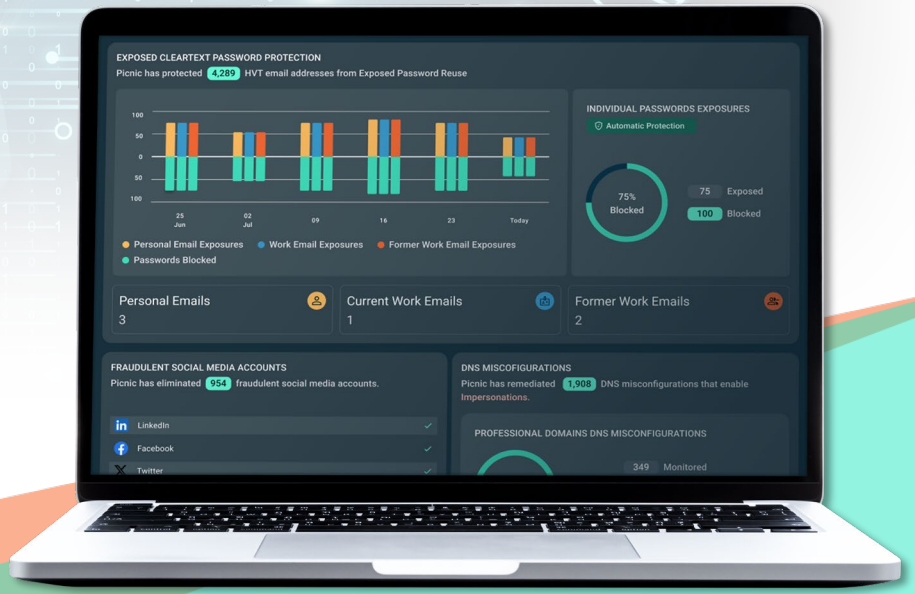
Many employees use the same passwords across their work and personal applications. Threat actors connect personal and work identities and leverage exposed credentials, including passwords associated with employee and contractor personal accounts, for credential-stuffing attacks that provide initial access to targeted infrastructure.

Outcomes

Picnic provides visibility and continuous monitoring of breach data to identify exposed corporate, personal, and third-party credentials and automatically prevents their reuse within the organization.

- Credential stuffing attack prevention
- Account takeover prevention

> Identity security is very important to our operation, and with Picnic's API, we automate credential reuse prevention and neutralize credential stuffing attacks without limitations. Picnic bridges the gap between work and personal identities, and I haven't seen any vendor doing this. Passwords are not going away, and you can't put MFA on everything.
>
> IT Security Leader
> @ Utilities Company



HUMAN ATTACK SURFACE PROTECTION (HASP)

TAILORED CYBER AWARENESS COACHING

Unlike generic cyber security awareness training that drives low employee engagement and questionable effectiveness, Picnic offers automated and highly targeted awareness coaching based on actual human risk data combined with threat intelligence. This methodology leverages relevancy, timeliness, and automated notifications to alert and educate employees at elevated risk of being subject to social engineering.

Outcomes

- Protection against phishing, smishing, vishing, and related social engineering attacks through increased awareness
- Increased awareness of personal exposure that educates about good security practices and cyber hygiene at home and work
- “Lunch with a hacker” in-person events

ENTERPRISE ATTACK SURFACE PROTECTION (EASP)

EXTENDING HASP COVERAGE TO BREAK ATTACK PATHWAYS

Enterprise Attack Surface Protection is a critical extension of Picnic's playbook to provide comprehensive pre-attack risk identification and timely protective measures. It leverages threat intelligence prioritization, human risk data, and targeted remediations to inform vulnerability patching priorities and disable attacker infrastructure.

Outcomes

- Protection against impersonation attacks using company email
- Protection against phishing attacks targeting employees, customers, and suppliers
- Dark web monitoring for corporate service accounts and domains
- Protection against infrastructure-based attacks, including those using known vulnerabilities
- Stealer malware exposure checks
- Identification and prioritization of exposed services with exploitable vulnerabilities

> Having a partner who watches over us beyond our perimeter defenses and helps us harden our external attack surface gives us peace of mind. Picnic combines many disparate types of attack data into a cohesive threat graph to understand the interplay between exposed assets and the human element.

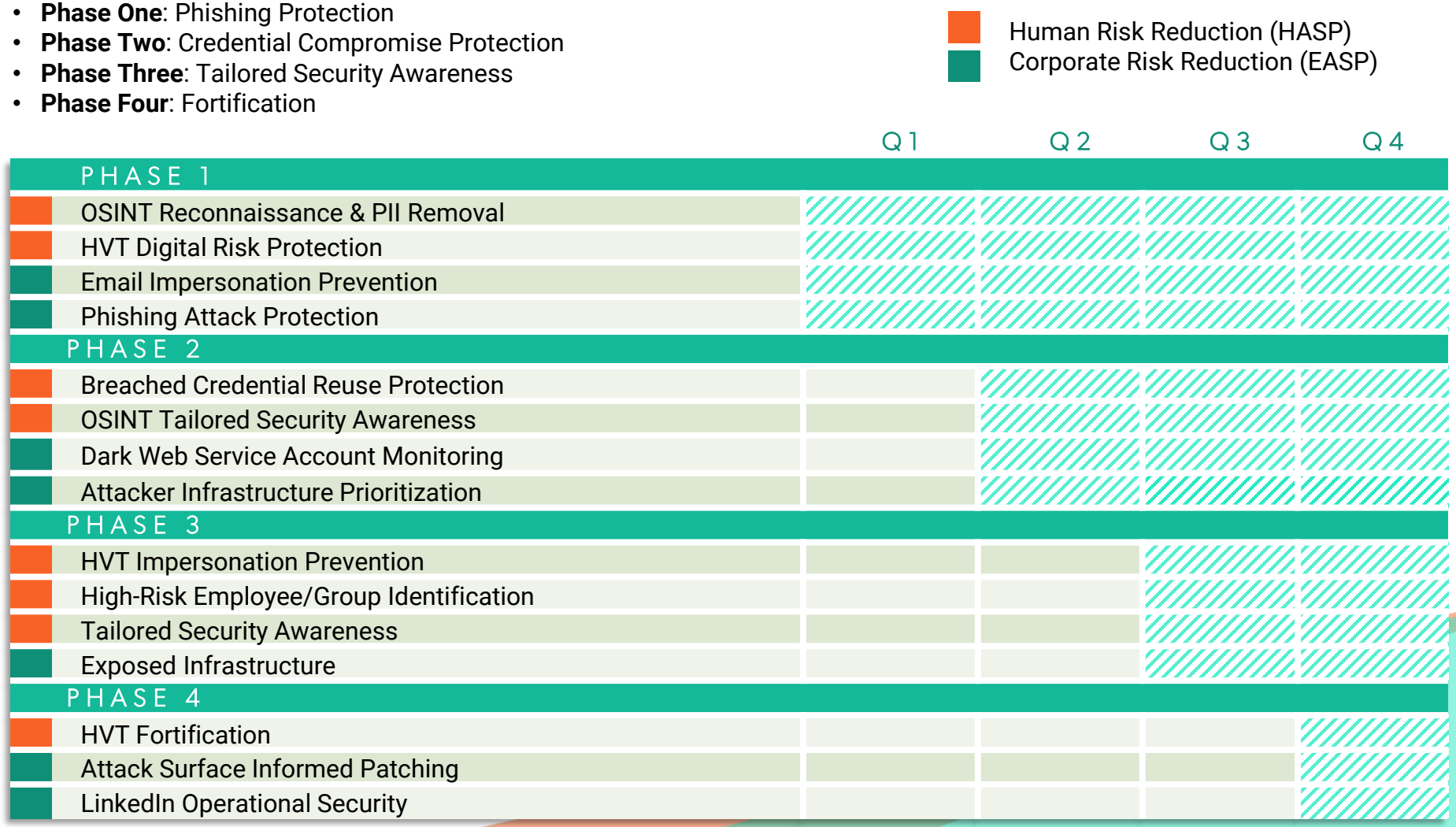
Security Leader
@ Fortune 500 Financial Services Company

PROGRAM TIMELINE

Tell us what's important for your organization, and we'll tailor a program that meets your cybersecurity goals.

A typical program consists of four phases, each emphasizing specific focus areas:

- **Phase One**: Phishing Protection
- **Phase Two**: Credential Compromise Protection
- **Phase Three**: Tailored Security Awareness
- **Phase Four**: Fortification



READY TO GET STARTED?

Start the journey by reducing organizational risk by 10% in the first month and by 65% in less than a year. Tell us what's important for your organization, and we'll tailor a program that meets your cybersecurity goals.

Schedule a meeting @
getpicnic.com/request-demo

Schedule Meeting

Follow us on

PICNIC™

getpicnic.com