PRODUCT BROCHURE

Dark Web ID

24/7 Dark Web Credential Monitoring & Threat Intelligence

Your employees' credentials may already be for sale on the dark web. Dark Web ID monitors continuously — so you know the moment your organization's data appears, before attackers can weaponize it.

24B+	80%	207	500+
credentials exposed on dark web marketplaces	of breaches use stolen credentials	days avg to detect a breach without monitoring	IRC channels and forums monitored 24/7

Degarmo Technologies | degarmo.tech | July 2026

THE THREAT

Your Credentials Are Already Out There

Stolen credentials are the #1 attack vector — and most organizations have no idea they're exposed.

HOW CREDENTIALS END UP ON THE DARK WEB

Every employee uses dozens of online accounts — work tools, personal services, industry sites. When any one of those third-party services is breached, the credentials your employees used there are harvested and sold on dark web marketplaces. Those credentials — especially if passwords are reused — can then be used to access your business systems directly.

THE ATTACK TIMELINE

Stage	What Happens	Time Frame
Breach	Third-party vendor or site your employee used gets hacked	Day 0
Harvest	Stolen credentials packaged and listed for sale on dark web	Hours–Days
Purchase	Cybercriminal purchases credential dump for pennies per record	Days–Weeks
Attack	Automated credential stuffing against Microsoft 365, VPNs, business systems	Ongoing
Discovery	Organization discovers breach — without monitoring	Average: 207 days
With Dark Web ID	**Degarmo alerts you within minutes of credentials appearing**	**Minutes**

The Solution: Know Before They Strike

Dark Web ID gives you advance warning — minutes after your credentials appear on the dark web, not months after attackers have already moved through your systems.

HOW DARK WEB ID WORKS

The Most Comprehensive Dark Web Monitoring Available

600,000+ sources. 500+ IRC channels. 10,000+ daily queries. Human-verified intelligence.

WHAT GETS MONITORED

Source Type	Scope	Frequency
Dark web forums & marketplaces	600,000+ sites	24/7 continuous
IRC hacker channels	500+ channels	Real-time
Paste sites (Pastebin, etc.)	All major platforms	Continuous
Private dark web exchanges	Invite-only communities	Human intelligence
Historical breach databases	All known breach data	On-demand search

WHAT HAPPENS WHEN CREDENTIALS ARE FOUND

Alert Generated Within Minutes

The moment matching credentials appear in any monitored source, an automated alert is generated. Speed is critical — the faster you know, the faster you can act.

Degarmo Reviews the Finding

Every alert goes through our security team before reaching you. We assess severity, add business context, and confirm the finding is actionable — no noise, no false alarms.

Clear Guidance Provided

We contact your designated point of contact with specific instructions: which accounts to reset, whether to activate MFA, and whether to investigate for compromise.

Incident Documented

All alerts and responses are documented for compliance purposes — providing an audit trail for cyber insurance, HIPAA, PCI, and NIST requirements.

Degarmo's Managed Response

Every Dark Web ID alert triggers our response workflow. We handle the investigation so you don't have to interpret raw threat intelligence data. You get the answer — not just the alarm.

COMPLIANCE & BUSINESS VALUE

Satisfy Auditors. Lower Premiums. Protect Revenue.

Dark web monitoring is no longer optional — it's a compliance requirement and cyber insurance prerequisite.

COMPLIANCE FRAMEWORK ALIGNMENT

FRAMEWORK	REQUIREMENT	COVERAGE
NIST CSF — Identify	ID.RA — Risk Assessment	✓ Active threat intelligence input
HIPAA Security Rule	Risk Analysis §164.308(a)(1)	✓ Credential breach evidence
PCI DSS v4.0	Req. 12.10 — Incident Response	✓ Breach detection & alerting
SOC 2 Type II	CC7.2 — Threat Monitoring	✓ Continuous monitoring evidence
Cyber Insurance	Dark web monitoring requirement	✓ Program reports for underwriters

THE BUSINESS CASE

Without Dark Web Monitoring

207-day average detection time. Attackers move freely through systems. $4.9M average breach cost. Cyber insurance premium spikes or non-renewal.

With Dark Web ID

Minutes to detection. Password reset stops the attack before it starts. Breach costs avoided. Insurer sees documented proactive monitoring.

One Prevented Breach Pays for Years of Monitoring

The cost of Dark Web ID is a fraction of the average breach cost. For most organizations, a single prevented incident more than justifies the investment — and that doesn't include reputational damage, customer churn, or compliance penalties.

DELIVERED BY DEGARMO TECHNOLOGIES

We configure, monitor, alert, and respond — on your behalf. You get enterprise-grade dark web intelligence with the responsiveness of a boutique, veteran-owned security partner. Same-day support. Human-reviewed alerts. Clear guidance every time.

Know Before Attackers Strike

Degarmo Technologies can run a free Live Data Search on your domains right now — showing you exactly what dark web exposure exists for your organization today. No commitment required.

- **Free Dark Web Scan — Results in 24 Hours**
- **Same-Day Support**
- **No Obligation**

Visit degarmo.tech | Oklahoma City, OK | Veteran-Owned MSSP