eSENTIRE

DATA SHEET

eSentire Dark Web Monitoring

Extend visibility for early detection of compromised credentials, minimize unauthorized access, and avoid costly data breaches.

Protect your brand, executive team, employees, and your sensitive corporate data across the Dark Web

Get continuous monitoring and broad visibility into the Dark Web to protect your executives, employees, and customers' sensitive data before it's used maliciously by threat actors.

We collect data from a wide range of sources including content from limited-access Deep Web & Dark Web forums, cybercrime marketplaces, invite-only messaging groups, code repositories, paste sites, and clear web platforms. We enrich them with context for our SOC teams to act on.

Correlate and predict threat actor moves to extend visibility into early Indicators of Compromise

Actively monitor Dark Web forums and channels to identify early indications of potential attacks, such as discussions about new malware, exploits, or stolen data.

eSentire MDR customers also gain contextual awareness into threat investigations that go beyond multi-signal telemetry, providing visibility into threat actor TTPs in the Dark Web.

Extend your team with our industry-leading eSentire Threat Response Unit (TRU)

Go beyond simple alerting and guided remediation actions with the support of eSentire's Threat Response Unit (TRU), a team of industry experts that has actively collaborated with law enforcement agencies to hunt and shut down well-known cybercriminals and ransomware gangs.

Unlike other providers, we leverage threat intelligence gathered from the Dark Web to take actual response actions, disrupt cyberattacks, and put our customers ahead of disruption.

Your Challenges

The Dark Web is an important hub for threat actors, where they sell leaked sensitive data, plan cyberattacks, and regularly publish attacker tools on various cybercrime marketplaces and private forums. Although rapid detection and identification of this exfiltrated data is valuable, manually analyzing the Dark Web is a time-consuming, arduous task that in-house security teams struggle to take on. In addition, your security team may not have the experience and expertise necessary to identify subtle patterns within conversations that may provide early indicators of a potential cyberattack.

You need a partner that goes beyond alerting to bring context to your data in the Dark Web in order to identify your vulnerabilities, prioritize, and address key areas of risk, and build resilience against future cyberattacks.

Our Solution

eSentire Dark Web Monitoring extends visibility beyond your on-premises and cloud environments to detect compromised user credentials, corporate sensitive data, and early indicators of potential cyber threats to protect your brand, executive team, and employees.

24/7 monitoring across the Dark Web identifies early indicators of potential cyber threats, indicators of compromise (IOCs), and tactics, techniques, and procedures (TTPs) that threat actors rely onto conduct sophisticated cyberattacks. In addition, we provide contextual awareness into known and unknown threat actor groups in the Dark Web for deeper threat investigations by observing forum discussions, recognizing communications patterns used within conversations, and using this intelligence to build a timeline to inform our threat response actions.

How We Help

- Enhanced visibility and alerting on compromised credentials, mentions by Initial Access brokers, or discussions of a targeted cyberattack
- 24/7 monitoring for leaked credentials of your top executives and key personnel
- Identification of potential phishing campaigns, domain infringement practices, and other malicious activities
- Proactive monitoring of third-party and supply chain vendors to manage, and reduce, supply chain risk
- Identification of employees, or other insiders, who are acting with malicious intent to violate security policies or sell their credentials/access on the Dark Web

Your Outcomes

- Avoid potential financial loss and minimize the impact of a security breach through:
  - Early detection of compromised user credentials
  - Rapid containment of threats by identifying and responding to threats quickly
  - Minimizing unauthorized access into your environment
- Stay ahead of the latest industry trends by accounting for any credential leaks on the Dark Web, discussion of phishing campaigns, and observing threat actor discussions so you can make informed decisions about your security strategy

The Value of Integrating eSentire Dark Web Monitoring Services with MDR

While eSentire's Managed Detection and Response services continuously monitor and respond to potential threats in your environment 24/7, our Dark Web Monitoring services go beyond your environment to monitor for potential threats and alert you on the earliest indicators of risk. This allows us to correlate your business's internal security context with our deep and dark web threat intelligence which informs our Elite Threat Hunters on what to look for, enabling them to conduct proactive threat hunts.

Moreover, eSentire MDR customers can also leverage the eSentire Threat Response Unit (TRU) and the eSentire Cyber Resilience Team for regular reports on relevant Dark Web alerts, get informed on industry-specific risk areas, participate in live TRU threat intelligence briefings, and more.

Additional Service Benefits Include:

- ✓ **24/7 monitoring of Dark Web activity:** Track key forensic evidence such as leaked credentials, cybercriminal activity, and second stage ransomware attacks by gaining access to external threat intelligence.

- ✓ **Alerting and investigation of security incidents:** Get actionable recommendations for new activity appearing on the Dark Web, social media platforms, or other malicious sources. If a breach-related security alert is generated, we also provide contextual awareness to our 24/7 SOC Cyber Analysts and complete support until the threat is resolved.

- ✓ **Correlated internal deep forensic investigations:** Get stronger correlation of external and internal risk indicators for better context into the potential cyber threat.

- ✓ **Extensive resources from the Deep, Dark, and Clear Web:** Gain access into the Deep Web & Dark Web forums, illicit underground cybercrime marketplaces, invite-only instant messaging groups (e.g., Telegram, Discord, QQ, etc.), code repositories, paste sites, clear web sources, and an indexed, searchable archive of historical data from as early as the 1990s.

- ✓ **Reporting:** Get comprehensive quarterly reporting on findings with tactical recommendations.

- ✓ **Engage with an eSentire expert:** Stay ahead of the latest threat trends on the Dark Web and the evolving attacker TTPs to make informed decisions about your security strategy.

Why Choose eSentire for Dark Web Monitoring

Gain Stronger Response Actions When Combined with eSentire MDR

Rather than being overwhelmed with alerts generated by traditional Dark Web Monitoring tools, we provide contextual awareness and actively respond to threats on your behalf. We also integrate Dark Web intelligence in our MDR threat investigations to deliver faster response capabilities.

Proven Partnership with Law Enforcement Agencies

Our industry-renowned Threat Response Unit (TRU) works closely with law enforcement agencies to hunt and take down threat actors on the Dark Web.

Comprehensive Coverage

We collect from 700+ sources from the Deep Web and Dark Web, which is 80% more than what our competitors collect.

Cost-Effective, Tiered Approach

We align with your organization's security goals, budget and maturity with tiered offerings including Credential Monitoring, and Advanced Dark Web Monitoring.

Ready to get started?

Connect with an eSentire Security Specialist to learn how you can build a more resilient security operation and prevent disruption.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US ☎ 1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit www.esentire.com and follow @eSentire.