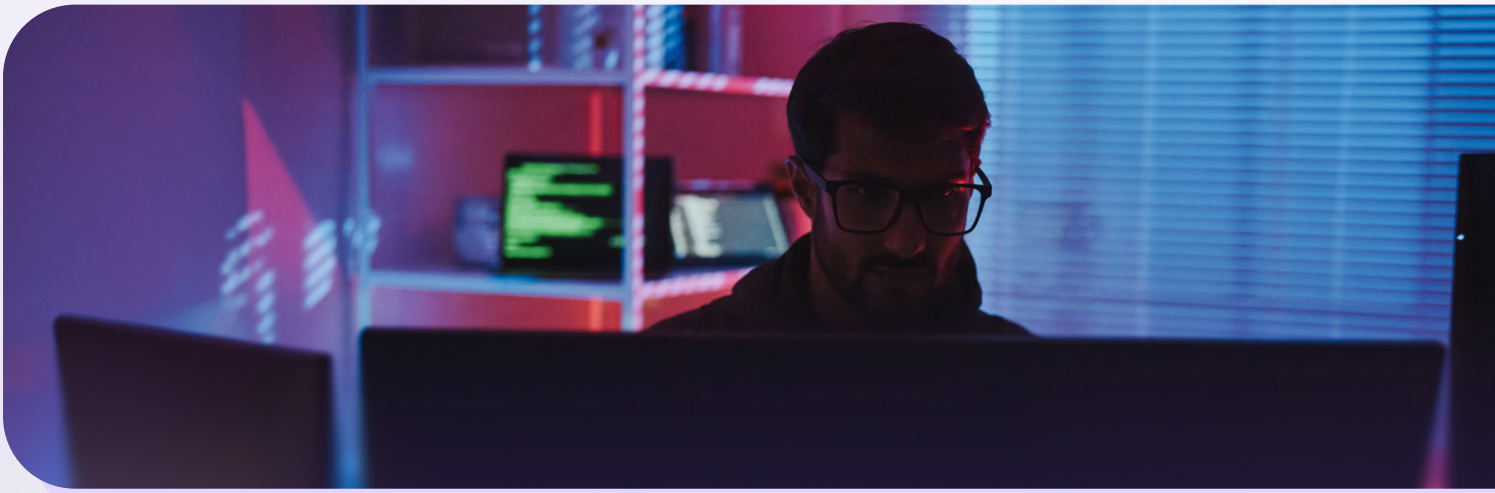
Ontinue

SOLUTION BRIEF



ION FOR DARK WEB MONITORING

The External Risk Outside Your Security Perimeter

Your organization's exposure extends beyond the systems, identities, and domains you control. Compromised credentials, corporate credentials exposed through third-party services, and lookalike domains can create risk before they lead to malicious activity or become visible to your security team.

Reduce Exposure Before It Becomes an Incident

Identify external exposure earlier, focus on what matters, and act before attackers can exploit it.

ION for Dark Web Monitoring extends your existing ION MXDR service to identify compromised credentials, typosquatting domains, and other external risks. Ontinue investigates and prioritizes relevant findings, then initiates pre-agreed response workflows through the same security operations and team already supporting your organization.

You gain greater visibility and faster risk reduction without another platform, deployment project, or vendor relationship.

What Makes Us Different

Act Earlier on Exposed Credentials
Identify compromised credentials sooner, giving your team more opportunity to reset passwords, revoke active sessions, or take other appropriate action before attackers can use them.

Your Outcomes With Ontinue ION for Dark Web Monitoring

Minimize risk from exposed credentials
Continuously uncover exposed credentials associated with your organization, reducing the likelihood of compromise and limiting attacker advantage.

Turn threat intelligence into action
Stay ahead of newly exposed data with ongoing monitoring, transforming findings into investigated, actionable incidents with response actions integrated into your existing MXDR workflows.

Uncover threats beyond your environment
Extend visibility beyond your security perimeter to identify external exposures and emerging risks before they become security incidents.

Reduce Impersonation Risk

Identify lookalike domains that could be used to impersonate your organization or target your employees and customers.

Focus Your Team on What Requires Action

Receive validated incidents with relevant context and a clear recommended next step, rather than another stream of unprioritized threat intelligence.

Extend Protection Beyond Your Environment

Identify risks originating outside your security perimeter that existing controls may not detect.

Why Customers Choose ION for DWM

Investigated, Not Just Detected

Dark web monitoring alerts alone leave your team to determine what matters and what to do next. ION for DWM validates potential exposures, assesses their significance, and provides the context your team needs to act.

Response Built In

Validated findings enter your existing ION MXDR workflows, enabling coordinated response without creating another process for your team to manage.

No Additional Security Silo

Gain external exposure monitoring through the platforms, workflows, and Ontinue team you already rely on, without adding another standalone solution.

Backed by 24/7 Expertise

The same Cyber Defense Center supporting your ION MXDR service monitors external exposure and investigates relevant findings 24/7, without requiring your organization to build a specialist monitoring function.

Ontinue

Ontinue offers nonstop SecOps through an AI-powered managed extended detection and response (MXDR) service. Ontinue ION MXDR combines powerful proprietary AI with the industry's first collaboration with Microsoft Teams to continuously build a deep understanding of our customers' environments, informing how we prevent, detect, and respond to threats.

Continuous protection. AI-powered Nonstop SecOps. That's Ontinue.

CONTACT US