The Morphick Managed EDR Compromise Assessment will identify any evidence of an active or recent security breach in your environment by combining Endgame’s industry-leading endpoint detection and response platform with advanced threat hunting services performed by NSA-CIRA accredited analysts.

Morphick threat hunters will uncover the most difficult to locate threats, whether attackers use malicious programs, malwareless techniques, or stolen credentials to traverse your environment and target proprietary data.

THE MORPHICK MANAGED EDR COMPROMISE ASSESSMENT DELIVERS:

- Complete analysis of all endpoints
- Identification of compromised systems
- Detailed description of attacker activity and extent of compromise
- Actionable findings and recommendations to remediate and prevent future compromise.

SERVICE DESCRIPTION

The length of the Morphick Compromise Assessment varies depending on the size of your organization’s environment. In most cases, the service is executed over a 6-week period.

- **Weeks 1-2** – Technology Deployment and Preparedness:
  Morphick deploys Endgame’s dissolvable endpoint sensors to provide immediate and comprehensive threat visibility.

- **Weeks 3-5** – Threat Identification and Discovery:
  Morphick identifies the presence of active attackers, artifacts from recent attacks, data exfiltration, and any suspicious behavior. Morphick threat hunters continuously monitor endpoint activity to accurately and quickly detect suspicious behavior. In the event of compromise, Morphick immediately notifies your team to ensure quick and effective response.
▪ **Week 6 – Actionable Recommendations:**
Morphick provides a detailed report outlining the analysis performed and key findings, including any evidence of active or recent compromise. Morphick provides your organization with specific recommendations to ensure you are protected moving forward.

**Managed by Morphick’s 24x7 Threat Intelligence Center Experts.** Compromise Assessment services are delivered by Morphick’s 24x7 US-Based Security Operations Center.

**Powered by Endgame’s Zero Breach Tolerance EDR Platform.** The Endgame platform applies machine learning and other advanced techniques to provide the industry’s deepest and most accurate inspection across every layer of the endpoint via dissolvable sensors.

**Proactive Threat Hunting.** Morphick’s threat hunters locate and analyze threats that have evaded your security controls. This service combines Endgame’s leading EDR platform with Morphick’s proprietary capabilities to uncover even the most difficult to locate cyber threats.

---

**ABOUT MORPHICK**
Morphick provides security Managed Detection and Response (MDR) services to organizations globally. Morphick’s proven approach combines attack detection, threat hunting, incident response, and tailored threat intelligence to deliver morphing defensive postures. The Morphick service provides multiple types of network security monitoring, full packet capture, and endpoint threat-hunting capabilities. All events are aggregated on the Morphick Defense Platform and are monitored, validated, and remediated by US-based dedicated security analysts in the Morphick Threat Intelligence Center. Organizations can also leverage Morphick’s NSA CIRA-Accredited Incident Response services for breach response support. Morphick provides threat intelligence for deep intelligence gathering and analysis, and other incident response services such as malware reverse engineering and customer signature development.

---

**ABOUT ENDGAME**
Endgame is a leading endpoint security platform that enables enterprises to close the protection gap against advanced attacks and detect and eliminate resident adversaries. Endgame transforms security operations teams and incident responders from crime scene investigators into hunters that prevent damage and loss, and dramatically reduce the time and cost associated with incident response and compromise assessment. Our IOC-independent platform covers the entire kill chain, leveraging machine learning and data science to uncover, in real-time, unique attacks that evade traditional defenses and respond precisely without disrupting normal business operations.