

Adaptive Recovery – Forensic Recovery

Secure Log Recovery and Incident Investigation

Morphisec's **Forensic Recovery** is a core feature of the **Adaptive Recovery** component within the **Anti-Ransomware Assurance Suite**. It proactively secures critical forensic data during ransomware attacks, preserving visibility into the attack's progression. By capturing and safeguarding volatile evidence—such as security events, application activity, and system behavior—it ensures key indicators remain available for investigation and recovery, even if attackers attempt to tamper with or erase them. This capability reduces response time, facilitates root cause analysis, and supports full recovery efforts.

Key Benefits



Proactive Forensic Data Protection

- + Secures critical forensic information during ransomware attacks to prevent tampering and ensure availability for investigations.
- + Implements immutable logging by storing logs in a tamper-proof location, ensuring preservation at all times.



Comprehensive Attack Visibility

- + Tracks attacker entry points, lateral movements, and privilege escalations.
- + Provides a clear timeline of the attack, aiding root cause analysis, recovery efforts, and strengthening adaptive cyber resiliency efforts.



Tamper-Proof Storage

- + Encrypts and stores forensic data in a secure, tamper-resistant format, ensuring data integrity.



Enhanced Incident Response

- + Enables faster investigation, recovery, and remediation by preserving actionable evidence; remediate vulnerabilities exploited during the attack.



Improved Compliance and Reporting

- + Facilitates regulatory compliance by providing secure, tamper-proof access to preserved logs for forensic investigations and audits.
- + Demonstrates accountability under frameworks such as GDPR, HIPAA, SOX, PCI DSS, and others.



Alignment with the MITRE Framework

- + Fully compliant with **MITRE ATT&CK Techniques T1070.001** and **T1562.002** to prevent and detect log tampering.

How It Works

Forensic Recovery operates by continuously safeguarding critical forensic signals—such as system events, application-specific activities, and attacker behaviors—into secure, tamper-resistant storage. This ensures visibility and integrity while enabling investigators to reconstruct the attack timeline and analyze tactics, techniques, and procedures (TTPs).

Morphisec's Forensic Recovery is a breakthrough solution for organizations combating ransomware threats. Unlike traditional methods that fail to preserve critical forensic evidence, Morphisec proactively secures forensic data during an attack.

By safeguarding volatile evidence and maintaining the integrity of key indicators, it enables faster investigations, root cause analysis, and complete recovery. This ensures that forensic insights remain intact, reducing response time and strengthening your organization's defenses against future attacks.

Get Started with Morphisec Adaptive Recovery

Morphisec's **Forensic Recovery** is available as part of the **Anti-Ransomware Adaptive Recovery Suite**. Protect your business from ransomware disruptions. With Forensic Recovery, you can ensure critical forensic data is preserved and accessible, enabling faster investigations and comprehensive recovery while maintaining adaptive cyber resilience.



See Morphisec in action

Stop ransomware with our
Preemptive Cyber Defense Platform

[Get a demo](#)

About Morphisec

Morphisec is the trusted global leader in prevention-first Anti-Ransomware protection, redefining cybersecurity with our industry-leading Automated Moving Target Defense (AMTD) technology. Our solutions are trusted by over 7,000 organizations to protect more than 9 million endpoints worldwide, stopping 100% of ransomware attacks at the endpoint and safeguarding businesses against the most advanced and dangerous threats, including zero-day exploits and ransomware.

At Morphisec, we don't just fortify defenses – we proactively prevent attacks before they happen, delivering unmatched protection and peace of mind to our customers. With our Ransomware-Free Guarantee and commitment to Preemptive Cyber Defense, we set the standard for accountability and innovation in the fight against modern cybercrime.

As a rapidly growing company, we are dedicated to empowering security professionals and organizations to adapt, protect, and defend against ever-evolving threats. Join us in shaping the future of cybersecurity with prevention-first strategies and unparalleled expertise.

To learn more, visit morphisec.com