

Morphisec Launches Data Exfiltration Control, a Major Expansion of It's Data Exfiltration Protection Capability

New Anti-Ransomware Assurance Suite Add-on Gives Security Teams Deterministic Control Over AI and Dual-use Tools to Stop Data Theft

NEW YORK, NY, UNITED STATES, September 23, 2026 /EINPresswire.com/ -- [Morphisec](#), a global

“

Data Exfiltration Protection gave every customer an automatic safeguard against ransomware-driven theft. Data Exfiltration Control is the giant leap forward; it puts security teams in command”

*Kobi Katzir, Head of Product
at Morphisec*

leader in prevention-first cybersecurity and anti-ransomware protection, today announced the general availability of Data Exfiltration Control (DXC), a significant expansion of its [Data Exfiltration Protection](#) capability and a major leap forward for the Anti-Ransomware Assurance Suite. DXC gives security teams policy-driven, enterprise-grade governance over the data-transfer tools used in modern double-extortion attacks, with zero content inspection, and on the same Morphisec Protector they already run.

Ransomware has shifted from locking data to stealing it. According to Sophos's State of Ransomware 2025, 77% of

ransomware intrusions exfiltrated data in 2025, up from 57% the prior year. Travelers reports that 87.6% of ransomware claims now involve double extortion, and Unit 42's 2026 Global Incident Response Report found that the fastest attackers reached first data exfiltration within 72 minutes of breaking in. Backups can restore encrypted systems, but they cannot un-leak stolen data and the breach-notification clock starts the moment data leaves.

Morphisec introduced Data Exfiltration Protection in 2025 as an included capability that automatically blocks ransomware-driven data theft using the company's patented [Automated Moving Target Defense](#) (AMTD) technology. Data Exfiltration Control builds directly on that foundation, expanding DXP from an automatic safeguard into a full, policy-driven control plane for outbound data movement.

“Data Exfiltration Protection gave every customer an automatic safeguard against ransomware-driven theft. Data Exfiltration Control is the giant leap forward; it puts security teams in command,” said Kobi Katzir, Head of Product at Morphisec. “Every supported tool starts in

Monitor Mode, so teams can see exactly what is leaving and where, then move to Preventive Mode with one-click allow rules. There is no content to classify and no months-long DLP project. It is deterministic from day one, on the agent they already run.”

Key capabilities of Morphisec Data Exfiltration Control include:

- Per-tool enforcement — Govern supported exfiltration tools (including rclone, AzCopy, WinSCP, MegaSync, and the AWS CLI) individually, with Monitor, Alert, or Terminate actions.
- Deterministic allow/block — Decisions are based on process context and network destination (root domain), with zero content inspection.
- Monitor-to-Preventive workflow — Baseline normal activity silently, then enforce, with one-click allow rules by domain, account, and host.
- Activity visibility and audit-ready incidents — Outbound transfers are grouped by tool and destination, with Critical-severity Exfiltration Violation incidents mapped to MITRE ATT&CK techniques T1567.002, T1537, and T1020.
- Cross-platform coverage — Windows, Linux, and macOS, managed centrally in the Morphisec Security Center alongside anti-ransomware.

“Attackers weaponize the same trusted tools your administrators use every day, which is exactly why detection and traditional DLP miss them,” said Michael Gorelik, Chief Technology Officer at Morphisec. “Data Exfiltration Control ties data-theft prevention to the ransomware kill chain, stopping exfiltration upstream of encryption. It is signatureless, deterministic, and requires no second agent, which is consistent with the prevention-first approach that defines everything we build.”

Unlike content-inspection data loss prevention, which can require thousands of classifiers and months of tuning, Data Exfiltration Control governs dual-use tools by what they are and where they are sending data, delivering protection on day one. As a module on the Morphisec Protector, it adds no new agent and no new console.

Data Exfiltration Control is available now as a licensed add-on to Morphisec's Anti-Ransomware Assurance Suite, with full Monitor and Preventive enforcement on Windows and expanding coverage across Linux and macOS. Like all Morphisec protection, it is backed by the company's Ransomware-Free Guarantee.

Organizations can request a demo at <https://www.morphisec.com/demo>.

About Morphisec

Morphisec is the global leader in prevention first cybersecurity and anti ransomware protection, delivering preemptive cyber defense that stops advanced attacks before execution. Founded in 2014 and headquartered in New York, Morphisec protects millions of endpoints across the finance, healthcare, manufacturing, and technology sectors, reducing dwell time, false positives, and incident response costs. With its Ransomware Free Guarantee and commitment to adaptive

cyber resilience, Morphisec is redefining how enterprises stay protected in an AI accelerated world. Learn more at www.morphisec.com.

Jeff Anderson

Morphisec

+1 617-826-1212

[email us here](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/944345663>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.