

Data Exfiltration Protection & Control

Stop data theft before it becomes a breach – in two layers, on one agent

The Challenge

Ransomware has changed. Encryption is no longer the point – leverage is. Attackers exfiltrate data first and threaten to leak it, so even a flawless backup can't make the problem go away. Double extortion is now the default, 77% of 2025 ransomware intrusions stole data before anything else, and the fastest attackers reached first exfiltration in as little as 72 minutes.

- **Backups can't un-leak data** – Recovery restores operations, but the moment data leaves, the breach-notification clock – and the regulatory exposure – has already started.
- **EDR sees generic processes** – Detection tools watch for malware behavior; they can't tell a legitimate rclone or AzCopy transfer from an attacker staging exfiltration.
- **DLP is a classification project** – Content-inspection DLP needs thousands of classifiers and months of tuning, and still misses the dual-use admin tools attackers actually use.

The Solution

Morphisec defends against data exfiltration in two layers, on the agent you already run. Data Exfiltration Protection (DXP) is included with Anti-Ransomware and automatically stops ransomware-driven data theft before it begins – signatureless, powered by AMTD. Data Exfiltration Control (DXC) is a paid add-on that adds policy-driven governance over the dual-use tools used to move data out: deterministic Allow/Block by process context and network destination, with zero content inspection. Both are part of Impact Protection.

Stops Data Theft Including:

- Ransomware-driven exfiltration across the top MITRE exfiltration and impact techniques
- Dual-use transfer tools – rclone, AzCopy, WinSCP, MegaSync, AWS CLI, and more
- Uploads to unsanctioned cloud storage and command-and-control destinations

Core capabilities

- ✓ **Automatic Exfiltration Prevention (DXP)** – Signatureless, prevention-first blocking of ransomware-driven data theft – included, always on.
- ✓ **Per-Tool Policy Enforcement (DXC)** – Govern each supported exfil tool independently: Monitor, Alert, or Terminate, by process + destination.
- ✓ **Deterministic Allow Rules (DXC)** – Allow by domain + account + host, with one-click baselining from the Activity view – no content inspection.
- ✓ **Activity & Audit Visibility (DXC)** – Outbound transfers grouped by Tool → Root Domain; Critical-severity, MITRE-mapped incidents with full audit log.
- ✓ **Cross-Platform, One Agent (DXP + DXC)** – Windows, Linux, and macOS, managed in the Morphisec Security Center alongside anti-ransomware.

Benefits

- + **Close the other half of ransomware** – Anti-Ransomware stops encryption; DXP and DXC stop the data theft that drives double extortion.
- + **Governance without a DLP project** – Block dual-use tools deterministically – zero classifiers, zero months of tuning.
- + **Safe for legitimate admins** – Every tool starts in Monitor; allow-list real workflows in one click before enforcing.
- + **Breach-notification defensibility** – Audit-ready, MITRE-mapped evidence of what was blocked and when.
- + **No new agent** – Both layers ride the Protector you already run.

DXC vs. Traditional DLP

Capability	Traditional DLP	Morphisec DXC
Decision basis	Content classification	Process context + network destination
Time to value	Months of tuning, 1,000s of classifiers	Deterministic from day one
Dual-use admin tools	Often missed or over-blocked	Governed per tool, with allow rules
Deployment	Separate DLP stack	Module on the agent you already run
Incident output	Policy alerts to triage	Critical, MITRE-mapped exfiltration incidents

Included vs. Add-On: How DXP and DXC Fit

Capability	DXP (Included)	DXC (Add-On)
Scope	Ransomware-driven data theft	Outbound transfers by supported exfil tools
Control model	Automatic safeguard	Policy-driven, per-tool enforcement
Visibility & allow rules	Built-in prevention	Activity view + domain/account/host allow rules
Modes	Always-on prevention	Monitor → Preventive

The Morphisec Difference.

Prevention-First by Design. Deterministic by Nature.

DLP tries to read your data; detection tries to recognize the attack after it starts. Morphisec does neither. DXP stops ransomware-driven theft before it executes, and DXC governs the tools that move data out by what they are and where they're sending – deterministically, on the agent already deployed across your fleet.

Ransomware-free Guarantee

Peace of mind, proven in practice. Morphisec backs its prevention with an industry-first Ransomware-Free Guarantee:



100% Money-Back Assurance

Full reimbursement of subscription fees if a ransomware breach occurs on a protected endpoint.

Expert Incident Support

A dedicated Morphisec Incident Response team for rapid containment, forensic investigation, and remediation.

Ransomware-Free Guarantee

Peace of Mind, Proven in Practice

Morphisec offers an **industry-first Ransomware-Free Guarantee**:

- **100% Money-Back Assurance:** Full reimbursement of subscription fees if a ransomware breach occurs on a protected endpoint.
- **Expert Incident Support:** Dedicated Morphisec Incident Response team for rapid containment, forensic investigation, and remediation.

Stop the data theft that drives extortion.

See Data Exfiltration Protection and Control in action today.

[Get a Demo](#)

About Morphisec

Morphisec is the global leader in prevention-first cyber defense and anti-ransomware protection, trusted by 7,000+ organizations to protect 9M+ endpoints. Powered by Automated Moving Target Defense (AMTD), Morphisec stops attacks before execution. Data Exfiltration Protection and Control are part of Impact Protection within the Anti-Ransomware Assurance Suite, backed by Morphisec's Ransomware-Free Guarantee. At Morphisec, we don't just respond – we prevent.