

Data Exfiltration Protection & Control

Two layers of prevention-first exfiltration defense – DXP included, DXC for governance

Modern ransomware has flipped the script: attackers steal data first, then encrypt. Double extortion now appears in the overwhelming majority of attacks, and 77% of 2025 intrusions exfiltrated data before doing anything else. Backups can't un-leak what's already gone, and the breach-notification clock starts the moment data leaves. Data theft – not downtime – is the leverage.

Morphisec stops it in two layers, on one agent. Data Exfiltration Protection (DXP) is included and automatic. Data Exfiltration Control (DXC) is a paid add-on that adds policy-driven governance over the dual-use tools attackers and insiders use to move data out. Both are part of Impact Protection, powered by Automated Moving Target Defense (AMTD).

DXP – Included

Signatureless, prevention-first. Automatically blocks ransomware-driven data theft before it begins, across the top exfiltration and impact techniques. Powered by AMTD + AEM.

DXC – Add-On

Policy-driven governance over dual-use exfil tools. Monitor → Preventive, per-tool Allow/Block by process + destination, with its own console and activity views.

Key Capabilities



Top-10 Technique Coverage (DXP)

Addresses the top 10 MITRE ATT&CK exfiltration and impact techniques used in double- and triple-extortion ransomware – broader coverage than traditional tools.
Included



Signatureless AMTD Prevention (DXP)

No signatures, no behavioral analysis to tune. Neutralizes known and unknown exfiltration and impact tactics before they execute.
Included



Per-Tool Policy Enforcement (DXC)

Govern supported exfil tools individually: Monitor, Alert, or Terminate. Deterministic Allow/Block by process context + network destination.
Add-On



Activity View & Allow Rules (DXC)

See outbound transfers grouped by Tool → Root Domain; allow by domain + account + host with one-click baselining. 30-day retention.
Add-On



Critical, MITRE-Mapped Incidents (DXC)

Dedicated Exfiltration Violation incidents (Critical severity), mapped to MITRE T1567.002, T1537, T1020, with full audit log.
Add-On



Cross-Platform, One Agent (DXP + DXC)

Windows, Linux, and macOS – managed in the Morphisec Security Center (MSC3) alongside anti-ransomware. No second deployment.
Windows / Linux / macOS

Impact Across the Kill Chain

Double- and triple-extortion attacks chain encryption, recovery sabotage, and data theft. Morphisec's exfiltration and impact coverage spans the techniques that do the damage:

MITRE ATT&CK Technique	Seen In	Typical Loss
T1486 – Data Encrypted for Impact	97%	\$48.6M
T1490 – Inhibit System Recovery	88%	\$46.4M
T1489 – Service Stop (EDR/backup)	76%	\$46.3M
T1567 – Exfiltration Over Web Service	17%	\$3.9M
T1537 – Transfer Data to Cloud Account	9%	\$1.2M
T1020 – Automated Exfiltration	9%	\$1.1M
T1485 – Data Destruction (post-exfil)	6%	\$1.1M

Frequencies and typical losses per Morphisec analysis of common ransomware exfiltration and impact techniques. DXP addresses the top 10 such techniques; DXC adds policy-driven governance over the exfil tools attackers use to execute them.

Governed Exfil Tools (DXC)

Supported out of the box – AzCopy, WinSCP, rclone, FileZilla, PuTTY, PSCP, MegaSync, AWS CLI, Azure Storage Explorer, Cyberduck, and FreeFileSync. **Extensible** – additional tools are added through Morphisec Support.

The Morphisec Advantage

Business Benefit	Impact
Prevention-first, signatureless	DXP stops ransomware-driven theft before execution – no signatures, no detection delay.
Governance without a DLP project	DXC blocks dual-use tools by process + destination – zero content inspection, deterministic day one.
One agent, two layers	Both ride the Protector you already run – no second agent, no new console.
Tied to the ransomware kill chain	Closes the data-theft half of double extortion, upstream of encryption.
Audit-ready and defensible	Critical-severity, MITRE-mapped incidents for breach-notification defensibility.

Why Now

77% of ransomware intrusions stole data in 2025 (up from 57%)	87.6% of ransomware claims now use double extortion	72 min fastest-quartile time to first data exfiltration
---	---	---

Sources: Sophos State of Ransomware 2025; Travelers 2025; Unit 42 2026 Global IR Report.

 **MORPHISEC**

Stop data theft before it becomes a breach.

Two layers of exfiltration defense – DXP included, DXC for governance – on one agent.

[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.