



The Exfiltration Era

Why Data Theft – Not Encryption – Is the New Ransomware

How double extortion rewrote the ransomware playbook –
and how to close the data-theft gap on the endpoint.

Authored by Brad LaPorte,
Morphisec CMO and Gartner Veteran

Table of Contents

01 Executive Brief: Data Theft Is the New Extortion	3
02 The Double-Extortion Playbook – and Why Backups Don't Help	4
03 Anatomy of an Exfiltration Attack	5
04 Why EDR and DLP Miss Exfiltration	6
05 A Two-Layer Defense: Data Exfiltration Protection and Control	7
06 Inside DXC: Policy-Driven Exfiltration Governance	8
07 What Security Leaders Must Do Now	9
08 Conclusion: Stop the Theft, Not Just the Encryption	10

01 | Executive Brief: Data Theft Is the New Extortion

For a decade, ransomware meant one thing: encryption. Attackers locked your files and sold you the key. Defenders answered with backups and recovery, and the strategy mostly held. That era is over.

Modern ransomware leads with theft. Attackers exfiltrate sensitive data first, then threaten to leak or sell it – often before any encryption occurs, and sometimes instead of it. The numbers tell the story: 77% of ransomware intrusions stole data in 2025, up from 57% a year earlier; 87.6% of ransomware insurance claims now involve double extortion; and the fastest attackers move from initial break-in to first data exfiltration in as little as 72 minutes.

Backups restore what was encrypted. They cannot un-leak what was stolen – and the breach-notification clock starts the moment data leaves.

This is the exfiltration gap. The tools most enterprises rely on were built for the wrong problem: EDR watches for malware behavior and can't tell a legitimate file transfer from an attacker staging exfiltration; content-inspection DLP demands a months-long classification project and still misses the dual-use admin tools attackers prefer. Meanwhile, data theft, not downtime, has become the leverage.

This paper examines how double extortion rewrote the ransomware playbook, why detection and DLP fail to close the exfiltration gap, and how a two-layer, prevention-first model – Morphisec Data Exfiltration Protection (DXP) and Data Exfiltration Control (DXC) – stops data theft on the endpoint, on the agent you already run.

02 | The Double-Extortion Playbook – and Why Backups Don't Help

In the classic single-extortion model, the attacker's leverage was your inability to access your own data. Backups neutralized that leverage, so attackers adapted. Today's playbook inverts the sequence: steal first, encrypt second – or skip encryption entirely.

Why the theft comes first

Exfiltrated data is leverage that survives recovery. Even an organization with flawless, immutable backups still faces the threat of its customer records, financial data, source code, or trade secrets being published or sold. Regulators don't care that you restored operations – once data has left, notification obligations, contractual penalties, and reputational damage are already in motion.

Encryption is now optional

A growing share of attacks skip encryption altogether. Pure-exfiltration extortion is quieter, faster, and harder to detect than a noisy mass-encryption event – there is no ransom note on the screen, no flurry of file-rename activity, just data quietly leaving through tools that look legitimate. For many victims, the first sign is an extortion email.

What this means for defenders

- **Recovery is necessary but insufficient** – you must prevent the theft, not just survive the encryption.
- **The window is minutes, not days** – exfiltration can complete in well under two hours.
- **The leverage is the data itself** – so the control has to act on data leaving the endpoint.

03 | Anatomy of an Exfiltration Attack

Double- and triple-extortion attacks chain a predictable set of techniques. Morphisec analysis of common ransomware exfiltration and impact behaviors shows just how frequently – and how expensively – they appear.

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

The dual-use tool problem

Attackers rarely bring custom exfiltration malware. They use the same tools your administrators use – rclone, AzCopy, WinSCP, MegaSync, the AWS CLI – because those tools are trusted, fast, and unremarkable. Rclone alone appears in 57% of incidents. To EDR, an Rclone upload to a cloud bucket looks like routine IT work; the maliciousness lives in the context – which process, on which host, sending what, to where – not in any signature.

Attackers don't need new tools. They weaponize the trusted, dual-use utilities already on the endpoint – and that's exactly why detection misses them.

04 | Why EDR and DLP Miss Exfiltration

Two categories of tooling are supposed to cover this risk. Both have structural blind spots.

EDR: built to recognize malware, not transfers

Endpoint detection and response watches for malicious behavior and known-bad patterns.

But a dual-use transfer tool moving data to a cloud destination isn't malware – it's an administrator's everyday workflow, until it isn't. EDR has no per-tool policy, no notion of an approved versus unapproved destination, and it acts after suspicious behavior is recognized – often after the data is already gone.

DLP: a classification project that misses the tools

Content-inspection DLP tries to identify sensitive data as it moves, which means standing up thousands of classifiers and tuning them for months – and still wrestling with privacy constraints and encrypted streams. Worse, DLP is oriented around content and channels, not the dual-use admin tools attackers actually use, so it frequently either misses exfiltration or over-blocks legitimate work, generating noise that teams learn to ignore.

Capability	Traditional DLP	Endpoint-Native Exfiltration Control
Decision basis	Content classification	Process context + network destination
Time to value	Months of tuning, 1000s 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 already deployed
Privacy exposure	Inspects content	Zero content inspection

05 | A Two-Layer Defense: Data Exfiltration Protection and Control

Closing the exfiltration gap means acting where the data leaves – the endpoint – and doing it deterministically, before the transfer completes. Morphisec delivers this in two complementary layers, both part of Impact Protection and both running on the Protector you already deploy.

Layer 1 – Data Exfiltration Protection (DXP), included

DXP is the included, automatic safeguard. Signatureless and powered by Automated Moving Target Defense (AMTD), it blocks ransomware-driven data theft before it begins, across the top exfiltration and impact techniques used in double and triple extortion. There are no signatures to update and no behavioral models to tune – it simply prevents. DXP is the baseline every Anti-Ransomware customer already has.

Layer 2 – Data Exfiltration Control (DXC), the paid add-on

DXC is the next tier up: policy-driven, enterprise-grade governance over the dual-use tools used to move data out. Where DXP stops ransomware-driven theft automatically, DXC gives security teams visibility and deterministic control – per tool, by destination – over the gray area of legitimate-looking transfers. It is the difference between an automatic safeguard and a managed control plane for outbound data movement.

Capability	Traditional DLP	Endpoint-Native Exfiltration Control
Scope	Ransomware-driven data theft	Outbound transfers by supported exfil tools
Control model	Automatic, always-on safeguard	Policy-driven, per-tool enforcement
Visibility	Built-in prevention	Activity view (Tool → Root Domain), 30-day retention
Allow rules	–	By domain + account + host, one-click baselining
Modes	Always-on prevention	Monitor → Preventive
Incidents	Within anti-ransomware	Dedicated Exfiltration Violations (Critical, MITRE-mapped)

06 | Inside DXC: Policy-Driven Exfiltration Governance

DXC governs each supported exfiltration tool through two phases, with deterministic decisions and no content inspection.

What makes AIUC different

- **Monitor Mode (default)** – Silently observes outbound transfers with no disruption, so teams can baseline normal activity before enforcing anything.
- **Preventive Mode (admin-activated)** – Enforces on any traffic outside the allowed rules. Every decision is Allow or Block, derived from process context plus network destination (root domain).
- **Per-tool enforcement** – Each tool is set independently: No Enforcement / Monitor, Alert (incident only), or Terminate (kill the process).
- **Deterministic allow rules** – Allow by domain + account + host (All Hosts, Protector Groups, or Specific Hosts), with one-click “Add to Policy” baselining from the Activity view.
- **Audit-ready incidents** – Exfiltration Violation incidents carry Critical severity, are classified Data Exfiltration, and map to MITRE ATT&CK T1567.002, T1537, and T1020, with a full audit log.

Supported tools and platforms

Out of the box, DXC governs AzCopy, WinSCP, rclone, FileZilla, PuTTY, PSCP, MegaSync, AWS CLI, Azure Storage Explorer, Cyberduck, and FreeFileSync – and is extensible through Morphisec Support. Coverage spans Windows (full Monitor + Preventive enforcement), Linux (socket and egress-layer enforcement with full-domain matching, IPv6, and fragmented-packet handling), and macOS (exfiltration awareness with cryptographic process verification) – all managed in the Morphisec Security Center alongside anti-ransomware.

DXC blocks the tools used for double-extortion theft by what they are and where they're sending – deterministically, on the agent you already run.

07 | What Security Leaders Must Do Now

The shift from encryption to theft demands a shift in controls – from recovery-after-impact to prevention-at-egress. A practical agenda:

An exfiltration-defense checklist

- ✓ **Assume theft-first** – treat data exfiltration, not just encryption, as the primary ransomware outcome to prevent.
- ✓ **Get visibility into outbound tools** – inventory which exfil and transfer tools run across your fleet, and where they send.
- ✓ **Govern the dual-use tools** – enforce per-tool policy by process and destination – start in Monitor, then Prevent.
- ✓ **Don't wait on a DLP project** – deterministic, content-free control delivers value on day one.
- ✓ **Make it defensible** – capture Critical, MITRE-mapped evidence for breach-notification and audit.

Crucially, enable rather than obstruct. Because every tool begins in Monitor Mode and legitimate workflows can be allow-listed in one click, security teams can govern exfiltration without blocking the administrators and engineers who depend on these same tools every day.

08 | Conclusion: Stop the Theft, Not Just the Encryption

Ransomware's center of gravity has moved. The damage that defines a modern breach happens before encryption – when data leaves the endpoint through trusted, dual-use tools, in minutes, invisible to EDR and unaddressed by DLP. Backups, however good, cannot close that gap.

Morphisec closes it in two layers, on one agent: Data Exfiltration Protection stops ransomware-driven theft automatically, and Data Exfiltration Control governs the dual-use tools deterministically – by process and destination, with zero content inspection. Together they shut down the data-theft half of double extortion, upstream of encryption, on the Protector you already run.

When the theft is the threat, prevention at the point of egress is the only strategy that scales.

77%

of ransomware intrusions stole data in 2025

87.6%

of ransomware claims now use double extortion

72min

fastest-quartile time to first exfiltration

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

Further reading from Morphisec

- Ransomware Without Encryption: Why Pure Exfiltration Attacks Are Surging – and Why They're So Hard to Catch
- Ransomware Evolution and Data Exfiltration: A Deep Dive for Cybersecurity Analysts
- Gone in an Hour: Why Law Firms Can't Afford to Ignore Data Exfiltration Risks
- Why Hedge Funds Need to Take Data Exfiltration as Seriously as Ransomware



MORPHISEC

Close the other half of ransomware.

See Data Exfiltration Protection and Control in action today.

Get a demo

About Morphisec

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. Founded in 2014 and headquartered in New York, and powered by Automated Moving Target Defense (AMTD), Morphisec stops attacks before execution. At Morphisec, we don't just respond – we prevent.



MORPHISEC