GuardWare
#1 in Data Security

guardware.com

The 2026 Data Control Crisis

Visibility is no longer enough. Your data needs to protect itself.

DSPM + Persistent Encryption

STEP 1

FIND AND CLASSIFY

Know exactly where your sensitive data lives across every repository, including M365. The foundation of resilience is not a dashboard. It is evidence. You cannot defend what you have not found.

STEP 2

MONITOR AND CONTROL ACROSS EVERY CHANNEL

Continuous visibility across endpoints, cloud platforms, M365, AI tools, USB activity, web traffic, and home environments. Risky behaviour is detected and acted on in real time, so threats are addressed before they become incidents.

STEP 3

ENCRYPT, REVOKE, AND STAY RESILIENT

Persistent file encryption means that even if data is breached, stolen, or exfiltrated, it cannot be read, ransomed, or published. Keys are yours. Access is revocable for any file at any time. A breach stops being a crisis and becomes a non-event.

Persistent encryption that protects even when breached.

What's changed in 2026.

Two structural shifts are making data exposure harder to ignore.

1. The Modern Way of Working Moves Data Continuously.

Organisations now operate across distributed collaboration environments, including:

- M365 (SharePoint, Teams, OneDrive, email)
- File shares and legacy archives
- Cloud repositories and SaaS platforms
- Contractors, suppliers, and partner ecosystems

Sensitive data no longer sits in a single location. It moves constantly across systems, teams, and organisational boundaries.

Traditional perimeter-based controls were not designed for this level of fluid data movement.

2. AI Accelerates Exposure — Including Shadow AI.

AI tools do not create sensitive data risk; they operate within existing permissions. If data is over-permissioned, poorly classified, or widely distributed, AI makes it easier to locate, summarise, and redistribute, at machine speed.

At the same time, Shadow AI usage is expanding exposure. Employees increasingly paste content into external AI tools outside formal governance frameworks. This behaviour is rarely malicious, but sensitive information can leave managed environments without visibility, auditability, or clear retention controls.

The risk is not AI itself, it is the absence of enforceable control over how data is accessed and shared.

Why Security Teams Lose Line of Sight.

This isn't about competence. It's about volume and sprawl.

- Unstructured data is the bulk of the risk (documents, designs, spreadsheets, email attachments).
- Ownership is unclear (projects finish, teams move on, access remains).
- Permissions drift (inheritance, nested groups, "everyone" access, exceptions).
- Classification is inconsistent (some labels, some policy, a lot of judgement).
- AI tools create data flows beyond traditional monitoring
- Evidence is hard to produce quickly (especially under pressure).

The result is exposure that expands gradually and goes unnoticed — until an event forces the question no one can answer cleanly. Security leaders end up working from assumptions. And assumptions are where incidents begin.

What "Control" Looks Like Now.

In 2026, control means being able to produce a defensible view of:

- Where sensitive data resides, across the repositories that matter most
- What it contains, PII, contracts, pricing, IP, customer records
- Who has effective access, not just what policy states
- How it is being accessed, moved, or shared
- What should be remediated first, prioritised by risk and effort

The Real Challenge in 2026.

Most organisations do not have a tooling problem. They have a control problem.

Sensitive data spreads across M365, file shares, endpoints, and supplier ecosystems. Monitoring alone does not enforce protection.

True control means:

- Knowing where sensitive data lives
- Understanding exposure
- Monitoring how it moves
- Retaining the ability to protect it, even if it leaves your environment

AI Has Exposed the Control Gap.

AI does not create new weaknesses.
It reveals the ones that were already there.

Over-permissioned repositories, inherited access, forgotten file shares, and sensitive information stored in the wrong location can now be located and synthesised rapidly.

This makes visibility gaps more consequential than ever.

**"AI doesn't create exposure.
It reveals what you never truly controlled.
In 2026, control must be enforceable, not assumed."**

Rizwan Mahmood, Co-Founder & CEO

When the Breach Hits, Can You Answer the Four Questions That Matter?

Security teams can see alerts, dashboards, and logs. But when something goes wrong, most still cannot answer the only questions that matter: which files were taken, where they were stored, who had access to them, and whether they left the environment.

That is the difference between visibility and control. Visibility tells you something happened. Control tells you exactly what was involved and gives you the evidence to prove it, to your board, your regulator, and your insurer.

Without that, incident response becomes a forensic reconstruction exercise. You are piecing together access logs weeks after the event, trying to work out what was in a SharePoint folder that no longer exists, or explaining to the Privacy Commissioner why you cannot confirm the scope of a breach within the required timeframe.

That uncertainty is where the real cost sits. Not the intrusion. The weeks of not knowing.

The Security Sequence That Will Close the Gap.

GuardWare's suite follows a deliberate sequence because that is how data risk actually works. You cannot monitor what you have not found. You cannot protect what you have not classified.

Discover your sensitive data and classify it. Monitor its movement and who touches it. Encrypt it so it stays protected, even beyond your environment. Revoke access the moment you need to.

Each step makes the next one possible. That is the difference between a collection of security products and an enforceable control model.

- Control that does not depend on the perimeter holding
- Control that does not collapse when data moves
- Control that holds even when AI accelerates the threat

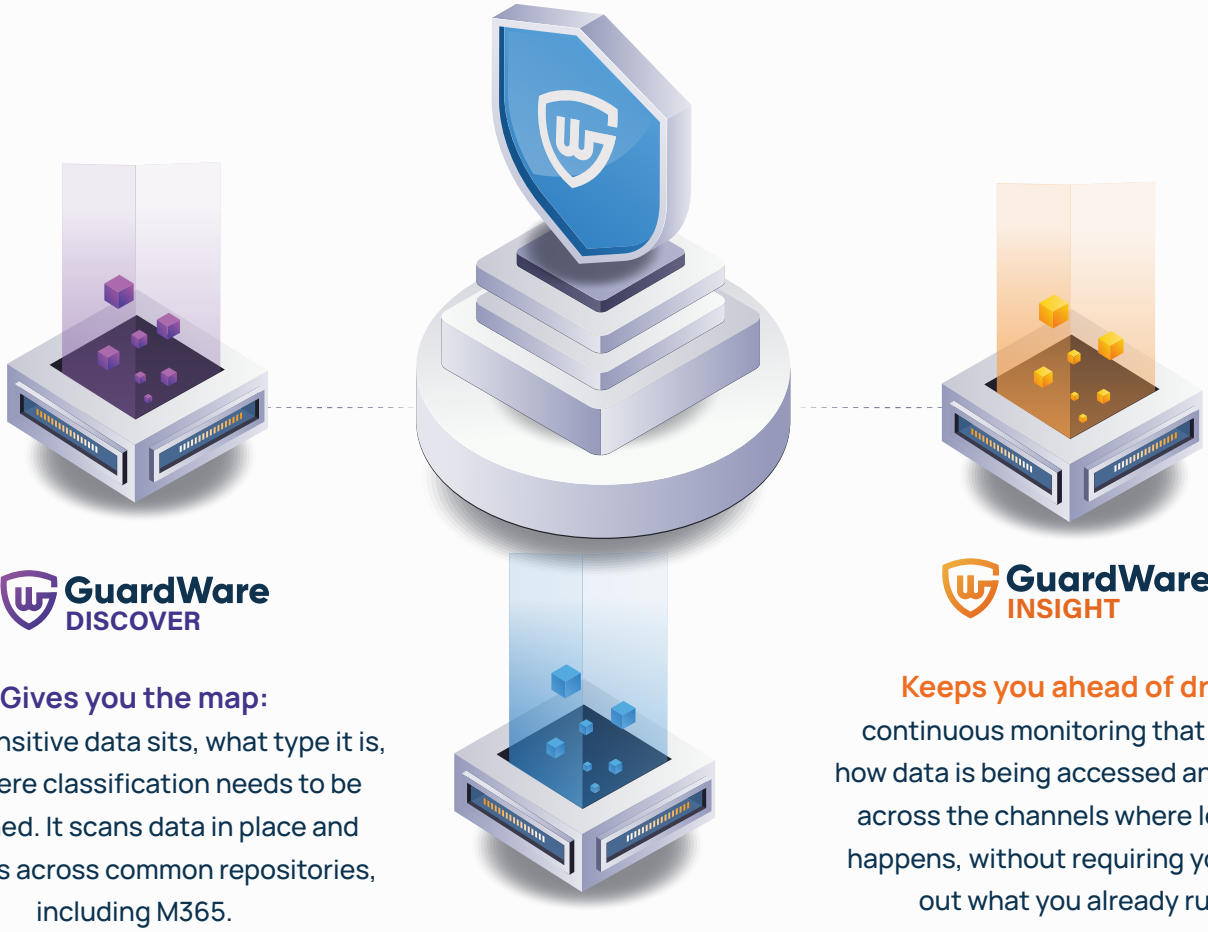
Data-Centric Security.

Built for the reality you manage.

Most organisations don't need another dashboard.

You need certainty, fast. Where does sensitive data live? Who can access it, and what changes day to day that quietly expand exposure.

GuardWare's Data-Centric Security suite is designed for this reality as an operational control model, not a standalone toolset.
It connects visibility, monitoring, and protection into a single, enforceable sequence.



GuardWare DISCOVER

Gives you the map:
where sensitive data sits, what type it is, and where classification needs to be tightened. It scans data in place and connects across common repositories, including M365.

GuardWare INSIGHT

Keeps you ahead of drift:
continuous monitoring that shows how data is being accessed and moved across the channels where leakage happens, without requiring you to rip out what you already run.

GuardWare PROTECT

"Even if it's stolen" control:
persistent file encryption designed so sensitive files remain protected when they leave your environment, with the ability to revoke access if needed.

GuardWare DISCOVER

Where does our sensitive data actually live?

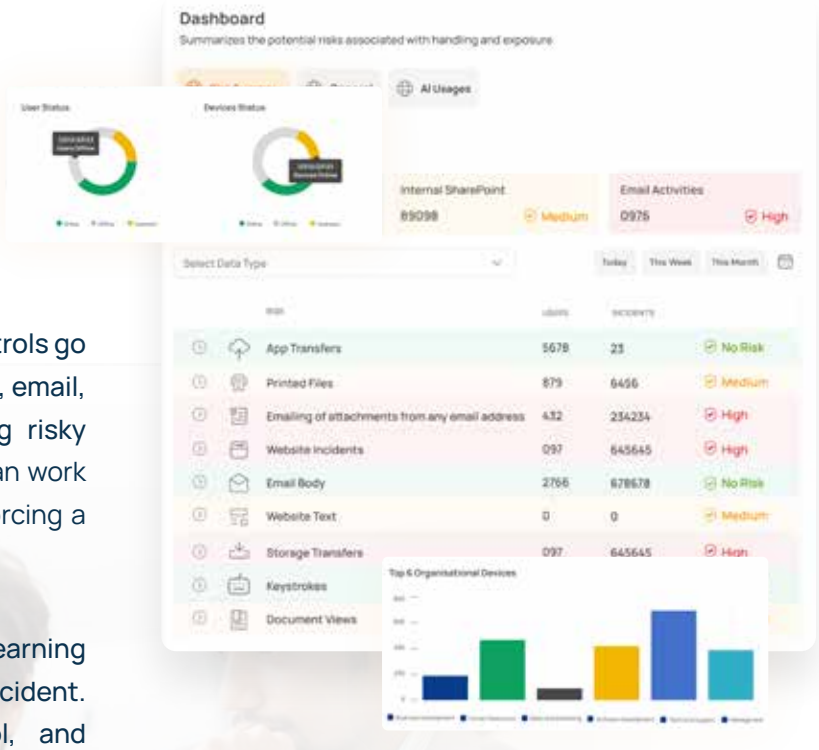
Most organisations can't answer one basic question with confidence.

DISCOVER is built to close that gap fast. It scans files in place and connects across core repositories, including remote scanning of M365 email and SharePoint, so you can locate and classify sensitive information without relying on guesswork or manual sampling.

The output is a practical view of your highest-risk repositories: what's sensitive, where it's concentrated, and where ownership and permissions need attention first. This is the step that makes AI rollouts, audit responses, and incident triage more controlled, because you're working from evidence, not assumptions.

GuardWare INSIGHT

Keeps a 24-Hour eye on your data.



INSIGHT is continuous visibility where most controls go blind: endpoints, file shares, cloud drives, M365, email, and web activity, with a focus on identifying risky behaviour in real time. It's next-gen DLP that can work alongside what you already have, rather than forcing a clean-slate replacement.

This is the layer that helps security teams stop learning about data movement after it becomes an incident. Instead, you get ongoing visibility, control, and monitoring, with alerts that align to how work actually happens including the messy reality of sharing, copying, and "temporary" exceptions.

GuardWare PROTECT

GuardWare PROTECT Design

Persistent Encryption Control That Survives a Breach.

PROTECT is for the scenario every CISO plans for but can't fully prevent: data leaves the building, through a breach, an insider, a supplier, or normal delivery. Protect applies persistent file encryption at Rest, in Transit and In USE so the file stays protected even when it's copied or exfiltrated, with controls designed to keep unauthorised parties locked out. It also supports a "remote kill" approach, destroying access by destroying keys, and provides a record of file access and usage that supports investigation and accountability.

PROTECT Design extends persistent file encryption to high-value engineering and intellectual property workflows. CAD files, technical drawings, and design assets remain encrypted, even while in use, ensuring control across project teams, contractors, and global supply chains. Access can be revoked at any time, providing enforceable protection for sensitive IP beyond the corporate perimeter.

From Design to Delivery

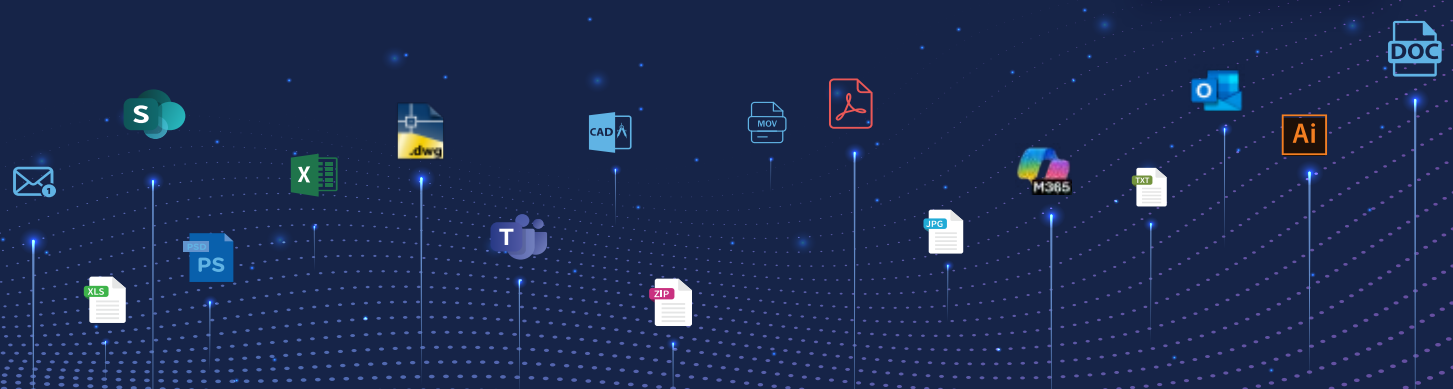
CAD Files Secured at Every Step

Now you can encrypt individual drawings – while in use

Start with a scoped sensitive data snapshot.

It only takes 2 hours to set up and produces a ranked exposure report and remediation plan that you can act on.

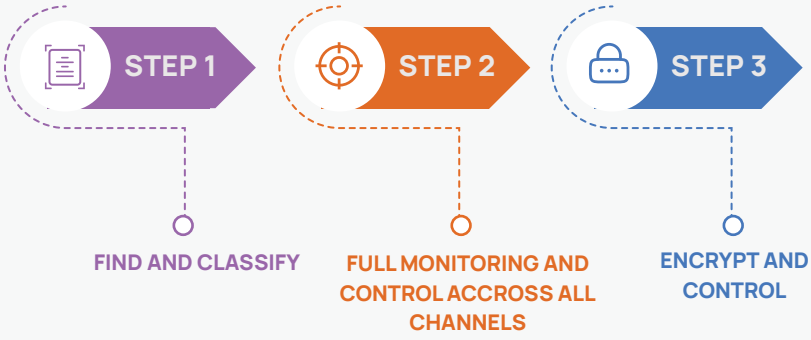
GuardWare Proof of Value, that is scoped to fit your data visibility challenge. We will scan the data repositories that hold your sensitive data to uncover PII, PCI, highlight risky handling of data and so much more.



GuardWare
#1 in Data Security

The GuardWare Suite

Allowing your data to protect itself



BOOK A DEMO

guardware.com
+61-2 8551 8500
sales@guardware.com.au