GuardWare PROTECT

guardware.com

Persistent encryption doesn't just protect your data. It removes the limits on how you use it.

Most organisations treat encryption as a last resort, something applied to the most sensitive files, in the most controlled environments, after every other control has been considered.

GuardWare PROTECT inverts that logic. When every sensitive file is persistently encrypted by default, across every repository, every device, every supply chain handoff, the question stops being "what happens if it's stolen?"

"Most encryption tech are limited to data at rest or when transferred but fail when it is accessed. With PROTECT you can now control data even accessed. Whereever it goes, what ever happens to it, whoever ends up holding the file, you are always in control."

Rizwan Mahmood,
Co-Founder & CEO, GuardWare

The Last Line of Defence.

A data-first security strategy accepts a difficult truth: perimeters fail. Controls are bypassed. People make mistakes. The question is not whether sensitive data will leave your environment, it's whether it matters when it does.

Organisations may have strong visibility and monitoring within their own systems, but they struggle to control and secure data once it leaves their environment. As data moves to external platforms like cloud services or third parties, traditional security measures become less effective, increasing the risk of unauthorised access and data breaches. This highlights the need for more flexible, data-focused security approaches.

The question most security strategies fail to answer is this: once the file is gone, what then?

Traditional encryption secures data at rest and in transit. Once the file is opened by an authorised user and passed along, forwarded, copied, exported, the encryption is gone too. The file is now unprotected, sitting wherever it landed, accessible to whoever can reach it.

PROTECT applies a different principle entirely. The encryption is not a gate the file passes through. It is a property the file carries permanently, so that control stays with you, not with whoever ends up holding it.

The four scenarios every CISO, CIO, and CSO plans for but cannot fully prevent:

The breach that gets through.
Even organisations with mature security postures experience breaches. Phishing succeeds, credentials are compromised, a zero-day is exploited. When that happens, the difference between a catastrophic event and a manageable one is whether the data that was taken can actually be read. With PROTECT, it cannot.

The ransomware demand that has no leverage.
Ransomware works because the attacker holds something you need. Encrypted data changes that equation entirely. If every sensitive file in your environment is persistently encrypted with keys only you control, exfiltrated data cannot be read, cannot be published meaningfully, and cannot be used as leverage. The ransomware business model depends on your data having value to someone else. PROTECT removes that value.

The insider who decides to leave.
Malicious insider breaches are the costliest data breach type for Australian organisations, averaging AUD $4.91 million per incident according to IBM's 2024 Cost of a Data Breach Report. A departing employee who copies sensitive files to a personal drive, a disgruntled contractor who exports a client database, these are not theoretical scenarios. They are regular occurrences that standard DLP tools detect after the fact, if at all. PROTECT means you can revoke access to every file they took, immediately, remotely, with no physical interaction with the device.

The supplier with good intentions and poor controls.
Modern project delivery requires sharing sensitive documents with third parties, contractors, partners, legal firms, design consultancies. You cannot control their security posture. You can control whether the files you send them remain under your authority, regardless of where they **end up. And you can revoke that access the moment the engagement ends.**

"The part that makes breaches expensive isn't the intrusion. It's the uncertainty afterwards, what data was taken, who has it now, and whether it can still be read. PROTECT removes the uncertainty. Even if it's stolen it's useless".

Rizwan Mahmood,
Co-Founder & CEO, GuardWare

What's changed in 2026.

The perimeter dissolved. Your data didn't stop moving.

The principle behind most data security investment is containment, keep sensitive data inside the boundary, and it stays safe. In 2026, that boundary is a fiction. Data moves across supplier ecosystems, cloud platforms, personal devices, and partner networks as a matter of routine. Containment, as a primary strategy, has run its course.

The supply chain is now the attack surface. Modern organisations don't operate in isolation. They operate through networks of contractors, technology partners, legal advisors, design firms, and subcontractors, each of whom handles sensitive data and each of whom has their own, often uncontrolled, security posture. A breach at a third party is a breach of your data, regardless of where it physically occurred or who was technically at fault.

Project delivery demands document flow. Tenders require IP disclosure. Contracts require financial data. Design projects require CAD files and engineering specifications. Healthcare engagements require patient records. In every sector, sensitive data must leave the organisation to enable work to get done. The choice is not whether to share, it's whether what you share can be revoked, tracked, and controlled after the fact.

Stolen data is only valuable if it can be read. The entire premise of a ransomware attack, a data exfiltration event, or an insider theft is that the data taken has value to someone.

Persistent encryption removes that value entirely, and does so permanently, not conditionally. A file protected by PROTECT is not a liability waiting to become a breach notification. It is a non-event, regardless of who takes it, where it goes, or how long they hold it.

100%

of protected files remain encrypted when stored anywhere, transferred by any method, and when in active use by a user or application.

AES 256 & RSA 2048

the hybrid encryption combination at the core of PROTECT. Military-grade. Applied at the file level. Persistent across the entire file lifecycle.

Remote kill

you can now control your data remotely when in possession of 3rd party suppliers. Destroy any time once the job is done.

Your data, under your control - wherever it goes.

PROTECT applies persistent file encryption so that sensitive files remain protected after they leave your environment. Not just during transit. Not just at rest. Persistently, when stored anywhere, transferred by any method, and in active use by a user or application. The encryption travels with the file. The control stays with you.

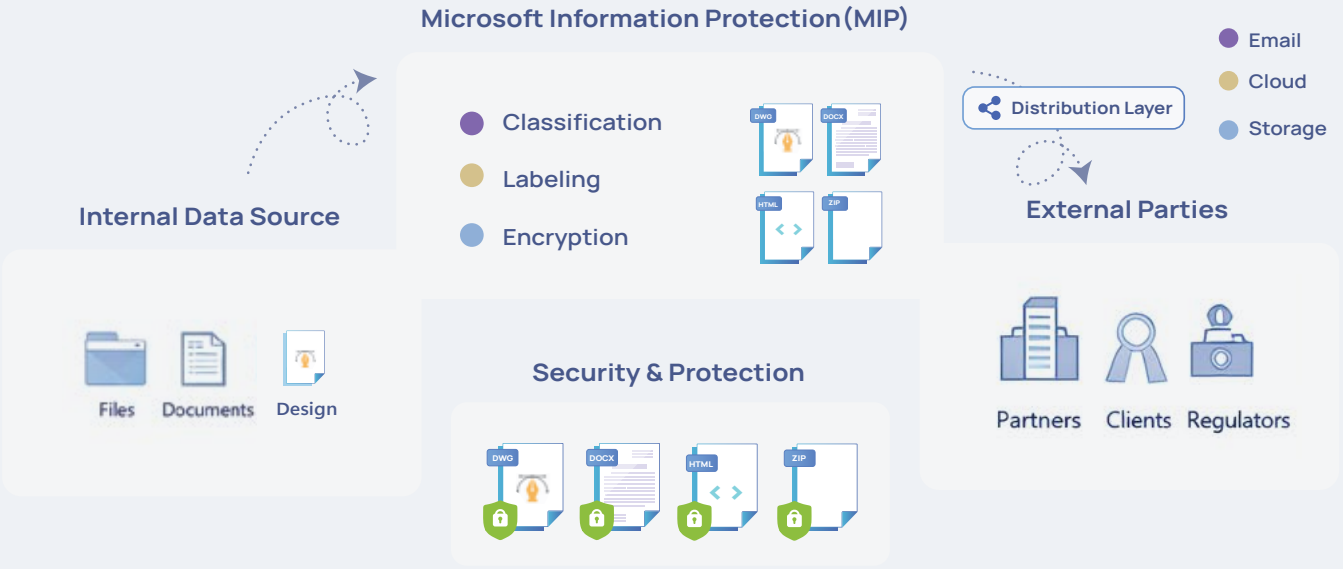
When a protected file is accessed by an unauthorised party, through a breach, through exfiltration, through a compromised supply chain, they cannot read it. **It cannot be weaponised in a ransomware demand. It cannot be published to cause reputational damage. It is, in every meaningful sense, worthless to them.** The keys that unlock it are yours. And when you need to revoke access, you can do so remotely, immediately, without any physical interaction with the file or the device that holds it.

Persistent encryption across the file lifecycle.
Protected files remain encrypted when stored anywhere, transferred by any method, and when in use by an authorised user or application. The moment a file reaches an unauthorised party, it becomes unreadable, permanently.

Remote kill.
Destroy access by destroying keys. If a file is exfiltrated, a device is lost, or a supplier relationship ends, access can be revoked instantly. No physical access required. No recovery operation needed. Every file you have ever shared externally remains under your authority until you decide otherwise.

Secure Collaboration

Organization can securely collaborate with external partners using Microsoft Information Protection (MIP), encrypted ZIP files, and secure HTML formats to protect sensitive data through encryption and access controls. It can extend this protection to suppliers via PROTECT, ensuring security beyond organizational boundaries and reducing data leakage risks. Key use cases include working with suppliers, collaborating with partners, and securely managing sensitive projects or confidential information with external stakeholders.



What PROTECT Does.

Encryption that stays on the file. Control that stays with you

Persistent File Encryption.
AES 256 and RSA 2048 hybrid encryption applied at the file level , not the folder, not the drive, not the platform. The file itself is protected, regardless of where it goes or how it gets there. When the file moves, the encryption moves with it. When an authorised user opens it, it works normally. When anyone else tries, it doesn't.

Unique Key Per File.
Each protected file receives its own unique encryption key. This architectural decision isolates risk, a compromised key affects only one file, not the entire protected data estate.

Offline, Online, and Hybrid Operations.
PROTECT is designed for the reality of how organisations operate, including scenarios where files are accessed offline, in air-gapped environments, or across hybrid infrastructure. Protection does not depend on network

Location based Monitoring.
A complete record of file access and usage, who opened a protected file, when, from where, and on which device. Supports investigation, accountability, and regulatory compliance.

Works with any DMS, cloud application, or ERP out of the box.
Compatible with the systems your organisation already uses, no rip-and-replace, no integration project.

Transparent to the authorised user.
Format-preserving encryption means authorised users work with files exactly as they always have. No workflow disruption, no productivity overhead.

Remote Key Destruction.
Revoke access to any file, at any time, from anywhere, by destroying the associated encryption key. Immediate effect. No physical access to the file or device required. **The ability to reach back into any environment, internal or external and remove access to a file your organisation created is a capability that no other**

Centralised Key Management.
All keys managed centrally by your security team. Full oversight of who has access to what, with the ability to grant, restrict, and revoke access as organisational needs change. **Every file you have ever shared, internally or externally, is visible, controllable, and revocable from a single point of authority.**

Unique Wrapper Technology.
Custom wrapper technology enables metadata definition for non-standard file types, extending persistent encryption to file formats that most protection tools cannot handle.

Classification and Labelling.
Ability to classify and label non-standard files, connecting PROTECT's encryption capability to the classification framework established by GuardWare DISCOVER.

Data Retention Management
Ensures that information is securely managed throughout its lifecycle by assigning defined expiry dates. Once the retention period has elapsed, files associated with a specific project or group become automatically inaccessible, supporting compliance, reducing data risk, and maintaining organizational efficiency.

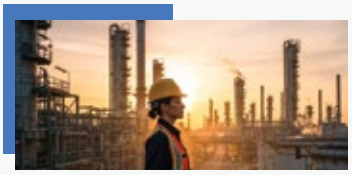
GuardWare
PROTECT Design

For the organisations where IP is the asset.

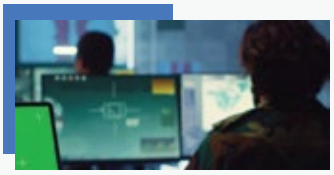
PROTECT Design extends persistent encryption to high-value design workflows, specifically the CAD files, engineering specifications, and intellectual property that move across project teams, subcontractors, and supply chains in defence, manufacturing, infrastructure, and professional services.

In industries where a single set of design files represents years of investment and competitive advantage, the risk of IP exfiltration during bids, tenders, or project delivery is existential. PROTECT Design closes that gap, applying the same persistent encryption and remote revocation capability to proprietary file formats that standard protection tools cannot reach.

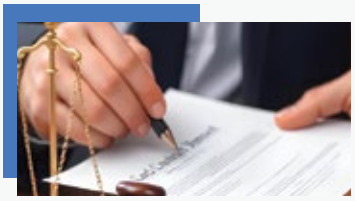
Built for: Defence supply chains



Manufacturing Engineering and infrastructure



Defence and Defence Supply Chain



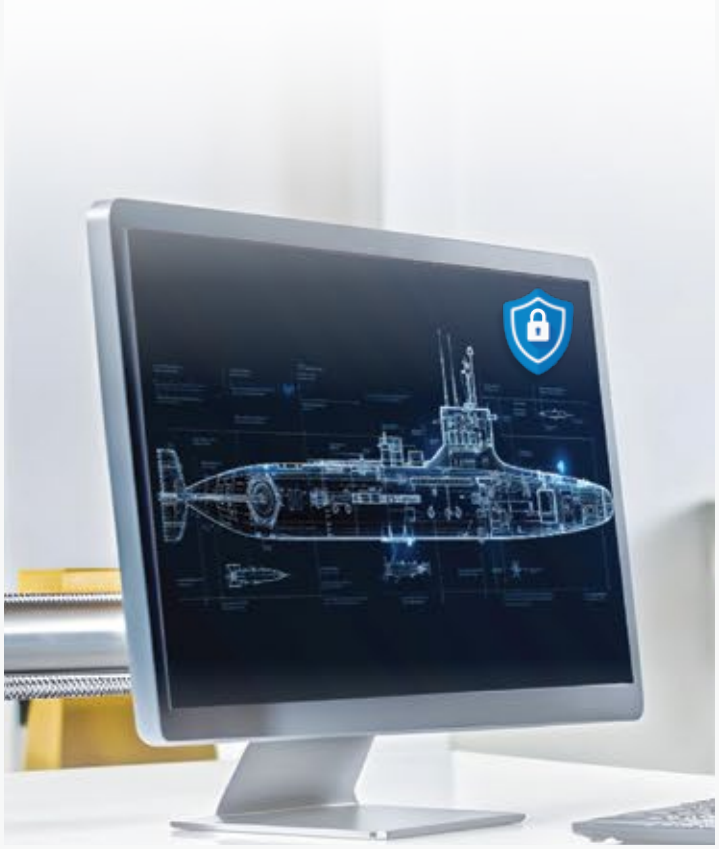
Professional services and legal

Medical and pharmaceutical research

From Design to Delivery

CAD Files Secured at Every Step

Now you can share CAD files freely. They remain protected - even if stolen.



Visit Us

- Simple to deploy
- Transparent to users

Real-World Scenarios.

The situations PROTECT was built for.

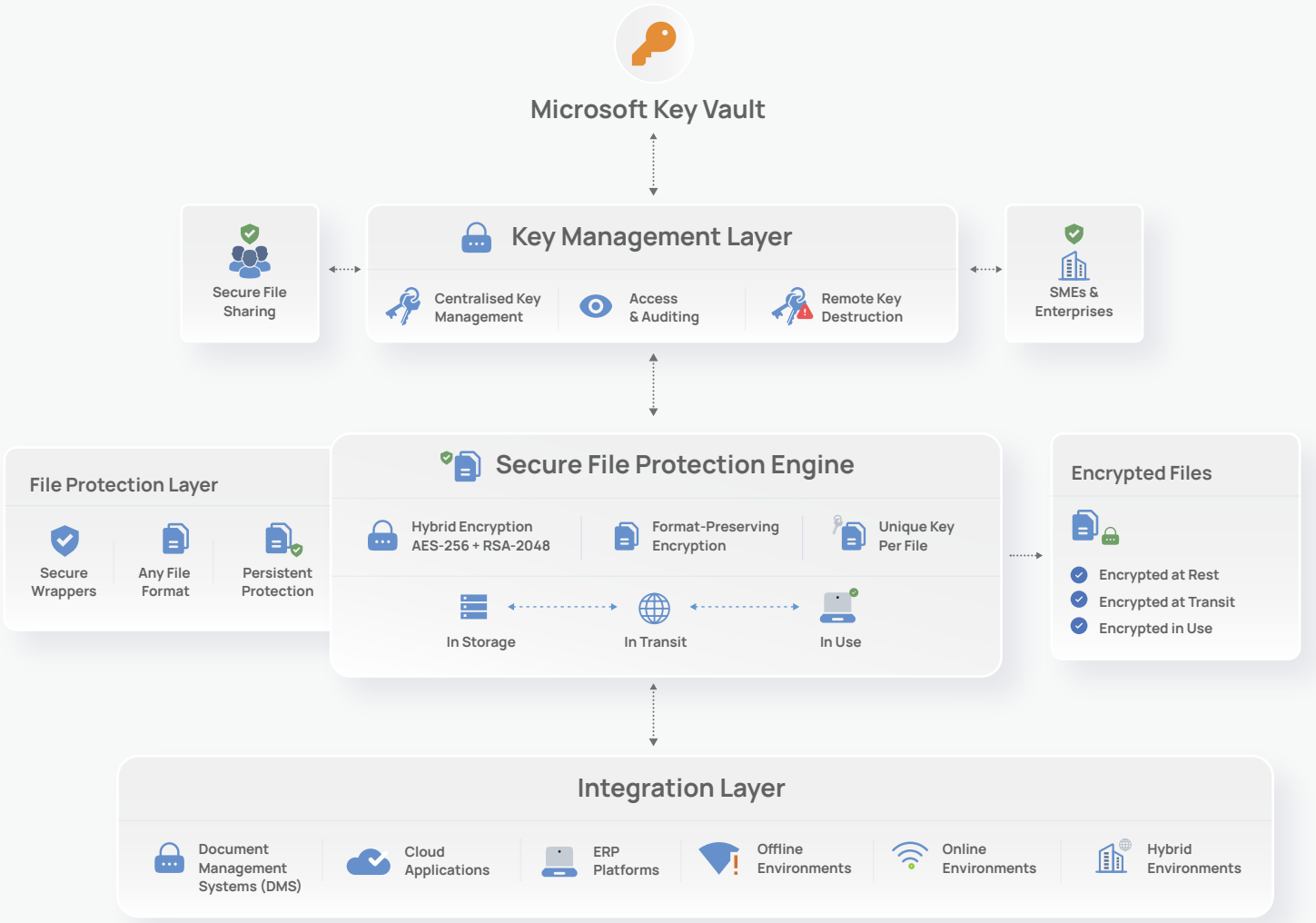
Exported data from business applications.
Reports, exports, and extracts from ERP, CRM, and financial systems routinely contain sensitive customer, pricing, or operational data. PROTECT applies encryption, so the file is protected from the moment it is created, regardless of where it ends up. The file cannot be read by anyone you have not explicitly authorised, and access can be revoked immediately upon departure.

Sharing IP during bids and tenders.
Responding to a government or enterprise tender requires disclosing your most valuable IP to an evaluation panel that includes, in some cases, your competitors. PROTECT ensures that the documents you submit remain under your control, accessible to legitimate evaluators, inaccessible to everyone else, and revocable the moment the process ends.

Insider Threat.
A departing employee who copies client data, a contractor who exports project files before their engagement ends, a disgruntled team member who decides to share proprietary information with a competitor. PROTECT ensures that even if the files leave with them, they cannot be read by anyone you have not explicitly authorised and access can be revoked immediately upon departure.

Double extortion ransomware has become the dominant attack model. Attackers encrypt your systems, then threaten to publish the data they took unless you pay. The second threat is often the more damaging one. Operational disruption can be recovered from. A public dump of customer records, financial data, or commercially sensitive IP is harder to walk back. PROTECT removes that second lever entirely. If the data that was exfiltrated is persistently encrypted, it has no publication value. There is nothing to threaten you with. The extortion model collapses, not because the attacker failed to get the files, but because the files are worthless to them without keys they will never have.

Secure by design. Compatible by default.



Built for all sectors.

- Finance and BFSI
- Government
- Defence and supply chains
- Manufacturing
- Software development and DevOps
- PLC and SCADA environments
- Medical and pharmaceutical research
- Legal

The GuardWare Suite.

GuardWare
#1 in Data Security

PROTECT is the final layer. Together, the suite makes data genuinely self-defending.

STEP 1

GuardWare DISCOVER

FIND AND CLASSIFY

Map sensitive data across all repositories, including M365. Know what you have, where it lives, and what needs to be tightened first.

STEP 2

GuardWare INSIGHT

FULL MONITORING AND CONTROL ACROSS ALL CHANNELS

Extends visibility beyond M365 to endpoints, cloud platforms, AI tools, USB activity, web traffic, and home environments. The complete picture, across every channel where data moves.

STEP 3

GuardWare PROTECT

ENCRYPT AND CONTROL

Persistent file encryption so sensitive files remain protected even when they leave your environment, with remote key revocation for every file, including files already shared externally.

GuardWare
PROTECT

If it's stolen, it should be useless. That's what PROTECT delivers.

Persistent encryption. Remote revocation. Complete audit trail. Data that cannot be read, cannot be ransomed, and cannot be published. PROTECT gives your organisation the one capability that no breach, no insider, and no supply chain compromise can defeat, data that protects itself.

BOOK A DEMO

guardware.com

+61-2 8551 8500

sales@guardware.com.au