HaloSHARE

How AECO can protect IP in 2026 without encryption

In this guide, you will learn:

- Why AECO IP is under threat in 2026
- Where your IP is most vulnerable in 2026
- How to close these IP security gaps without encryption
- How Secude's solutions work in practice with Autodesk Construction Cloud

Secude

www.secude.com

AECO companies that only rely on data loss prevention tools (DLP) to protect their IP are walking a dangerous tightrope.

Last year, digital transformation, AI adoption and cloud-based collaboration brought widespread productivity and efficiency gains to Architecture, Engineering, Construction and Operations (AECO) workflows. But they also opened the door for more sophisticated and damaging cyber threats, such as AI-powered digital supply chain attacks.

$4.4M

2025 cost of average AECO data breach (but IP data leakage costs ways more)

When the offense changes, so must the defense — especially when it comes to protecting your 'crown jewels'.

According to IBM, the average cost of a data breach in 2025 was $4.4M. But IP data leakage is way more costly for AECO companies than hard figures. Losing your IP disrupts your projects, damages your reputation, exposes your trade secrets, and potentially erases your competitive advantage forever.

Much of AECO's IP is contained in CAD files, such as 3D models, infrastructure designs and engineering blueprints. But completely locking down these files - as well as other sensitive PDFs and MS Office files that contain your IP - is not suitable for the collaborative nature of AECO workflows. So what should you do?

Losing your IP disrupts your projects, damages your reputation and exposes your trade secrets.

In this guide, you will learn:

- Why AECO IP is under threat in 2026
- Where your IP is most vulnerable in 2026
- How to close these IP security gaps without encryption
- How Secude's solutions work in practice with Autodesk Construction Cloud

From file-level CAD security to non-encrypted digital watermarking software, AECO has the tools to secure its IP without adversely impacting digital workflows. It's time to use them.

Why AECO IP is under threat in 2026

Digital transformation not matched by cybersecurity resilience

Digital transformation is a double-edged sword for AECO. While the growing reliance on AI tools, CAD files, digital twins and Building Information Modeling (BIM) has delivered noticeable productivity gains for AECO projects, the embrace of digital workflows has also increased the cybersecurity risks. In the last few years, 59% of AECO firms have suffered a cybersecurity incident.

> **Digital workflows are the lifeblood of modern AECO operations, but if they get infected, they can very quickly poison an entire AECO supply chain. What AECO needs is a way to secure these workflows and protect its most valuable IP without disrupting the flow of information.**
>
> Blake Wood, VP Global Alliances, Secude

To make matters worse, AECO already lags behind more cyber-resilient sectors, such as Defense, Financial Services and Healthcare. With AECO's multi-partner supply chain networks, fragmented data practices, widespread use of IoT-enabled devices and less tech-savvy workforce, the industry is highly susceptible to attack and cyber criminals know it. That's why the construction industry has been one of the most targeted sectors by cyber criminals in recent years (with 220+ incidents per year).

Sophisticated AI-powered threats and data leakage

While AI fuels AECO project efficiencies, it's also enabling more sophisticated cyber threats. According to the World Economic Forum's *Global Cybersecurity Outlook 2026*, **data leaks (30%) and advanced adversarial capabilities (28%) are CEOs' most significant security concerns** related to generative AI. Cyberattackers can now hijack internal AI agents to export proprietary data, use realistic deepfakes (i.e. of the CEO of a supply chain partner) to ask employees to disclose IP data, and employ highly-personalized phishing emails to dupe even the most security-conscious employees.

What's more, the increasing reliance on AI tools - be it for forecasting budget constraints or controlling building management systems - introduces new gaps for IP data leakage. IBM found that 13% of data breaches involve AI applications (and 16% of breaches involve attackers using AI), yet a third (34%) of companies still do not assess the security of AI tools before implementing them.

Huge volumes of IP data shared with third parties

Designers and architects. Construction managers and consultants. Suppliers and subcontractors. Every AECO project involves a myriad of external contractors and third-party vendors: each with their own software, security protocols and data standards.

According to Verizon's 2025 Data Breach Investigations Report, **30% of cyber breaches in 2025 involved third parties** - double the year previous - and 65% of CEOs think supply chain disruption attacks have increased in the past year. Given the huge volume of sensitive IP data now moving between internal systems, cloud platforms, BIM/CDE environments and IoT devices in the AECO industry, the chance of IP data leakage from supply chain hacks or vendor misuse is on the rise.

30%

of cyber breaches in 2025 involved third parties - double the year previous

Where AECO IP is most vulnerable (and how Secude closes the security gaps)

AECO's digital workflows are vulnerable to both external and insider threats - be it cyber attackers infiltrating your supply chain or a rogue engineer downloading confidential secrets.

In particular, there are five key areas where your IP data is most vulnerable that AECO must address.

CAD file use

From digital designs and technical drawings to custom processes and engineering layouts, CAD files contain your most precious IP and are essential to modern AECO workflows. But most AECO companies rely on inadequate DLP tools to protect them.

DLP solutions, such as threat detection software and firewalls, act like an external shield or security vault, protecting files within their security perimeter once they are classified. But **DLP security is not embedded in CAD files by default** and does not granularly protect CAD file formats. As most DLP security only kicks in at the storage level, there's a significant risk window between CAD file generation and storage, and when CAD files travel outside of cloud systems (i.e. shared with third-parties).

How Secude closes the gap: file-level CAD security

Secude's automatic file-level security protects CAD files containing your IP as soon as they're generated. Built into the application layer of all major CAD file formats (i.e. Autodesk, Siemens, PTC, and Dassault Systemes etc), Secude can either encrypt your CAD files automatically or add non-encrypted file-level security and data governance when CAD files are created.

As Secude's file-level CAD security lasts for the lifetime of the file, your CAD files are protected before the data is stored internally (or in a cloud-based system like Autodesk Construction Cloud) and no matter where they travel.

	DLP protection	DLP + Secude
Protected in storage	✓	✓
Protected from creation	✗	✓
Protected in transit	✗	✓
Protected for file's lifetime	✗	✓

Sensitive file sharing

Be it sustainability consultants reviewing construction plans or legal advisors picking over contract details, sharing sensitive files with external partners is part and parcel of AECO projects. But DLP does not protect files shared outside of your IT perimeter, so every time a file containing your IP travels beyond your secure environments, you're putting your company at risk.

Encryption is the strongest level of file security, preventing unauthorized third-parties from accessing, stealing, duplicating or forwarding your IP data. But encrypting all AECO project files is inefficient and unnecessary, hindering collaboration and slowing down projects. For some CAD files - and other less-sensitive AECO project files like PDF contracts or building blueprints - AECO needs a lower level of file security with in-built data governance.

How Secude closes the gap: Unencrypted labelling

With Secude's HaloSHARE, you can add visible watermarks to CAD, PDF and MS Office files in bulk. This unencrypted data security simplifies file sharing (your partners don't need decrypting software) and adds traceability of shared files, so you know where and when files travel, and the source of any leaks.

For example, if you want to share factory blueprints with a third-party production partner, HaloSHARE can add visible watermarking of the document ownership. Additionally, HaloSHARE can implant metadata within the files to identify who the file is being shared with and digitally sign them to prevent unauthorized modifications. This metadata also enables traceability of any file leaks.

BIM/CDE environments

From real-time data sharing to seamless project workflows, BIM/CDE environments such as Autodesk Construction Cloud (ACC) and Bentley ProjectWise are vital to modern AECO operations. But when multiple users share access to a system, network or cloud server folder, you not only risk unauthorized access to sensitive files, but increase the possibility of accidental file sharing, file modification and overwriting of files. Meanwhile, as BIM systems become more complex, it's increasingly difficult to prevent unauthorized access (and actions) to your sensitive files.

For example, many BIM/CDEs provide role-based access control to ensure files are only viewed by authorized personnel, but this does not extend to CAD files when they leave these systems. Encrypting CAD files at creation keeps them safe, but prevents collaboration as **file encryption is not compatible with most BIM/CDE environments**, such as ACC. This leaves AECO with an uncomfortable choice: seamless but risky CAD file collaboration with low/no security or secure but inefficient collaboration with heavy file security.

How Secude closes the gap: DLP extension

Secude's unencrypted file-level security provides AECO with a middle ground: seamless collaboration on BIM/CDE environments with heightened data security and monitoring. By implanting metadata into your files' application layer, you can govern which files are allowed to be shared on the CDE and provide controls for who the files are shared with. This ensures that collaborators are digitally authorized to download project files from your AECO collaboration environment.

What's more, with HaloSHARE, you can apply DLP rules to files containing your IP that would not usually be covered. For instance, you can apply Microsoft Purview Information Protection (MPIP) sensitivity labels to files being transported from ACC Docs to another partner Cloud storage location for sharing (i.e. SharePoint) and remove MPIP protection for single or bulk file transport to ACC. In addition, you can add metadata to files uploaded to ACC that can be scanned by data governance platforms (like MS Purview) and used to enforce granular DLP rules, such as preventing downloads or emailing files as an attachment.

Tendering processes

Tenders are a fundamental part of AECO life. Whether it's seeking help from consultants with design & planning or looking for a specific contractor in urgent or specialized projects, AECO contractors often need to share information publicly in an RfP. This information is unlikely to be highly sensitive (i.e. specifications and contract terms), but you still don't want them to be downloaded, misused and shared widely.

On the other side of the fence, AECO subcontractors often need to supply both sensitive and non-sensitive IP data as part of a tendering process to win contracts (i.e. showing designs and previous work). Encrypting these files would make them inaccessible, but leaving them without protection makes the files prone to leakage.

65%

of CEOs think supply chain disruption attacks have increased in the past year

How Secude closes the gap: improved data governance

For AECO firms, Secude's data governance can improve the security and digital rights of files without encryption. By adding discreet and visible watermarking to files and digitally signing them, you can document who has permission to access files, and also hold partners accountable if files are found to be leaked.

In addition, Secude enables you to **protect all of your tender submission documents in one go**, simply by adding files to a specific folder (i.e. OneDrive or SharePoint) using drag-and-drop. Pre-configured access controls also enable you to set expiration dates on certain folders (i.e. once the tender submission period has finished) and add new project partners without the need for additional security procedures.

Supply chain gaps

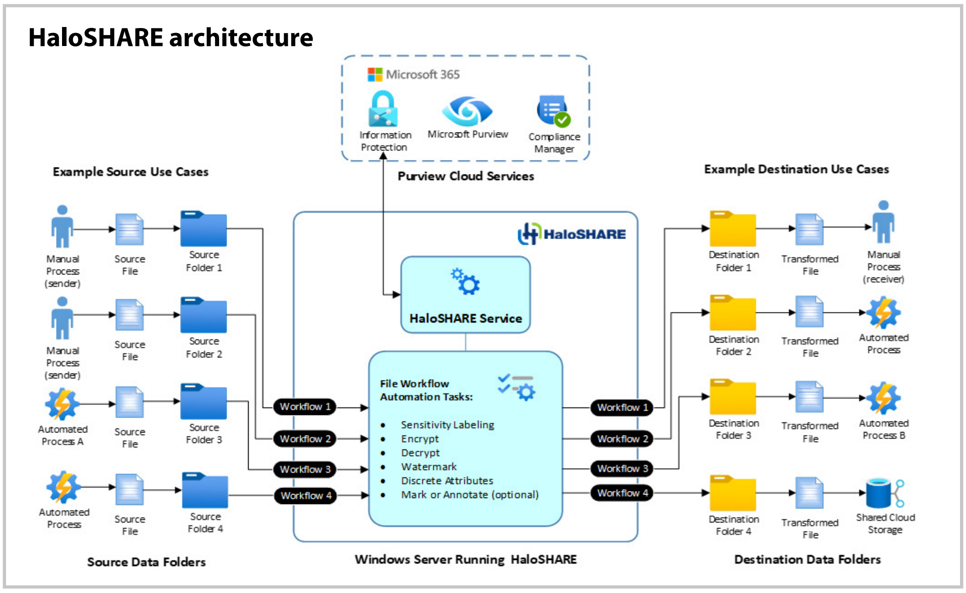
Be it building blueprints or detailed specifications, today's architects and engineers need to share CAD designs with existing and potential supply chain partners. But as soon as these files leave your IT perimeter, they are at risk of duplication, accidental leaking and targeted attacks. Given AECO's high level of third-party collaboration, the industry is particularly exposed to digital supply chain breaches.

For example, imagine you work with a security-focused contractor. You collaborate exclusively on your BIM/CDE environment. You think you're safe. But the contractor subcontracts part of the project work to a fourth-party subcontractor. They download files from your BIM/CDE and share them with the smaller, less security-focused subcontractor. This is where digital supply chain risks arise as even if you require your third-party suppliers to undergo security training, maintain security certifications and conduct regular vulnerability assessments, all it takes is one security lapse in your subcontractor network to compromise the entire project supply chain.

How Secude closes the gap: Lifelong file security

With Secude, you can add lifetime sensitive labels to CAD files that prevent unauthorized access even if there is a data breach further down the supply chain (i.e. fourth or fifth party subcontractors). By extending DLP rules to your IP data, you can set sensitivity labels and custom permissions that ensure only designated users access, edit and download specific files - even when they travel outside of your organization. This not only protects your IP, but also simplifies compliance.

As HaloSHARE enables adjustable sensitivity labels, which can be revoked or set to expire, you can work closely and securely with external suppliers and vendors without impacting the end-user experience. You can also monitor usage and revoke third-party access at any time (i.e. after an NDA expires or project finishes), protecting sensitive files from unintentional leaks and misuse.


HaloSHARE architecture

Example: Autodesk Construction Cloud (ACC)

Autodesk Construction Cloud (ACC) is one of the most widely used BIM/CDE environments by AECO companies. By streamlining operations and connecting workflows, it speeds up project delivery times by up to 50%. But collaborating on ACC has two security issues that can put AECO's IP at risk.

1. Encrypted files break ACC, so you cannot upload encrypted CAD files.
2. Third-party contractors and suppliers can download files from ACC, so if their ACC credentials are compromised, there's nothing to stop hackers from stealing your files.

The solution? Secude's discreet marking and document signing works seamlessly with ACC. By adding discreet watermarking metadata to files before they go into ACC, you can provide file ownership provenance and enforce confidentiality with partners you share files with.

For example, thousands of Madison Square Garden Entertainment's confidential documents were unprotected when sharing from ACC Docs. The HaloSHARE implementation allowed MSG to:

- Apply non-restrictive file protections that did not break ACC Docs functionality.
- Create a path for legally proving file ownership.
- Make AECO partners accountable for data leaks.

As a result, MSG has more confidence sharing their proprietary construction CAD files on ACC and can hold any collaborator that leaks the file legally accountable.

[Download HaloSHARE for AECO]

> **“HaloSHARE is the only solution that addresses our need to identify and trace details of assets shared outside the organization. Prior to HaloSHARE, it would take us days or weeks to mark the large quantity of documents we must share externally. Now we can mark those files in minutes.”**
>
> Global Engineering Group

Remain competitive. Protect your IP.

In the past, AECO project managers have worried that data security could impact their workflows and competitiveness. But nothing derails competitiveness more than IP data leakage.

Intellectual property data makes up the very essence of your company. It’s what makes you stand out in a crowded AECO market, helps you win tenders and fuels your growth. But if you lose your IP, your secrets are exposed and your competitiveness tanks.

Now, with Secude working alongside your existing DLP tools, you can protect your IP data from insider threats, targeted attacks and supply chain vulnerabilities without slowing down your workflows.

Get in touch to find out more: **contact@secude.com.**

Download our **AECO x HaloSHARE brochure**.

HaloSHARE

For more information about Secude: www.secude.com

Email: USA/Canada: AmericasSales@secude.com | **EMEA:** EMEASales@secude.com