THE END OF UNAUTHORISED THIRD-PARTY PLUGINS—A BLESSING OR CURSE FOR K-12 TECHNOLOGY ENVIRONMENTS

A MEMBER-ONLY BRIEF

Many education technology vendors are moving away from supporting third-party plugins and custom code, which understandably raises concerns among school districts. For many technology leaders, these integrations have become essential components of daily operations, connecting student information systems, learning platforms, communication tools, and countless other applications.

These changes may be inconvenient, especially as some will require replacing third-party plugins, including those that have been custom built by districts, that have been working reliably and adding capabilities to their systems. However, this shift is an important improvement for K-12 cybersecurity, data privacy, and system stability.

Third-party plugins have offered great flexibility over the years, allowing technology teams and vendors to customize systems and meet local needs by extending the capabilities of commercial systems. Unfortunately, flexibility also introduced cybersecurity and privacy risk into systems. When a third-party plugin is installed, it becomes part of the system's trusted environment. If the plugin contains a security vulnerability or isn't maintained, it can become an entry point for attackers.

Cyber adversaries view K-12 organizations as attractive targets because Student Information Systems (SIS), Enterprise Resource Management (ERP) including human resources and finance, and Learning Management Systems (LMS) contain an abundance of personally identifiable information (PII) and financial data that require protection. Every additional third-party plugin or piece of custom code in those systems increases the complexity of securing the IT environment and expands the attack surface.

Custom code and third-party plug-ins also make technology environments unpredictable and harder for vendors to support. Updates and patches often break or disable plug-ins, causing unplanned outages. This level of instability is increasingly unacceptable for systems that districts need to be reliably available to operate schools.

This is why many software vendors are moving toward standardized APIs, managed integrations, and formal partner programs. Rather than allowing custom code to run within their applications, vendors are encouraging integration through secure interfaces that use modern

authentication methods, clearly defined permissions, and documented data access methods. While some view this as limiting flexibility, from a security and sustainability perspective, it is establishing healthy guardrails.

Implementing integration standards and oversight makes technology environments more secure, predictable, and easier to support. The architecture and code reviews conducted by vendors of secure APIs and third-party plug-ins created through partner programs are designed to ensure new code does not inadvertently introduce security holes and requires minimum permissions necessary to function. Managed processes for these integrations also provide better logging, auditing, and monitoring, making it easier to identify unusual activity and comply with security and student privacy requirements.

Additionally, a shift to standardized integrations makes the technology environment easier to support. Software updates are less likely to break critical functionality because the integrations are built using documented standards and are known to the software vendor. This improves supportability and reduces downtime. Many district technology departments have experienced the frustration of applying a software update only to discover a custom plugin no longer works. A more managed and standardized approach means technology teams can spend less time troubleshooting integration issues.

Recommendations for Managing Third-Party Plugins

As districts navigate this transition, strong local governance of existing plugins becomes essential. Technology leaders should implement a structured review process to understand what is currently installed, how it operates, and what risks it introduces.

Build and Maintain a Complete Inventory

• Maintain a current inventory of all plugins across systems (SIS, LMS, ERP, HR, finance, transportation, etc.).
• Document where each plugin connects, what systems it touches, and what data flows through it, the purpose of the plug in, and who is responsible for the plug-in (vendor).
• Identify whether any vendor has announced plans to sunset plugin support.

Review Data Access and Permissions

For each plugin:
• Review what data is being sent or accessed.
• Determine the minimum data the plugin needs to function and eliminate unnecessary access.
• Document and review permissions, writable access, and data minimization practices.
• Confirm whether a data-sharing or privacy agreement exists for the plugin.

Evaluate Authentication and Credential Management

• Identify what usernames and passwords the plugin uses.
• Determine whether credentials are ever changed or rotated.
• Review how these credentials are stored, managed, and protected.

• Ensure authentication methods align with modern standards (e.g., OAuth2, SAML, OpenID Connect).

Validate Secure Transmission

• Identify how data is transmitted between systems.
• Confirm that all data in transit is encrypted using TLS 1.3 or another modern, secure protocol.

Assess Update and Maintenance Practices

• Document how often each plugin is updated.
• Review whether the vendor actively maintains the plugin.
• Identify plugins that have not been updated recently or rely on deprecated technologies.

Preparing for the Transition

Will this transition impact IT teams' work? Yes. Some existing integrations will need to be redesigned, and districts may need to work closely with vendors to adopt new connection methods or identify alternatives to current third-party plugins.

While this kind of transition may be disruptive, there are significant long-term benefits, including fewer security vulnerabilities, fewer software-update-related disruptions and outages, and reduced support complexity. While districts may lose some customization options, they will ultimately gain a more secure and resilient technology environment to support the mission of K-12 education.

CoSN is vendor neutral and does not endorse products or services. Any mention of a specific solution is for contextual purposes.

CoSN
Leading Education Innovation