Enabling and Securing the Digital Supply Chain Using IAM and IoT

How can you ensure that specific pieces of the never-ending stream of data reach only the right people and only for a limited time? Identity and Access Management is the key.

Sponsored by

opentext™

Enabling and Securing the Digital Supply Chain Using IAM and IoT

How can you ensure that specific pieces of the never-ending stream of data reach only the right people and only for a limited time? Identity and Access Management is the key.

True supply chain integration, driven by cloud computing, artificial intelligence (AI) and the Internet of Things (IoT), finally appears within the reach of many companies. But it's a complex process involving many moving parts – companies, proprietary software, users and devices, all sharing data.

AI and machine learning offer deeper supply chain insights, but other technologies are necessary to track and manage the flow and transmission of data and, in time, automate and govern the processes behind that data. But as personnel, customers and partners are in constant flux, can this integrated, automated ecosystem ensure that only the right people and devices are accessing the right information for the right reasons – and only for as long as they are cleared to do so? It's one thing to build such an ecosystem and quite another to manage and secure it. Welcome to the next frontier of supply chain management: Securely connecting people, applications and things through Identity and Access Management (IAM).

For decades businesses have relied on electronic data interchange (EDI); the transaction sets governing domestic and international freight movements, advising when specific end-to-end steps in a shipment are certified as initiated and completed. Closing the huge information gaps in between – such as congestion delays, changing weather conditions, equipment malfunction, terminal dwell time, paperwork entry errors, cargo damage in transit – has been the holy grail for supply chain professionals. IoT can close these gaps. But the volume of supply chain data generated by thousands, millions or even billions of embedded sensors tracking the location and condition of equipment and freight assets is daunting, making security and management a significant challenge.

Statista predicts that the number of connected IoT devices worldwide – now estimated at around 23 billion – will more than triple to 75 billion by 2025. Boston Consulting Group forecasts that half of all IoT spending by 2020 will come from manufacturing, transportation/logistics and utilities. Among the primary IoT benefits cited in a 2017 business survey by research firm IDC: inventory management; supply chain visibility and responsiveness; order tracking; and inventory replenishment.

Finally, add the relevant internal emails, texts, insurance boilerplate, compliance documentation, RFQs and responses, internal reports and more that make up as much as 80 percent of shipment-related data – known as unstructured data – and now you're talking serious bandwidth traffic.

Supply chain data: EDI meets IoT and AI

Managing high volumes of information places unique demands on often unrelated and, at times, competing parties in a network. Partners must first undertake digital transformation (DX) – the digitizing of a company's essential data, shareable across a common single-window platform, to enable collaboration. Data access can no longer be "inside-out" – a term used to describe traditional employee identity and access management (IAM) to internal resources – it must be "outside-in." In other words, data access for a connected, secure and intelligent supply chain needs to stem from the external partners by and across that decentralized supply chain network – in the cloud and accessible in real time (and an important counterpoint: to make information totally inaccessible in real time). Visibility must be "pervasive," across people, systems and devices – not only to manage shipments but also to collect and analyze data to measure performance, identify chokepoints and improve customer experience. Yes, it's a complicated reality.

"In a sense, IoT is nothing new in terms of the supply chain," says Bob Slevin, director of product marketing, Covisint IoT, part of enterprise information management firm OpenText. "We're constantly checking on the truck and driver to get visibility into the mobile part of the supply chain. The idea now is to collect real-time data from people, machines and systems at a higher level than just where things are and convert that to get meaningful insights."

OpenText branched into IoT through its 2017 strategic acquisition of Covisint, a cloud platform providing digital identity management and IoT applications for the largest automotive companies in the world as well as their supply chains, which include auto parts suppliers from Canada, Europe, Asia and the U.S. Through its Magellan AI/data analytics platform, OpenText also offers cloud-based AI and IoT software-as-a-service (SaaS) solutions for enterprises looking to enable, secure and analyze their business ecosystems.

Slevin offers the example of such a solution in action: Picture a North American supplier that ships perishables to a Brazilian retailer in a refrigerated container equipped with GPS and temperature sensors programmed to issue status reports every half hour. The sensors are programmed to send an alert if the temperature inside the container exceeded a range of 36-41^{0}F. Once the shipment clears Brazilian customs on a truck and is in transit, the temperature inside the container briefly spikes to 48 degrees in the daytime heat, and then cools back down. The retailer is then sent an advance notification and is able to segregate and inspect the shipment. If there is damage, both the retailer and supplier have a digital record of when, by how much, for how long and in whose custody the damage occurred – in this case a last-mile third-party logistics provider (3PL).

Additionally, AI and IoT working in combination can monitor location and condition of equipment – such as trucks, containers, locomotives, forklifts and more – as well as freight, to spot maintenance and repair problems early, order parts and schedule service. It can issue exception alerts about weather, traffic and other contributors to delays and recommend alternative routing and scheduling options. And it can even track the end-to-end movement and condition of a shipment to minimize risk of theft or tampering and to validate compliance with government regulations, industry standards and corporate policies.

Beyond shipment visibility, predictive analytics can monitor location, quantity and condition of goods in the warehouse to assist with inventory replenishment and quality control. From a broader perspective, the capability to aggregate and interpret structured and unstructured data from all supply chain partners over time enables the system to spot consumer demand patterns and to track waste and costly duplication and measure partner and system performance.

McKinsey estimates that by 2025, IoT will contribute anywhere from $4tr to $11tr to the global economy. Of that total, 70 percent will come from business-to-business (B2B) uses. More than half will accrue in component areas of the supply chain including manufacturing, logistics, work sites and vehicles. Companies deploying the IoT technology stand to reap up to 90 percent of the benefits.

Data generated versus data accessed

Collecting, managing and sharing information across networks of people, systems and devices inevitably raises security concerns. External third parties hacking into devices to gain access to enterprise resources is becoming commonplace. Where do we keep this data, so that it's both safe and accessible? Where and how will this continuous stream of data be captured, stored, analyzed and managed to ensure that specific pieces reach the right people for the right reasons and only for a limited time, while limiting access for everyone else? The key is IAM, an increasingly important supply chain differentiator.

A case in point is the cross-border North American auto parts supplier network, which has been in place for decades but expanded greatly under the 1989 Canada-U.S. Free Trade Agreement and NAFTA. More than 100,000 companies and more than 600,000 users participate within the ecosystem. Each company introduces nuance: Some compete, some may have smaller supply chains while others manufacture or have headquarters outside North America. Detroit cloud computing firm Covisint, now part of OpenText, was among the first vendors to solve the problem of granting secure access to a supplier user. The automotive OEM network described above was Covisint's founding project and from it an IAM solution was borne that is now used by banks, oil and gas companies, insurance companies, consumer products companies, distributors and many others.

"We had to figure out how to provision people, systems and things on a massive scale," explains OpenText director of product marketing - Covisint IAM John Notman. "We're talking about offering information within an organization to others outside of that organization. Identity and access management comes down to trust that you have total visibility into who sees what information and what they can do with it. Put another way: If this process happens without you knowing it, it's called a data breach." The automotive ecosystem is the perfect example of utilizing outside-in IAM. It's among the largest supply chains in the world, and complexity is high due the technical challenges as well as from government regulations. A solution needs to be dynamic, performant and auditable, and users need to be managed differently than internal employees would be.

As companies join the network, supplier employees are onboarded through a registration process where their identities are created, known as "provisioning." Because OpenText Covisint supports delegated administration, supplier IT admins manage the identities from their business so that the originator company doesn't have to, which helps to eliminate process pains along the way. Systems and devices, too, are assigned identifiers to communicate with each other and issue notifications. Users may be provisioned by function or by project – some for a single project or piece of a project. Supplier users may change functions within a project, transition out of a project or position, or leave their organizations. These changes must be tracked. The replacements must be onboarded, and the system must be updated on an ongoing basis. Overlaying those changes are complex authentication and authorization protocols that are handled within Covisint's technology.

One might think that the IAM process is transparent and that the data captured is readily visible, but supply chains need the right technology foundation in place to support transparency. This foundation requires understanding how an IAM solution is applied quite differently to internal employees versus granting resource access to external users from other companies. One such example comes from a leading automotive brand where they use IAM to establish and govern access for their external supplier users to their internal engineering applications. Supplier users leverage a portal for secure connectivity to the engineering applications hosted on the automotive company's intranet, and the users outsource identity management and governance to their IAM vendor. As a result, the automotive company can share key resources with trusted suppliers knowing that security won't be compromised, and the supplier users will have direct access to engineering information, such as product design requirements.

Gaining buy-in across each enterprise in the supply chain is commonly assumed to be the trickiest part of IAM; but since the benefits are equally rewarding for both parties, buy-in isn't the main hurdle. The main hurdle is ecosystem complexity. Unlike with traditional employee IAM, managing external user identities and their access between businesses and resources offers complexities many software vendors have not figured out. And the complexity matters because making even a small mistake could mean either a cybersecurity breach or noncompliance with a regulation like the General Data Protection Regulation (GDPR) or California Privacy Act (CCPA).

One aspect that introduces cybersecurity risk is when the originator company fails to de-provision access for users at a supplier organization after that user changes positions or leaves the company. This issue is almost totally resolved when the right IAM vendor manages that relationship within the broader ecosystem. Another real threat exists due to potential breaches through IoT devices, also known as edge security: as the number of devices increases, so do the number of potential entry points into enterprise systems.

Notman believes the networked supply chain is beyond its early days, that the benefits are real and that risks can be controlled. He believes that the initial growth of networked supply chains came from large companies that had to figure out how to securely connect their ecosystem of external users, such as their suppliers, logistics partners and customer bases. "It's happening," Notman says, "and the world's largest companies are realizing the power, control and security they achieve by combining technology like IAM, IoT and AI. Supply chain ecosystems benefit immediately. Consumers benefit immediately. It's good for the entire system."

Real-time supply chain visibility once was a vision for the industry. Early adopters gained major first-mover advantages and getting there wasn't a walk in the park. Now, businesses can fully appreciate the benefits of a securely connecting supply chain.

To learn more about ways to drive digital transformation and enable an intelligent supply chain and enterprise with IoT and IAM, visit:
opentext.com/
connected-supply-chain