Why Identity and Access Management and Zero Trust Architecture Are Essential to Supply Chain Risk Management

IAM and ZTA are critical components of a comprehensive system for protecting the supply chain from internal, external, and third-party threats.

Preventing and deterring cyberattacks in the ever-changing supply chain landscape involves more than just safeguarding against external threats. Cyber threats can spread quickly throughout the complex network of vendors and suppliers that make up a supply chain. To prevent that from happening, safeguards must also protect supply chains from internal threats as well as third-party threats that might enter a network through authorized channels on the backs of partners and suppliers.

Identity and access management (IAM) and zero trust architecture (ZTA) operate under the premise that there is no single perimeter within a supply chain or even within an organization. IAM and ZTA support supply chain security by providing mechanisms for identity verification and device validation to maintain ongoing defenses against invisible threats.

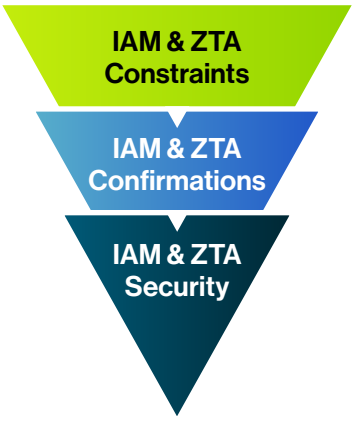
Layers of IAM and ZTA Security

Today's organizations face complex challenges and threats throughout their supply networks, making supply chain risk management (SCRM) a top priority. IAM and ZTA are critical to enhancing SCRM in three key ways:

1. They help prevent unauthorized outsiders from accessing an entity's systems and networks. IAM and ZTA technologies create an external bubble around the entity, protecting against unauthorized entry by "bad guys" or others seeking to get "inside" without the necessary credentials, cyber profiles, and identifying features. This is not a one-time challenge. Unauthorized outsiders must overcome these barriers every time they try to breach the entity's computers, data, systems, and networks.

2. IAM and ZTA safeguard against third parties whose own systems may have been breached. There have been cases where a third-party contractor did not have strong IAM features and, as a result, was hacked. This enabled the attacker to obtain superuser credentials for different organizations with which the contractor was affiliated. These superuser credentials can serve as a springboard to get to the real targets—an organization's customers.

3. These technologies forestall insider threats via increased containerization. In containerized systems, authorized access to one part of a network does not allow for access to others, unless IAM and ZTA checks are passed. Different levels of user privilege are provided only based on authentication of IAM and ZTA protocols.



Layers of SCRM Protection

Comprehensive SCRM Protection

Effective deployment of these crucial access tools provides digital fortification at every level of an organization. Using a physical security analogy, imagine an office building or government agency with many different companies, departments, and/or offices inside.

- IAM and ZTA constrain how close those without access credentials can get to the facility, to the front door, or beyond the guards and turnstiles. This keeps outsiders out. That is the first layer of a multilayered defense and is crucial to stopping those wanting to undermine supply chain integrity.
- For a second layer, if someone with access (e.g., a third-party technician, such as an independent IT maintenance contractor) presents the proper credentials, that individual can proceed through the first layer. But without proper IAM and ZTA confirmations, the individual will not be able to proceed to the floor they are seeking (their badge will not allow them to press that floor in the elevator or overcome additional barriers or guards). Thus, whether the individual has malevolent intentions or is unaware that their software, tools, or equipment has been compromised, they cannot access or harm the part of the agency or company they are servicing.
- For the third layer, strong IAM and ZTA security can help protect against even those who are authorized to access various parts of the building or system gaining access to areas for which they do not have authorization. For instance, if someone has access to the financial parts of a company's system, that individual could be blocked from getting into others (e.g., IT server rooms) or—even within the server room—from making modifications to some servers.

Organizations can reduce risk to supply chains and other valuable parts of an organization's data, systems, and networks by implementing lateral user authentication and utilizing multilevel permissions for creating and maintaining access policies. There are multiple steps to enhancing the security of supply chains, from employing and checking SBOMs (software bill of materials) to undertaking due diligence on third parties and testing for counterfeits and substandard parts. Having strong IAM and ZTA capabilities is a vital element of ensuring that supply chains are secure and a strong SCRM program is in place. Doing so helps to safeguard against unauthorized individuals or entities gaining access to your supply chain in the first place—and ensures that even permitted users can enter and use only those systems to which they have vetted access.

How Guidehouse Can Help

Guidehouse has the supply chain risk management expertise, capabilities, tools, data, and discretion necessary to provide government and industry organizations with deeper insights into their supply chains and address any identified risks to the organization or clients. This information is critical to helping organizations understand how much risk they are currently exposed to and how to reduce that risk in the future. This includes deep experience with IAM and ZTA technologies, as well as other strategies for protecting supply chains from hidden threats. We have a proven track record of successfully delivering these insights to sensitive agencies and industrial and technology companies. Guidehouse's experience can help your organization better protect and manage the risks in your supply chains.

Contacts

Amanda Kane
Partner, Cybersecurity
amkane@guidehouse.com

Jason Dury
Director, Cybersecurity
jdury@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 55 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit **www.guidehouse.com.**

Web: guidehouse.com/cybersecurity / @GHTechSolutions / linkedin.com/company/guidehouse-technology-solutions/

Guidehouse outwit complexity™