How Zero Trust Protects a Vulnerable Supply Chain

Modern

The Industrial Internet of Things is shaking up the world of manufacturing and all of its supply chains. Thanks to IoT devices and the steady rollout of 5G connectivity, companies have an unprecedented look into the health of the shop floor, can monitor for shipping-disruptive weather conditions, and can plan maintenance to ensure the least amount of downtime. These sensors are an absolute revolution, but there's a dark side to the sensors as well.

Manufacturers must consider new cybersecurity concerns as each new IoT device represents a potential weak point in the company's network. Each device presents a tempting target for hackers who are looking to break into the network, but focusing on the individual devices is the wrong answer to the problem. The solution should be a secure network using a zero-trust model.

Supply chains are more vulnerable than ever

Supply chains are notorious for housing security loopholes sensitive to attacks. In response, companies have focused on making all of the individual devices within the supply chain more secure. However, with increasing connectivity and layers of complexity, such an endpoint-focused approach isn't sustainable.

For example, companies often password protect only their administrator-level devices or they fail to use multi-factor authentication. Attacks can then happen from third-party software, going undetected until the next update—something that caused one of the worst supply chain attacks in recent history at A.P. Møller-Maersk.

The National Counterintelligence and Security Center identified the reduction of threats to U.S. supply chains as a 2021 top priority, and the urgency hasn't changed as we enter 2022. As adoption of the latest technologies brings more opacity and complexity to the supply chain– and the threat reduction focus is coupled with increased reliance on IoT– both small and enterprise supply chain models need a new approach to cybersecurity.

Zero trust security mitigates vulnerabilities

Companies cannot eliminate third parties, nor can they go back to a time before IoT. Instead, addressing weaknesses is a network-wide endeavor. A zero-trust model assumes that there is no difference between "the good" and "the bad" because every access point is treated with the same scrutiny. Each request for network access is individually validated and then access is only provided to the resources and applications specified for that device or user within the zero-trust framework.

The NIST-developed framework for zero trust architectures assumes that all access up and down the chain is a threat. Organizations don't have the same level of transparency for operations thanks to third and even fourth-party activities, so assuming all actors are a potential threat until proven otherwise is a very effective strategy to keep the network secure.

Zero trust can be implemented through either an on-premise solution or a cloud-based solution, but continuous monitoring is key to ensuring that the company's security remains intact. Ideally, every organizational partner involved in a company's supply chain also adopts a zero-trust architecture (ZTA).

Defining the zero-trust architecture

There are three core components of a ZTA:

1. **Policy engine**: Makes the decision to grant, deny, or revoke access to a resource for a given user. It calculates the trust score of the actor based on a variety of factors. It works by filtering requests through a trust algorithm running on strict role-based permissions.
2. **Policy administrator**: Responsible for establishing or terminating a transaction. It uses the policy engine's permission decisions to generate session-specific authentication.
3. **Policy enforcement point**: Handles enabling, monitoring, and terminating connections between subjects and the network. It stands between an enterprise resource and a potential actor and is configured using policy updates from the policy administrator.

This framework assesses all requests from all sources, assuming that all are threat actors until proven otherwise.

Implement ZTA with a data fabric

A data fabric contains the capabilities necessary to create a zero-trust security framework for enterprise logistics and supply chains. This is done through several pieces of core data fabric functionality, each of which are described next.

Enhanced governance
The first issue with ZTA is establishing governance capable of evaluating each request without slowing the data flow. A data fabric provides AttributeBased Access Control (ABAC), making it easy for administrators to set parameters for access that are effective, secure, and consistent.

A data fabric supports several different kinds of zero trust models, including identity governance and micro-segmentation. It provides access to data that stakeholders need—no more data locked in prisons — but can monitor and pivot to establish or terminate access as necessary.

Automated controls and reporting
A data fabric provides necessary automations to keep enterprises enabled to access data in a timely and secure fashion. The solution offers a contextual understanding of data. The enterprise can set controls based on a wide range of parameters, and those are applied with uniformity across the entire network. There are no more silos preventing access to diverse data stores.

Then, companies can monitor their data health with robust reporting controls and pivot data operations based on those reports. It offers the company transparency and observability of their data, something not previously possible.

Not another third party
Trusting a third-party service to monitor other third-party services is not a good way to manage security. Instead, a data fabric provides a software solution that provides absolute control of data to the company itself instead of creating a new security risk.

DataOS, for example, encodes data policies into the solution. Users have the appropriate level of access using defined tags that are immediately configurable by authorized managers. This level of granularity doesn't compromise flexibility or create pipeline delays.

Curious about how DataOS makes security and compliance automatic? Download our whitepaper for a closer look.

Protecting the supply chain

Supply chains aren't just vulnerable; disruption can cost the economy dearly. The consequences of the SolarWinds attack, as a recent example, are still unfolding and will likely be felt far into the future. Leveraging a zero-trust architecture supported by data fabric capabilities, enterprises can reduce the risk that bad actors can gain access to any part of the network.

ZTA is at the core of DataOS. Schedule a demo to discover how DataOS can transform siloed data stores into a coherent pipeline with clear insights, safely and effectively.

It's time to free your data →

BY E. WALLACE

The Modern Data Company
306 Cambridge Ave
Palo Alto, CA 94306
TheModernDataCompany.com
info@TMDC.io