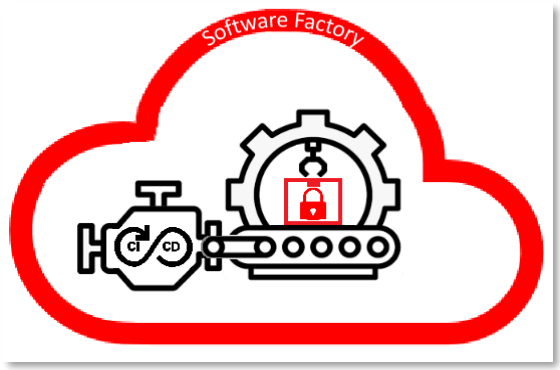
KARTHIK CONSULTING
Beyond the expected

3120 Fairview Park Drive
Suite 800
Falls Church, VA 22042
www.karthikconsulting.com

AT A GLANCE

Zero Trust via Software Factory

An opportunity exists at the intersection of two leading-edge IT movements: Software Factories (SFs); and Zero Trust. With Karthik Consulting's unique combination of cloud-based Software Factory development and our deep cybersecurity expertise, we are well-positioned to accelerate the implementation and adoption of Zero Trust Architectures and the associated policies.



Using the Cybersecurity and Infrastructure Security Agency's (CISA) Foundation of Zero Trust as a basis for discussion, this whitepaper provides an overview of the various techniques we use to implement Zero Trust via Software Factories. Figure 1 presents CISA's Foundation of Zero Trust.

"Success occurs when opportunity meets preparation."

- Zig Ziglar

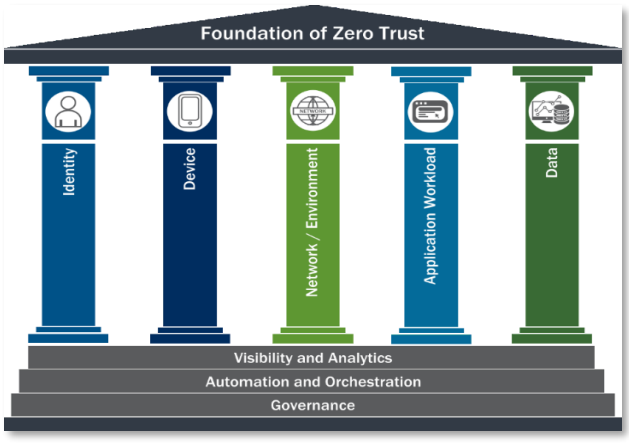


FIGURE 1: CISA'S FOUNDATION OF ZERO TRUST

With CISA's model as our guidepost, this paper explores the methods and functionality we integrate into our Software Factories to support Zero Trust initiatives. We start by describing how we promote the Foundation of Zero Trust, then delve into the details for each pillar in the model. With Zero Trust being this paper's topic, we want to emphasize there are many Software Factory features and benefits which are not addressed herein (i.e., those beyond Zero Trust).

Continued on next page

With Software Factories processing an agency's full portfolio of projects, each factory is positioned as an IT hub within an organization. Hence, through the factory, we achieve the following:

- Leverage various cybersecurity tools to improve the security posture of each project and thus the organization as a whole.
- Ensure compliance with the organization's Zero Trust Architecture (ZTA), including assistance with practical progression towards full implementation of the ZTA.[1]
- Collect metrics on all projects, including quality and "security maturity" of the code.
- Determine where training efforts would be most effective within the organization (e.g., to address frequently occurring security issues within code).
- Assess the effectiveness of the factory and its tools; identify areas for improvement such as new, additional, or upgraded tools.
- Through the integration of common Zero Trust functionality into each processed project, SFs permit an organization to centralize[2] and thus streamline the maintenance of policies which govern permissions for subjects and devices – including Policy-Based Access Controls (PBAC) and Comply to Connect (C2C) rules.

General Approach

By providing an organization's developers with a common authentication toolkit for subjects, Software Factories standardize authentication processing and centralize the administration of authentication policies. Additionally, the organization-wide use of an authentication toolkit familiarizes developers with its ease-of-use (i.e., API-based integration), allows users of the associated apps to acquire firsthand experience with the in-app authentication processes, and gives all members of the organization insight into the toolkit's benefits.

The authentication toolkit operates on two different types of subjects: (a) Users (humans); (b) Non-person entities (NPEs).

General Approach

Karthik Consulting's Software Factories deliver another valuable security toolkit to projects: one for device authorization. Through the integration of this toolkit into an organization's projects, Software Factories provide the platform to perform real-time C2C assessments of a project's endpoints as well as any component of its Solution Architecture infrastructure.

Through configurable policies, we also enforce the usage of authorized devices to access our Software Factories – including but not limited to hardware devices such as Government Furnished Equipment (GFE) or user sessions via Virtual Desktop Infrastructure (VDI).

[1]For a practical roadmap to guide the transition to a ZTA, reference CISA's "Zero Trust Maturity Model" (https://www.cisa.gov/sites/default/files/publications/CISA%2520Zero%2520Trust%2520Maturity%2520Model_Draft.pdf)

[2] Throughout this whitepaper, we use the term "centralize" (and its derivatives) to convey the concept of streamlining reusable processing among a core team of experts, tools, and processes. Following best practices, we also implement high-availability of the underlying logic and data (e.g., via distributed microservices and replicated data). Thus, "centralize" does not imply single points of failure.

Continued on next page

General Approach

The fundamental purpose of a Software Factory is to process source code from the full set of projects within an organization's IT portfolio. This could amount to hundreds if not thousands of projects. Therefore, it's important for a factory to avoid the unintentional introduction of dependencies and interference between the projects it handles at any given time – lest the projects could work while running within the factory, but malfunction when operating outside the factory. Additionally, certain factory processing should be conducted in isolation, such as performance testing.

Micro-segmented networks – the building blocks of Zero Trust Networks (ZTNs) – are a natural fit to meet these requirements. That is, micro-segmented networks give SFs the ability to isolate a single project from all others.

General Approach

By integrating monitoring functionality into all factory-built containers, Software Factories lay the roads for simple, practical, and effective SIEM via Continuous Monitoring (ConMon) within each project. Besides improving the security posture of each project and enabling continuous ATO (cATO), SIEM and ConMon integrate with: (a) system auto-scaling based on resource consumption driven by application workload; (b) dynamic policy updates based on threat detection and real-time risk analysis; and (c) automatic self-healing for known issues which are auto-detected.

Software Factories also enforce process tagging standards in each project's code base, thus aiding with the detailed analytics associated with application processes.

General Approach

Software Factories enforce the usage of Policy-Based Access Controls (PBAC) to (a) improve the granularity of resource access (web services, system data, etc.); and (b) provide flexibility to adapt to organizational change in real-time (e.g., the expansion or reduction of access privileges for one or more users or groups thereof).

Additionally, Software Factories can enforce the usage of: (a) data encryption functionality for all projects, to include coverage of data at rest and in motion; and (b) keystores to manage certificates and private keys used in cryptographic protocols.

ABOUT US

Karthik Consulting was founded in 2008 to be a reliable and trusted advisor for our customers, providing independent, unbiased, and proven solutions that mitigate risk and help solve enterprise-wide IT challenges.

Our Cyber Security, Software Development and Program Management focus areas (and work methodology) ensure that we can deliver not just solutions, but architecture that scales and grows with the customer's needs over time. We are able to assist in projects ranging from short advisory engagements to assembling a full team to deliver a solution from concept through implementation and on-going management. KC has access to industry experts in various technologies and teaming partners to meet any of your IT challenges. The vision of KC is to bring the innovation, passion and agility of the commercial IT industry to meet the unique challenges of the federal government. We are a DOD Cleared Facility with a DCAA-approved accounting system.

CONTACT
Felix Martin, 571 435 7632
fmartin@karthikconsulting.com

CAGE: 56GH3
DUNS: 828199880
UEI: FGNNM7KNUPF6

PRIME CONTRACT VEHICLES:
GSA STARS III 8(a)
GSA MAS
GSA OASIS Pool 1 and 3
NIH CIO-SP3 8(a) & SB
Air Force SBEAS
Army RS3
Navy Seaport-NexGen
FAA eFAST