Zero Trust Strategy for Comprehensive Security

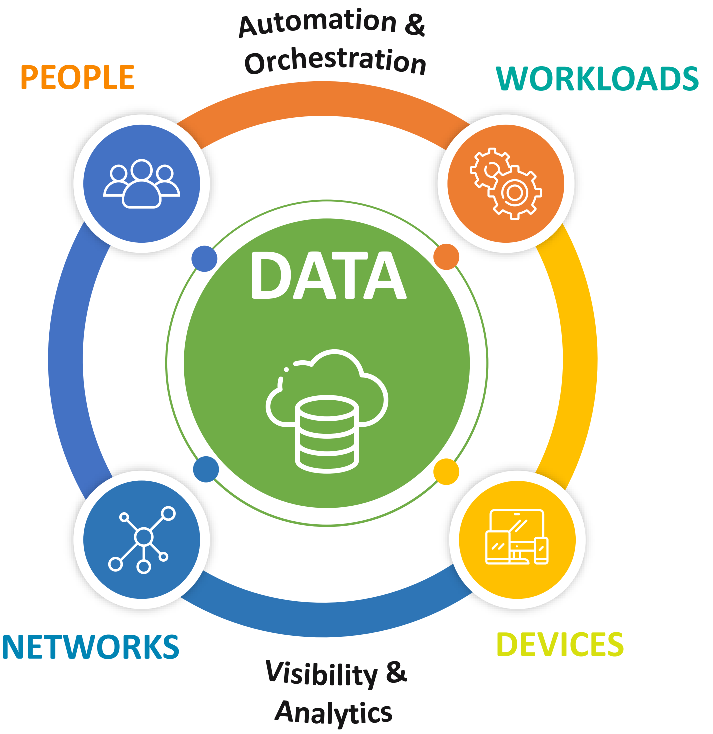
What is Zero Trust?

BMC recognizes that Zero Trust is not a solution or product but rather a philosophy or framework that assumes a network's security is *always* at risk due to both internal and external threats. Zero Trust is a shift of defenses towards a more comprehensive IT security model that allows organizations to restrict access to networks, applications, and environments—without sacrificing performance and user experience. BMC and our partner network can help you in your Zero Trust journey.

Why this matters

In today's environment, organizations must assume their network has been penetrated. Zero Trust assumes that all users, data, and devices pose a threat. In other words, trust no one. The Federal zero trust architecture (ZTA) strategy requires agencies to meet specific cybersecurity standards and objectives by September 30, 2024, to reinforce the government's defenses[1].

Forrester's Zero Trust eXtended (ZTX) Framework[2]



Why BMC?

Every cabinet-level agency and every branch of the US military already use BMC in production:

UNITED STATES NAVY	DEPARTMENT OF THE TREASURY
UNITED STATES MARINE CORPS	DEPARTMENT OF AGRICULTURE
UNITED STATES AIR FORCE	DEPARTMENT OF COMMERCE
UNITED STATES ARMY	DEPARTMENT OF HEALTH AND HUMAN SERVICES
DEPARTMENT OF HOMELAND SECURITY	DEPARTMENT OF ENERGY

ZERO TRUST CORE PILLARS–ENTERPRISE

DATA

BMC coordinates secure and reliable data movement throughout the enterprise and enables orchestration of data pipelines

DEVICE & ENDPOINT

BMC discovers and monitors all devices, endpoints, and applications to identify blind spots, enforce compliance, and manage patching requirements to protect the enterprise from intrusion

NETWORK & ENVIRONMENT

BMC provides management and monitoring of enterprise network environments to analyze vulnerabilities, enhance visibility, and respond to threats across network devices

APPLICATION & WORKLOAD

BMC automates developer workload deployment to enhance DevSecOps and assists in the integration between disparate application workflows

USER

BMC can provide vendor-agnostic identity integration, multifactor authentications with CAC, multi-tenancy, and data-masking to ensure environment access is only provided when necessary

VISIBILITY & ANALYTICS

BMC discovers all enterprise assets and provides real-time visibility and analytics from mobile to mainframe to support threat detection and SIEM through AI/ML-driven predictive analytics

AUTOMATION & ORCHESTRATION

BMC provides full AI/ML-enhanced SOAR capabilities to orchestrate and automate incident response as well as remediation patching for operating systems and applications

> *“The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access."*
>
> **- Department of Defense Zero Trust Reference Architecture, Feb 2021**

[1] MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, M-22-09; Moving the U.S Government Toward Zero Trust Cybersecurity Principles

[2] Forrester: The Zero Trust eXtended (ZTX) Ecosystem, 2021