FORUM SYSTEMS™

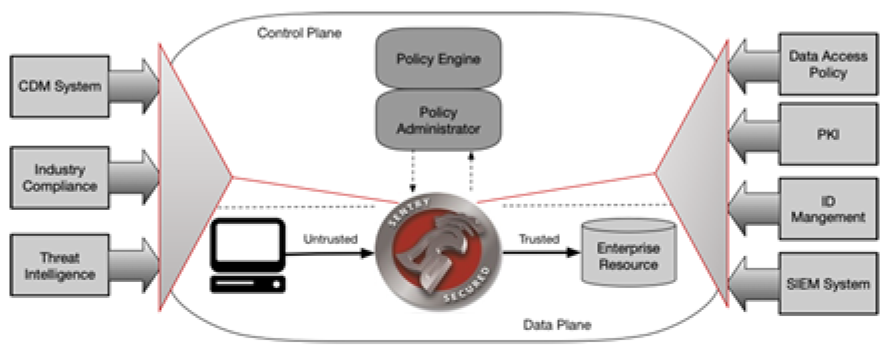
THE LEADER IN API SECURITY & ZERO TRUST

ACHIEVING SECURE ZERO TRUST ARCHITECTURE

With the evolution of mobile and cloud computing, traditional information borders no longer reside at network boundaries. Applications, devices, and systems communicate with each other on premise and in the cloud, exposing sensitive information with each of those communications. The traditional "brick and mortar" cybersecurity umbrella approach of network border protection is a proven failed model where breaches are often a result of internal application or system compromise. Thus, the perimeter security hardened shell on the outside does nothing to ensure protection of the internal applications and their communications on the inside.

In September 2019, the National Institute of Standards and Technology (NIST) issued draft Special Publication 800-207 titled "Zero Trust Architecture" (ZTA) to, "...develop a technology-neutral set of terms, definitions, and logical components of network infrastructure using a ZTA strategy." ZTA is defined as, "a collection of concepts, ideas, and component relationships (architectures) designed to eliminate the uncertainty in enforcing accurate access decisions in information systems and services. This definition focuses on the crux of the issue, which is to eliminate unauthorized access to data and services, coupled with making the access control enforcement as granular as possible".

The enabling mechanisms recommended by NIST to implement and maintain a ZTA are a Policy Decision Point (PDP) and a corresponding Policy Enforcement Point (PEP).



Seamless, Agentless, Cyber-Secure PEP

Cyber Secure PEP

Agentless policy enforcement point with protocol, message, and identity security built-in. Protocol and message security with authentication and access control combined for identity and data analysis and enforcement. FIPS 140-2 Certified PKI, US Department of Defense (DoD) Certified PKI, Common Criteria NIAP NDPP Certified Hardware.

Integrated SSO and MFA

Role-based policy controls with universal support of user credential and tokens ranging from on premise to cloud-based. Automatic conversion of identity formats allows multiple-to-one credential normalization.

Agentless Monitoring

Seamless deployment with no footprint on the client or service endpoints. In-line communication flow provides real-time data collection with analysis, alerting, and consolidated reporting. Integrates with SIEM and dashboard systems and Machine Learning and AI engines.

Data Level Policy Controls

Content and application level threat detection and prevention for intrusion detection and data leakage. Data at rest encryption for content-level data security.

FORUM SENTRY™

HARDWARE | AMAZON AMI | AZURE IMAGE | VMWARE | DOCKER | LINUX | WINDOWS

FIPS 140-2 · DoD PKI · NIAP NDPP · PATENT 7,516,333

www.forumsys.com

FORUM SYSTEMS™

THE LEADER IN API SECURITY & ZERO TRUST

Forum Systems provides a solution to the Zero Trust cybersecurity challenge with a state-of-the-art, rapidly scalable, rules-based security technology that will allow federal and commercial organizations to deploy a best-in-class, nimble, agile, and highly performant enterprise Policy Enforcement Point (PEP) solution for a Zero Trust network model.

ZERO TRUST CAPABILITY	FORUM SENTRY - COTS PRODUCT SOLUTON FIPS 140-2 and NDDP Certified Technology
Securely Enforce and Enable Communications	Forum Sentry provides a comprehensive set of standardized formats and technologies to provide seamless interoperability. Forum Sentry delivers data transformation, data mapping, and data validation, enabling secure PEP enablement with seamless deployment and no coding or environment disruption.
Fast and easy authentication with SSO and MFA	Forum Sentry provides built-in capabilities for modern and legacy identity token formats ranging from username/password and PKI paradigms to modern token formats such as Security Assertion Markup Language (SAML), Open Authentication (OAuth) and JSON Web Token (JWT). SSO session management and token services are part of the built-in technology capabilities, as are step-up authentication mechanisms that provide MFA.
Encrypt On Premise and Cloud Communications	Forum Sentry provides accelerated FIPS 140-2 encryption to ensure complete data privacy for data in motion and at rest.
Ensure Integrity of Data	Forum Sentry provides integrated hashing and digital signatures to ensure communications can be signed and verified.
Leverage Machine Learning and AI	Forum Sentry captures contextual metrics for individual data transactions and provides a meta-data AI logging format with over 20 universal transaction properties for advanced machine learning heuristics.

About Forum Systems

Forum Systems is the global leader in API Security and Zero Trust with an industry-certified and patented COTS product that secures enterprise infrastructure. Forum Systems has built the core architecture of its technology on the foundation of FIPS 140-2 and NDPP requirements.

The Forum Systems technology has been trusted in the commercial and government networks for over 18 years with proven mission critical deployments such as protecting the US revenue stream with a Zero Trust PEP for the Internal Revenue Service electronic tax returns as well as for the FAA weather feeds coming from NWS and NOAA.

Learn more at http://www.forumsys.com/zero-trust