TYCHON

TYCHON Agentless
Product Sheet

STIG AND IAVA MANAGEMENT WITH NO NEW INFRASTRUCTURE

- TYCHON Agentless delivers STIG, CVE/IAVA, and Endpoint Protection status without adding new server infrastructure or services to endpoints.
- Datasets fully comply with Vulnerability and STIG reporting standards and integrate into Comply-to-Connect (C2C) for instant zero trust value.
- A lightweight delivery of our most valuable content – designed to interface with Elastic, Splunk, Microsoft Sentinel in Azure, and more.

TYCHON Agentless delivers a seamless *DOD integration.*

- **Comply-to-Connect:** Integrated with DoD C2C services for seamless decisions.
- **Serverless + Agentless:** No new services on endpoints and nothing added to infrastructure.
- **Local Access:** 3rd party tools and administrators gain insight without additional configurations.
- **Cloud and On-Prem:** Run from your own IL5/IL6 stack or run on-prem/deployed environments.

725 Jackson Street, Suite 101 I Fredericksburg, VA

tychon.io | info@tychon.io

TYCHON

Integrated with Existing Investments

TYCHON Agentless deploys through Intune/MECM and is designed to enhance DoD focused investments in Elastic, Microsoft, Splunk, DISA CMRS, and Forescout for an easy install and zero-added maintenance.

Forescout | Elastic | Microsoft | Splunk | DISA CMRS

TYCHON LLC'S DOD ZERO TRUST ALIGNMENT

The table below outlines the current DoD strategy for Zero Trust capabilities. The colored boxes represent how TYCHON Enterprise, in combination with Elastic, aligns to meet these needs.

DOD ZERO TRUST ARCHITECTURE

User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	2.1 Device Inventory	3.1 Application Inventory	4.1 Data Catalog Risk Assessment	5.1 Data Flow Mapping	6.1 Policy Decision Point & Policy Orchestration	7.1 Log All Traffic (Network Data, Apps, Users)
1.2 Conditional User Access	2.2 Device Detection & Compliance	3.2 Secure Software Development & Integration	4.2 DoD Enterprise Data Governance	5.2 Software Defined Networking	6.2 Critical Process Automation	7.2 Security Information & Event Management
1.3 Multi-factor Authentication	2.3 Device Authorization with Real-Time Inspection	3.3 Software Risk Management	4.3 Data Labeling & Tagging	5.3 Macro Segmentation	6.3 Machine Learning	7.3 Common Security & Risk Analytics
1.4 Privileged Access Management	2.4 Remote Access	3.4 Resource Authorization & Integration	4.4 Data Monitoring & Sensing	5.4 Micro Segmentation	6.4 Artificial Intelligence	7.4 User & Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	2.5 Automated Asset, Vulnerability, & Patch Management	3.5 Continuous Monitoring & Ongoing Authorization	4.5 Data Encryption & Rights Management		6.5 Security Orchestration Automation & Response	7.5 Threat Intelligence Integration
1.6 Behavioral, Contextual ID, & Biometrics	2.6 Unified Endpoint Management & Mobile Device Management*		4.6 Data Loss Prevention		6.6 API Standardization	7.6 Automated Dynamic Policies
1.7 Least Privileged Access	2.7 Endpoint & Extended Detection & Response		4.7 Data Access Control		6.7 Security Operations Center & Incident Response	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

Legend