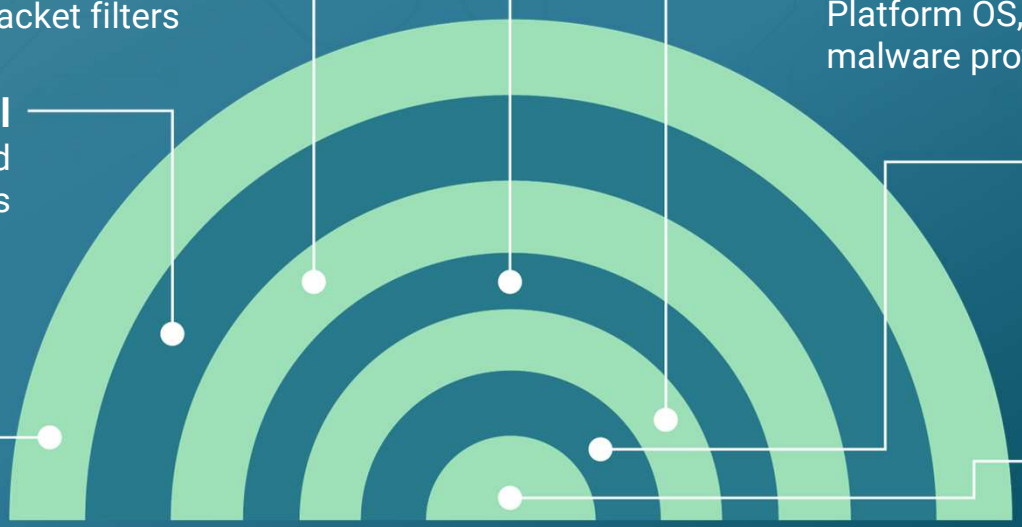
Trust in the Commonwealth's Future!

ZERO TRUST STRATEGY FOR MANAGED SECURITY SERVICES CONTRACTS

Michael Watson – VITA Chief Information Security Officer

Current threat defense model: defense in depth



Internal network
Firewall, intrusion detection and encryption

Perimeter
Firewall, VPN and packet filters

Host
Platform OS, patches and malware protection

Physical
Locks, fences and security guards

App
SSO, authentication and authorization

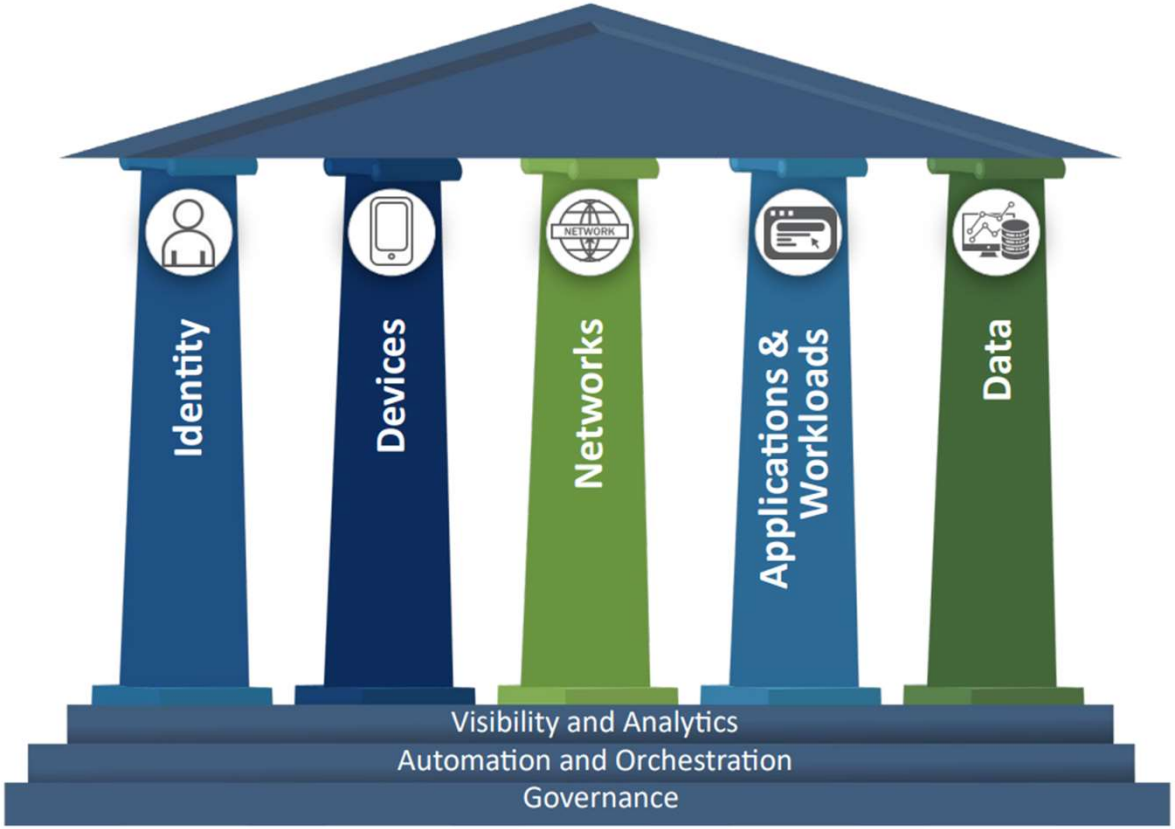
Policies, procedures and awareness
Passwords, policies and data classification

Data
Database, content and message security

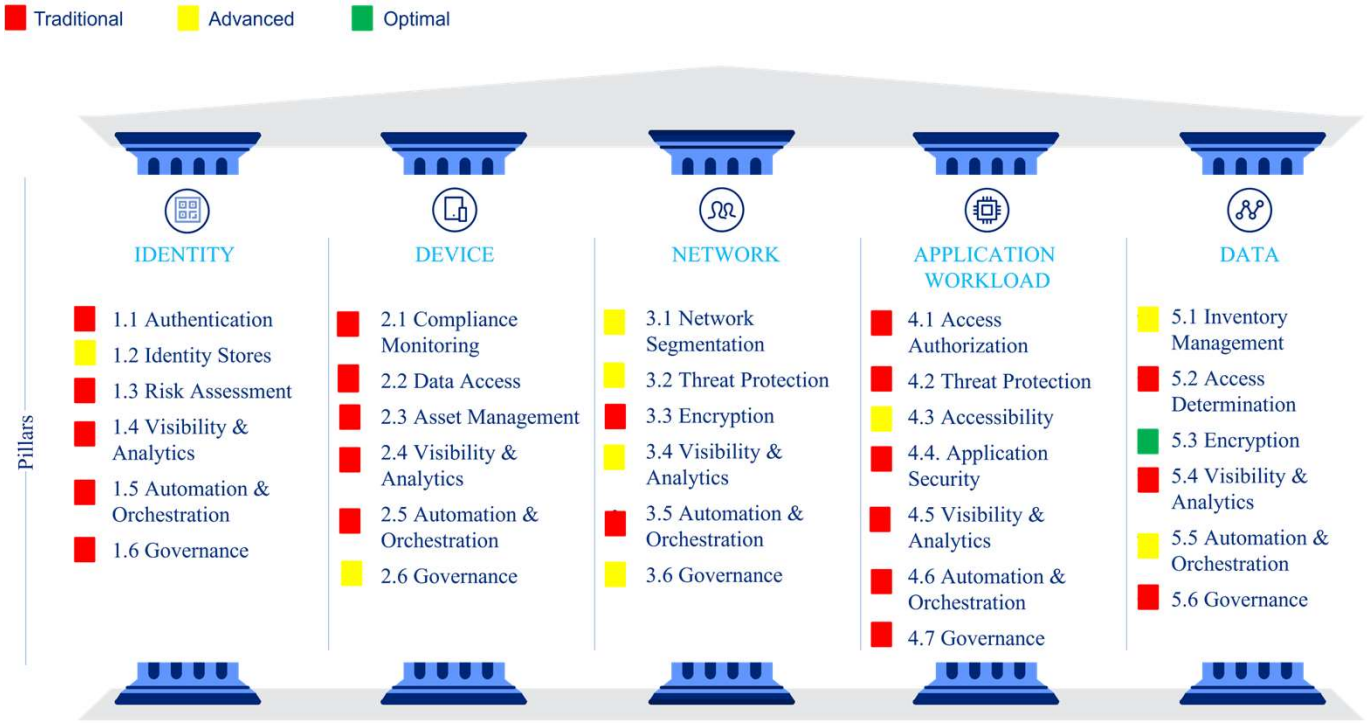
VIRGINIA IT AGENCY

vita.virginia.gov

The Zero Trust Model

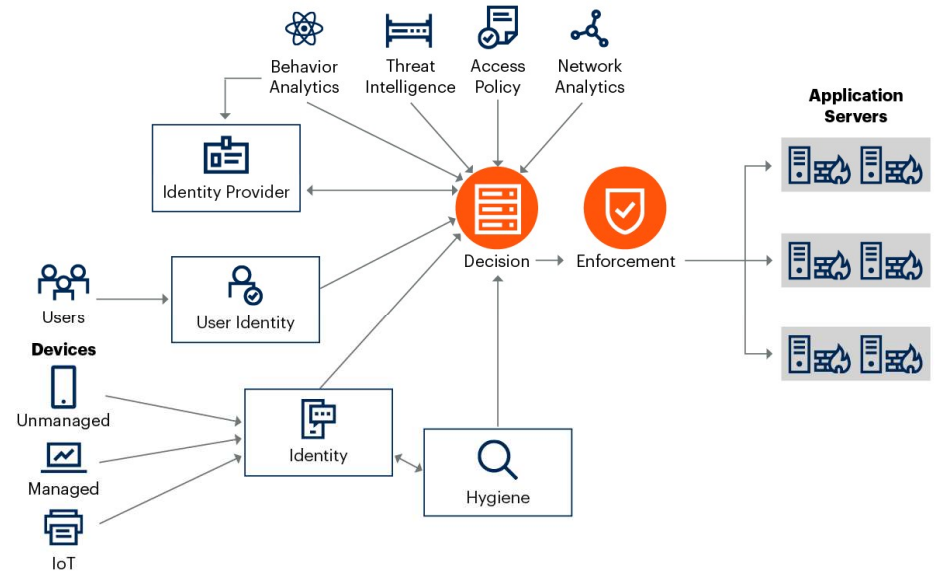


Where We Started: Zero Trust Pillars



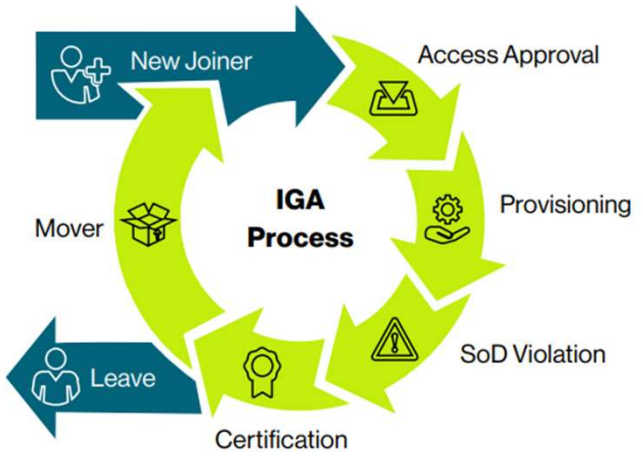
Implementation Principles

- **Aggregation and Visibility**
  - Leverage existing toolsets and data sources to identify the attack surface
  - Capture data and system relationships
- **Technology Independence**
  - Solutions understand the technology instead of depend on the technology
- **Controls at the Data**
  - Controls should protect the data directly not just the access to the data
- **Identity and Access Verification**
  - Solutions must understand identities



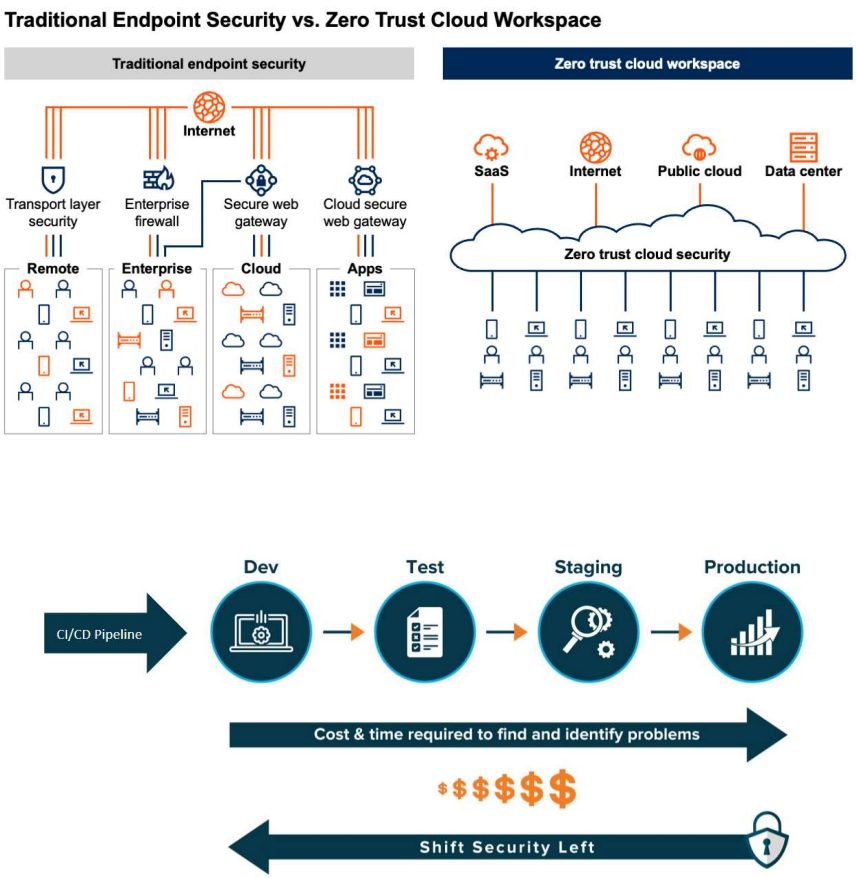
Identity Pillar

- **Continuous Identity Governance**
  - Identity actions assigned based on risk
  - Certifications and entitlements
- **Just-in-Time Access**
  - Redefine the term for administrator
  - Remove privileged accounts
- **Automated User Provisioning**
  - Must be authenticated, continuously monitored and verified for access
- **Leverage Centralized Identity Stores**
  - One identity for all



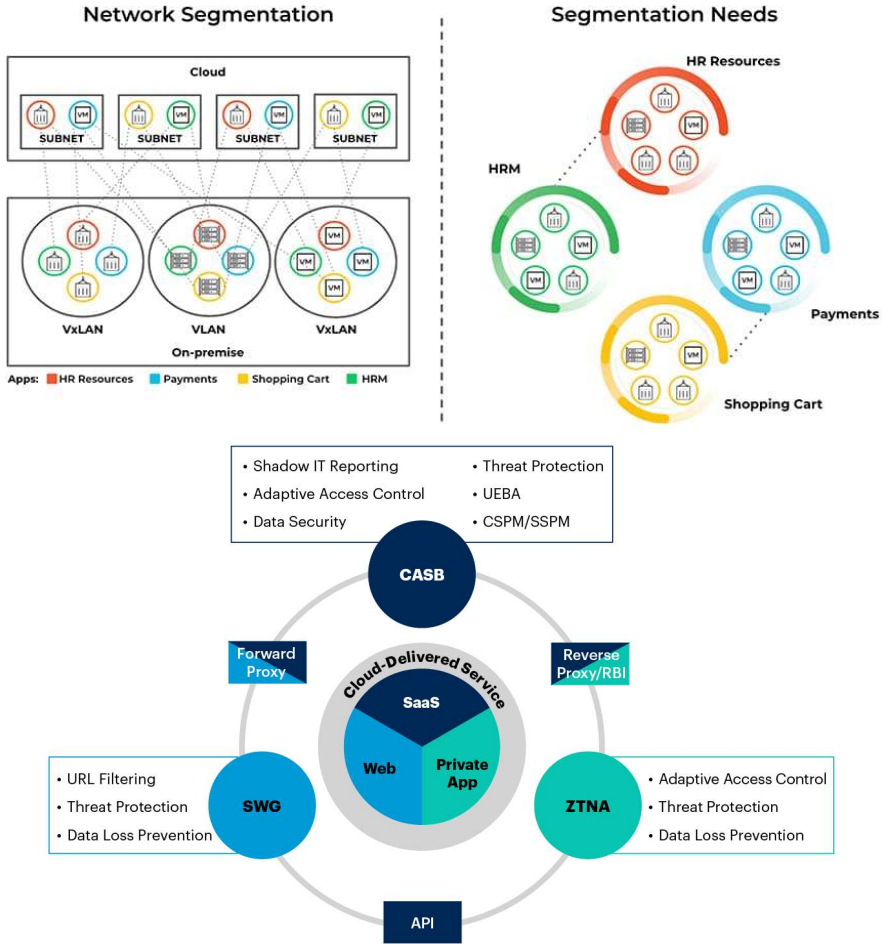
Device Pillar

- **Centralized Policy Management**
  - Move away from dependency on network devices for applying policy
  - Perform file analysis for data that must be stored on endpoints
- **Infrastructure as Code Deployments**
  - Repeatable structured deployments that must meet policy
  - Security review integrates into infrastructure pipeline
- **Posture Validation and Risk Based Access**
  - Must be authenticated, continuously monitored and verified for access



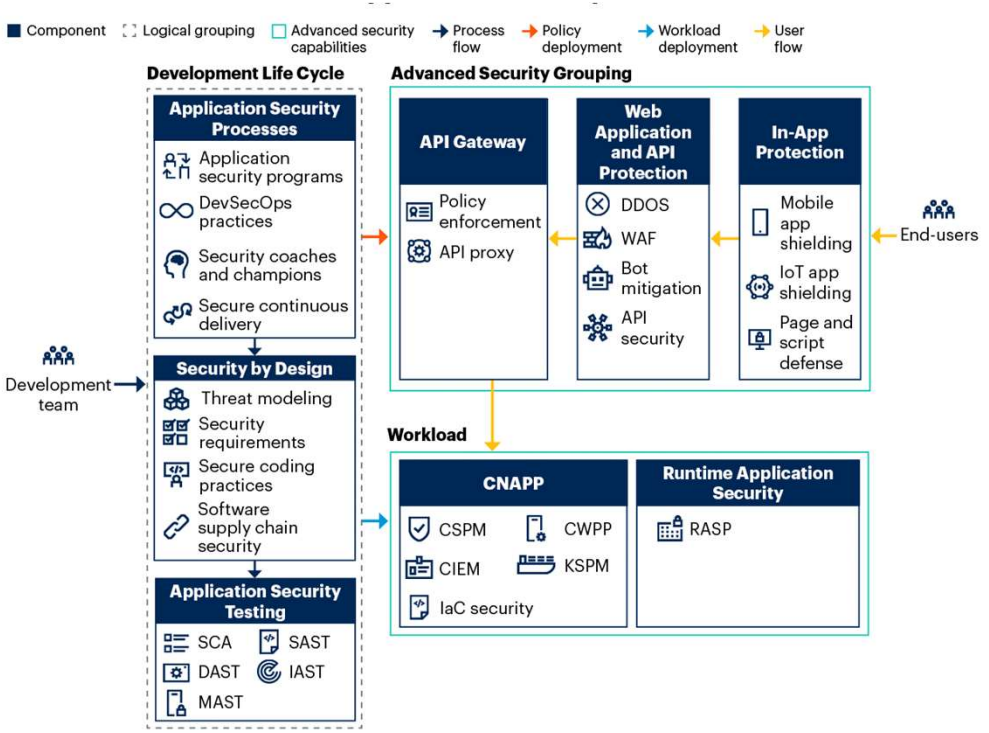
Network Pillar

- **Microsegmentation**
  - Only devices that need to talk to each other can reach each other
  - Each application resides in its own zone
- **Least Privilege**
  - Dynamically applied to network access requests
  - Verification prior to accessing resource
- **Network Traffic Analysis**
  - Provides insight into traffic patterns
  - Integrated anomaly detection



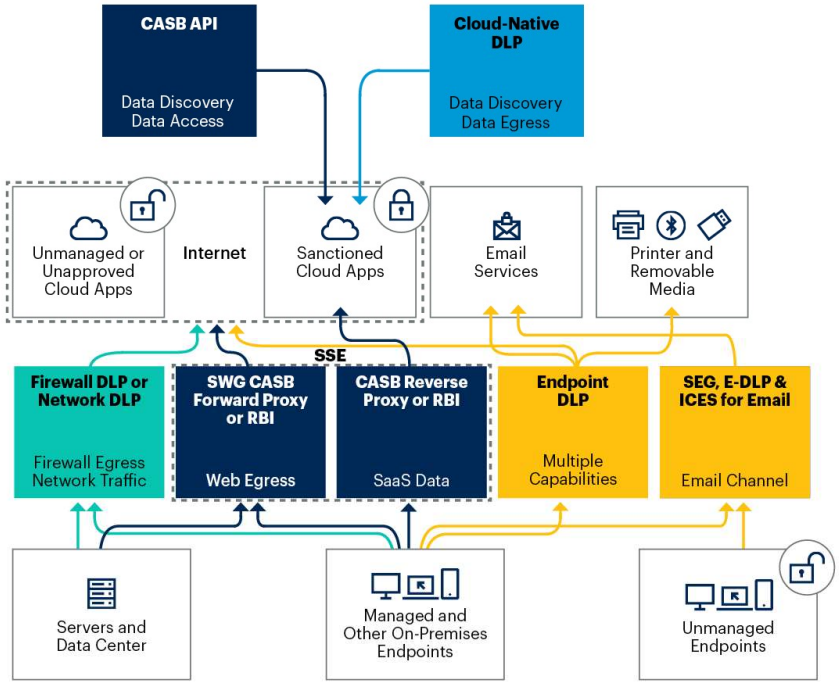
Application Workload Pillar

- **Application Development Security**
  - DevSecOps
  - Centralized key store (HSM)
  - Code and application review tools
- **API Security**
  - Policy management
  - Web application firewall
- **Workload Posture Analysis**
  - Privilege analysis
  - Access analysis



Data Pillar

- **Data Loss Prevention**
  - Provides organization policy controls for data management
  - Focuses on unauthorized sharing movement or leaking of targeted data
- **Data Detection and Response**
  - Monitors and responds to attempts at accessing unauthorized data access
  - Provides visibility into data threats and unauthorized access
- **Encryption**
  - Standardized secrets management
  - Key management infrastructure



Why Automation & Orchestration Matter

Reduce human error

Enable faster, consistent security architecture and responses

Integrate identity, device, network, application, and data protections

Support CI/CD and Infrastructure as Code (IaC) models

Aggregate results across monitoring tools

vita.virginia.gov