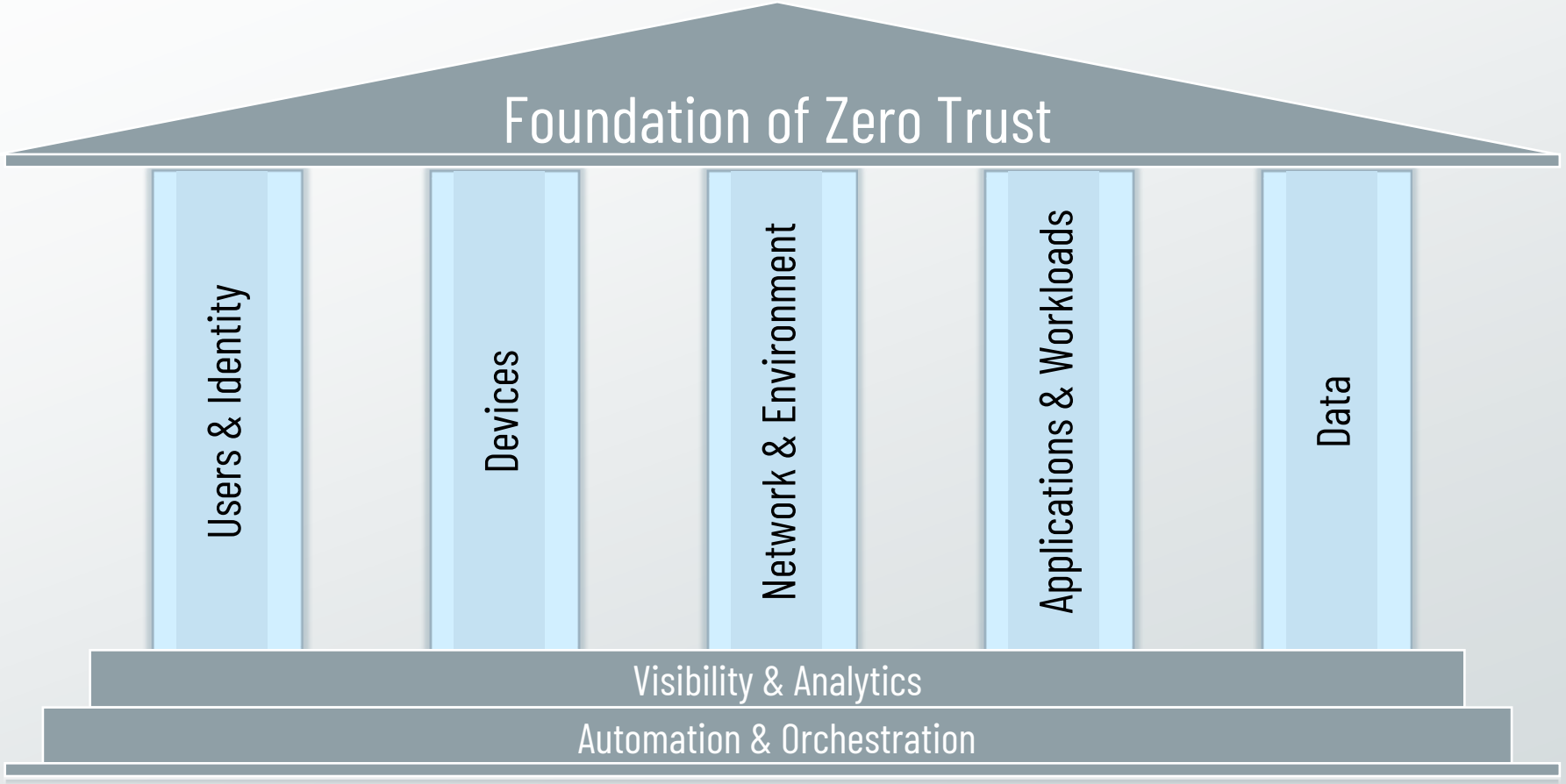
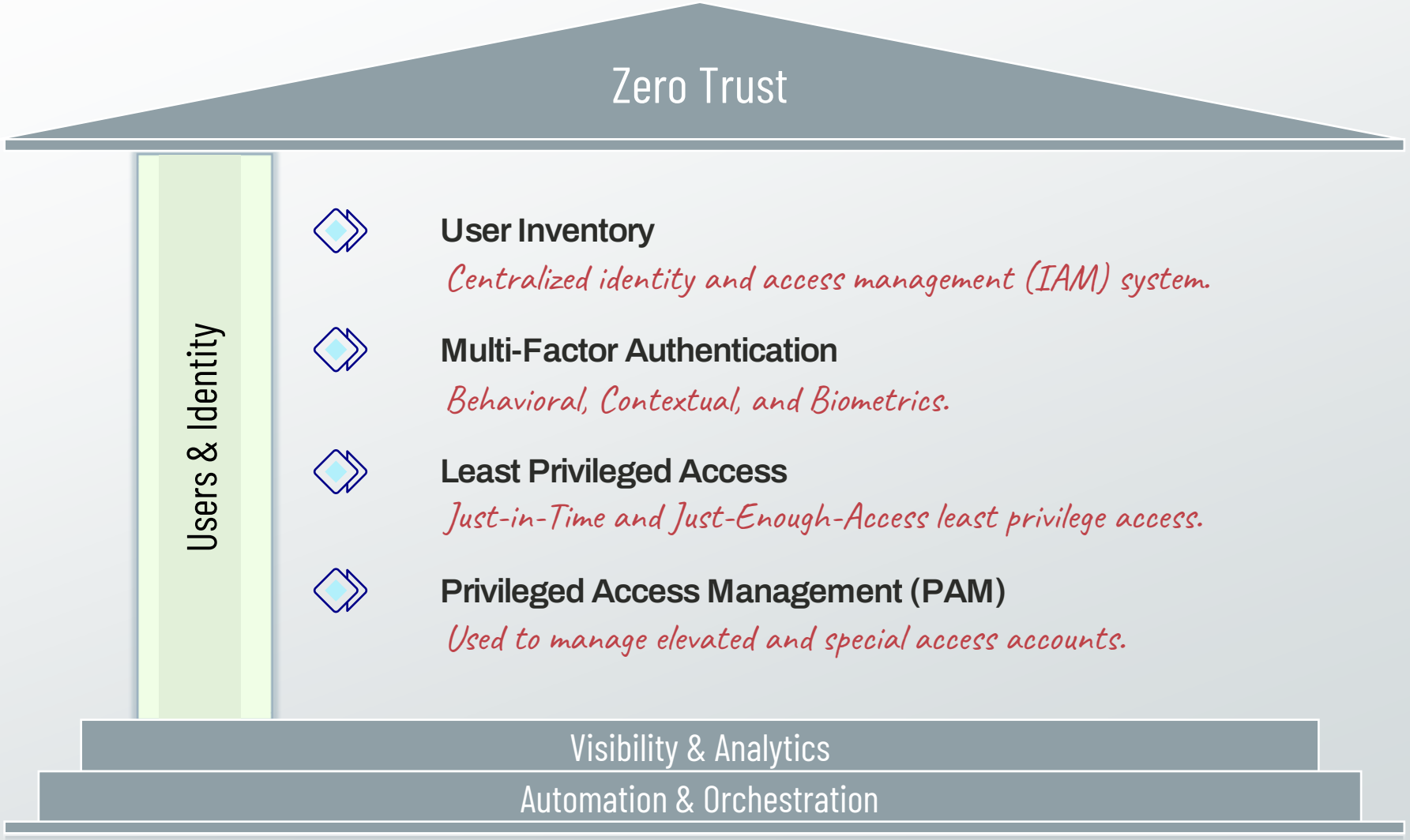
Zero Trust Architectural Pillars

Zero Trust Pillars



1. GSA and DoD Zero Trust Pillars

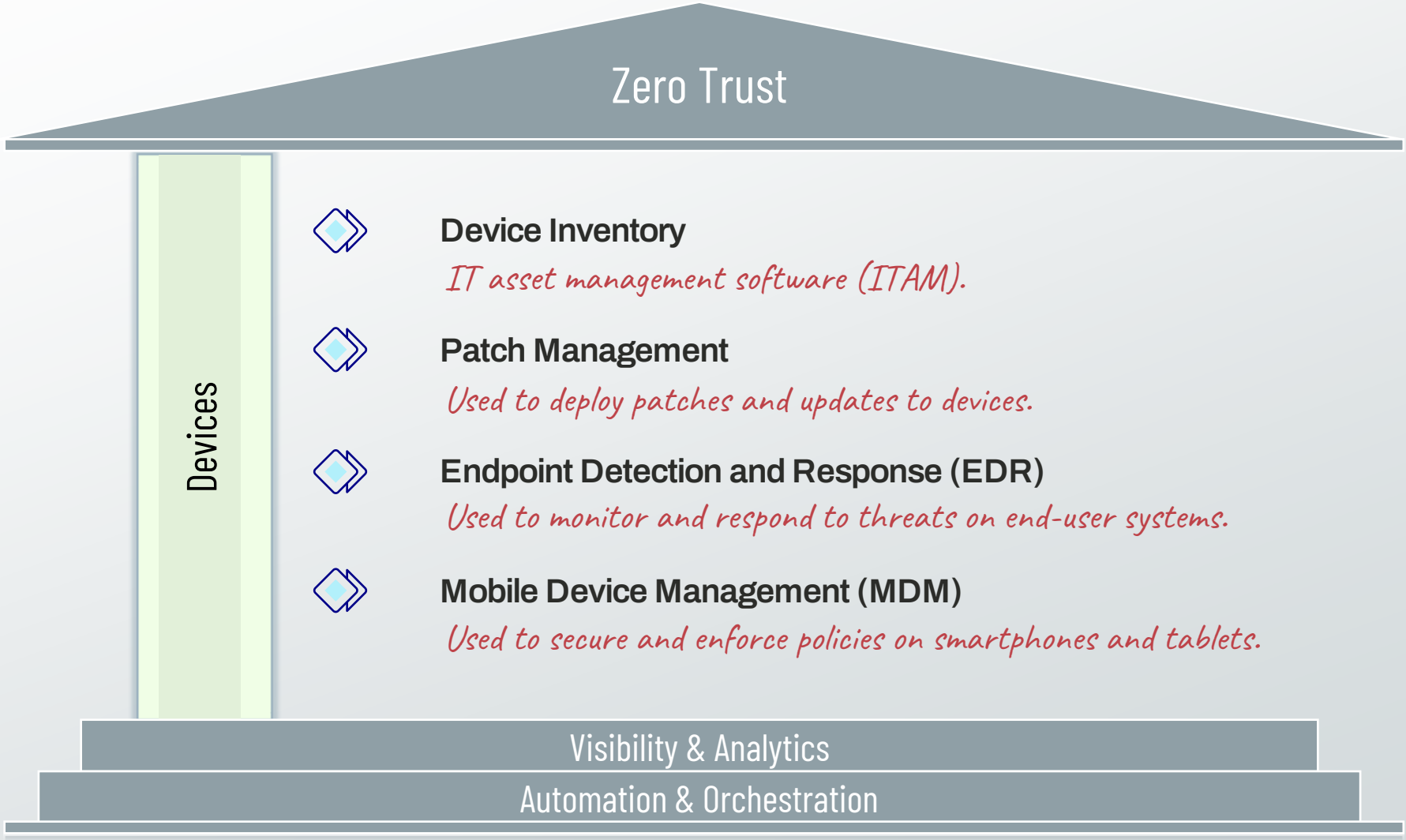
Securing the Users & Identity Pillar



The Users & Identity Pillar focuses on user identification, authentication, and access control policies using dynamic and contextual data analysis.

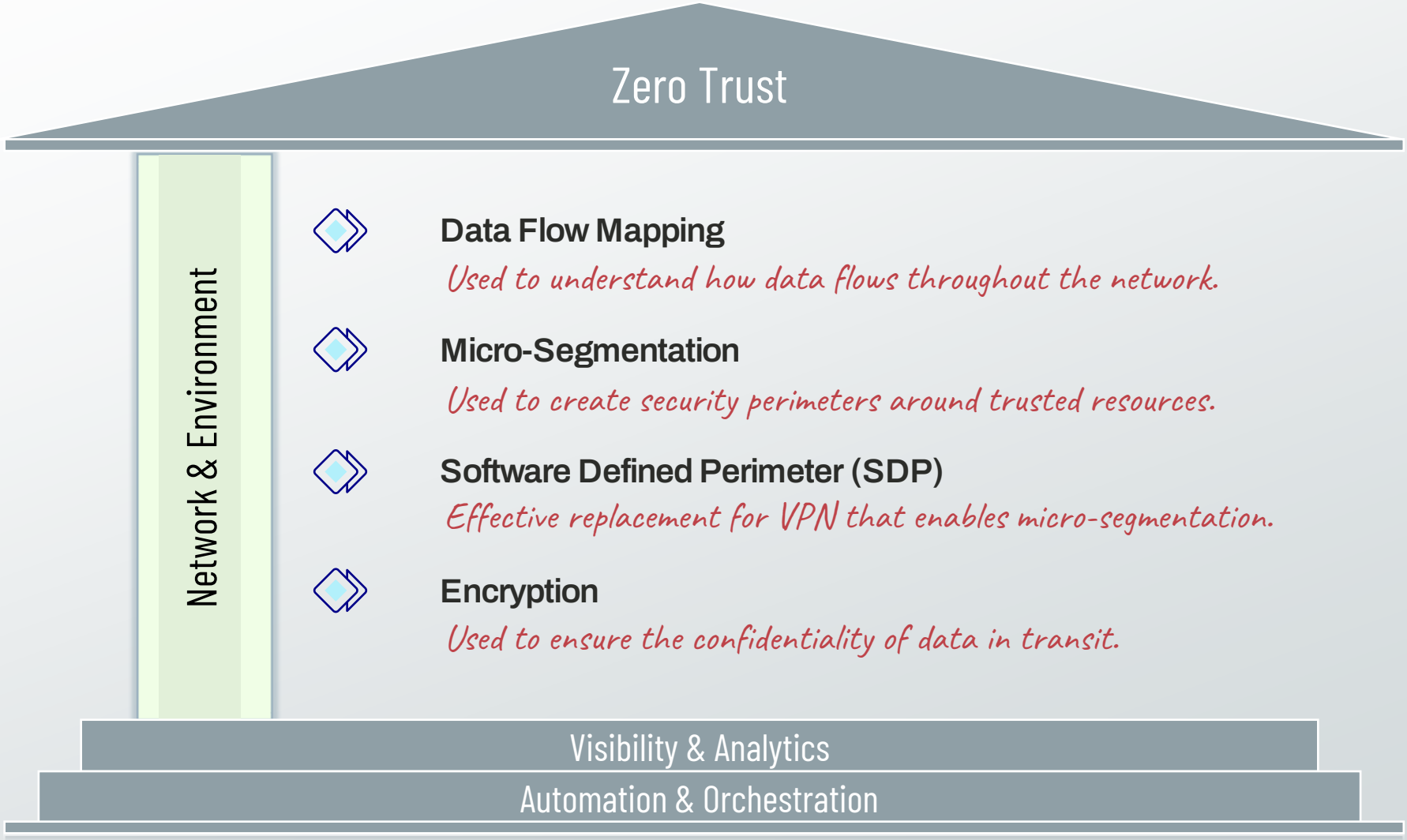
Securing the Devices Pillar

INSTRUCTOR
ALTON



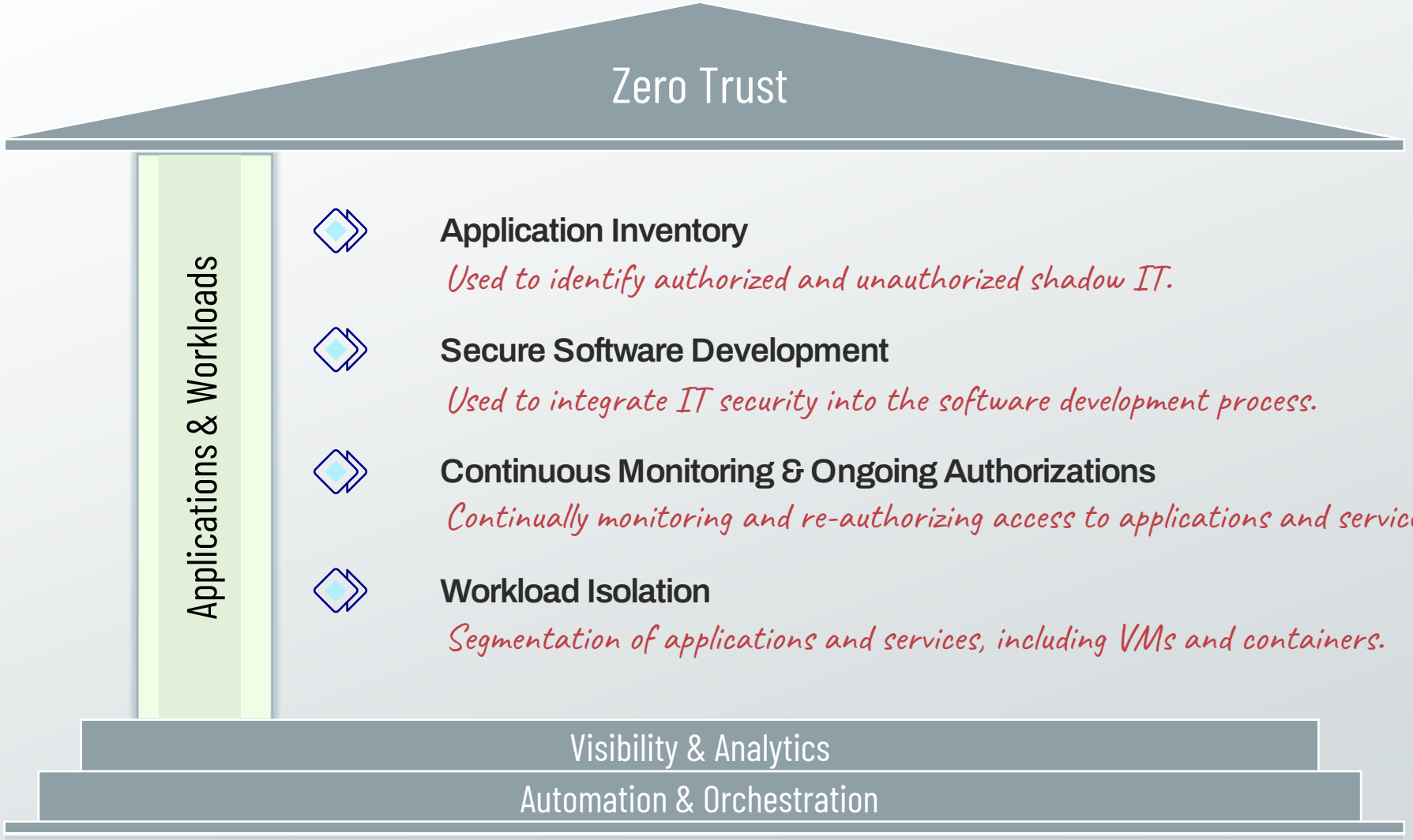
The Devices Pillar performs validation of user-controlled and autonomous devices to determine acceptable cybersecurity posture and trustworthiness.

Securing the Network & Environment Pillar



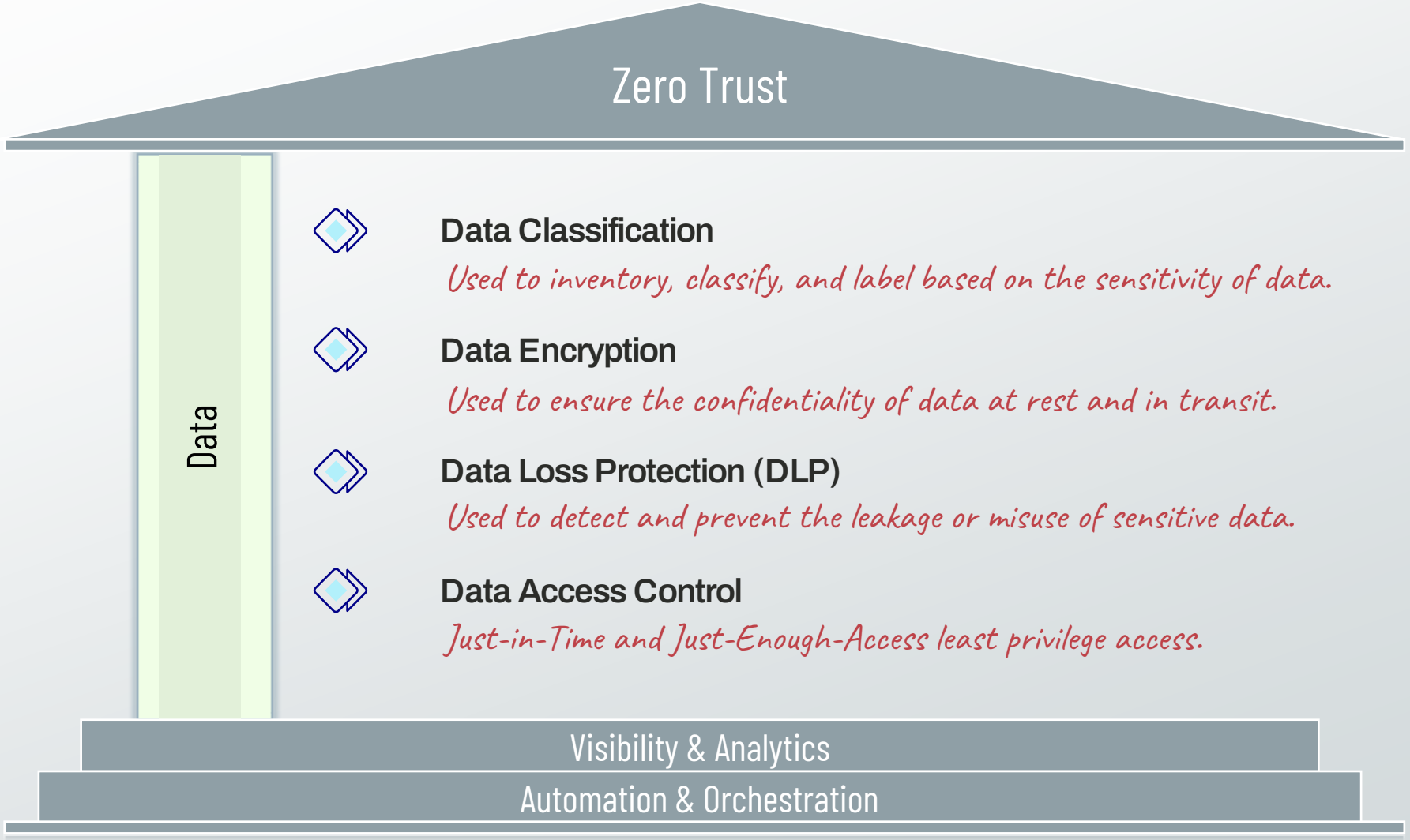
The Network & Environment Pillar segments, isolates, and controls the network environment with granular policy and access controls.

Securing the Applications & Workloads Pillar



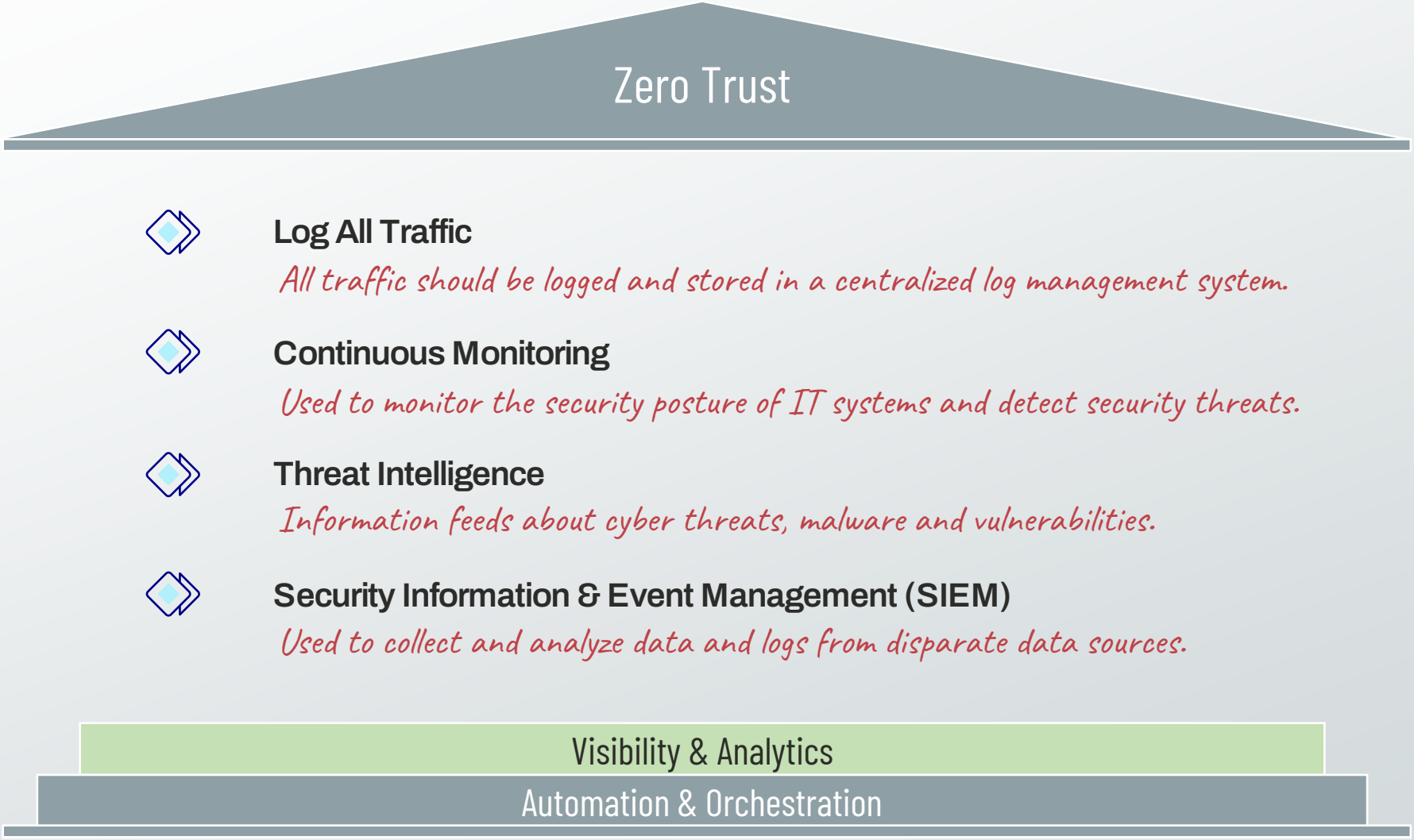
The Applications & Workloads Pillar secures everything from applications to hypervisors, including containers and virtual machines.

Securing the Data Pillar



The Data Pillar focuses on securing and enforcing access to data based on an data's categorization and classification to isolate the data from everyone except those that need access.

Foundational Components



Log All Traffic

All traffic should be logged and stored in a centralized log management system.

Continuous Monitoring

Used to monitor the security posture of IT systems and detect security threats.

Threat Intelligence

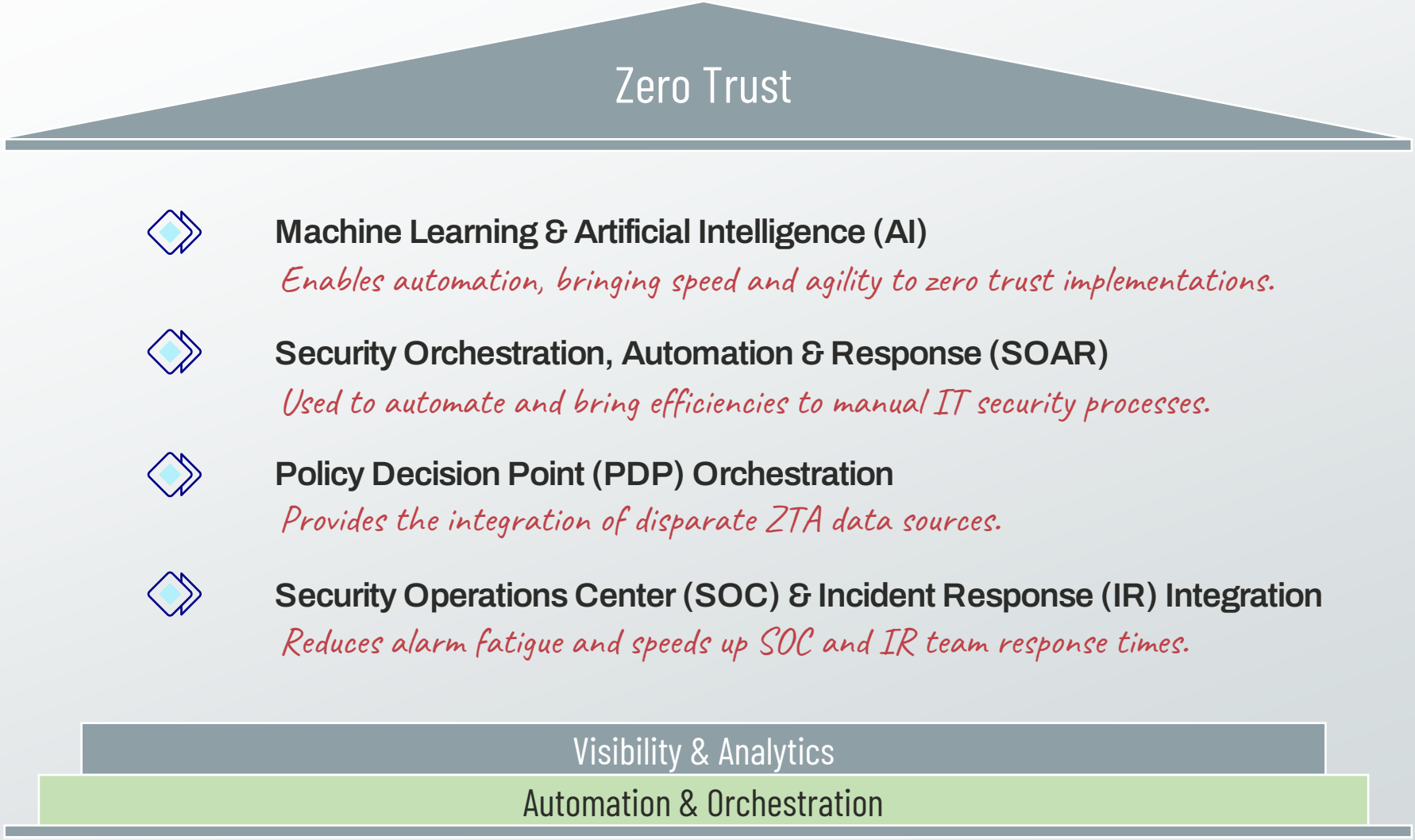
Information feeds about cyber threats, malware and vulnerabilities.

Security Information & Event Management (SIEM)

Used to collect and analyze data and logs from disparate data sources.

Visibility & Analytics provide insight into user and system behavior by observing real-time communications between all Zero Trust components.

Foundational Components



- **Machine Learning & Artificial Intelligence (AI)**
  Enables automation, bringing speed and agility to zero trust implementations.
- **Security Orchestration, Automation & Response (SOAR)**
  Used to automate and bring efficiencies to manual IT security processes.
- **Policy Decision Point (PDP) Orchestration**
  Provides the integration of disparate ZTA data sources.
- **Security Operations Center (SOC) & Incident Response (IR) Integration**
  Reduces alarm fatigue and speeds up SOC and IR team response times.

Automation & Orchestration automates security and network operational processes across the ZTA by orchestrating functions between similar and disparate security systems and applications.

Bringing It All Together