Cisco Zero Trust

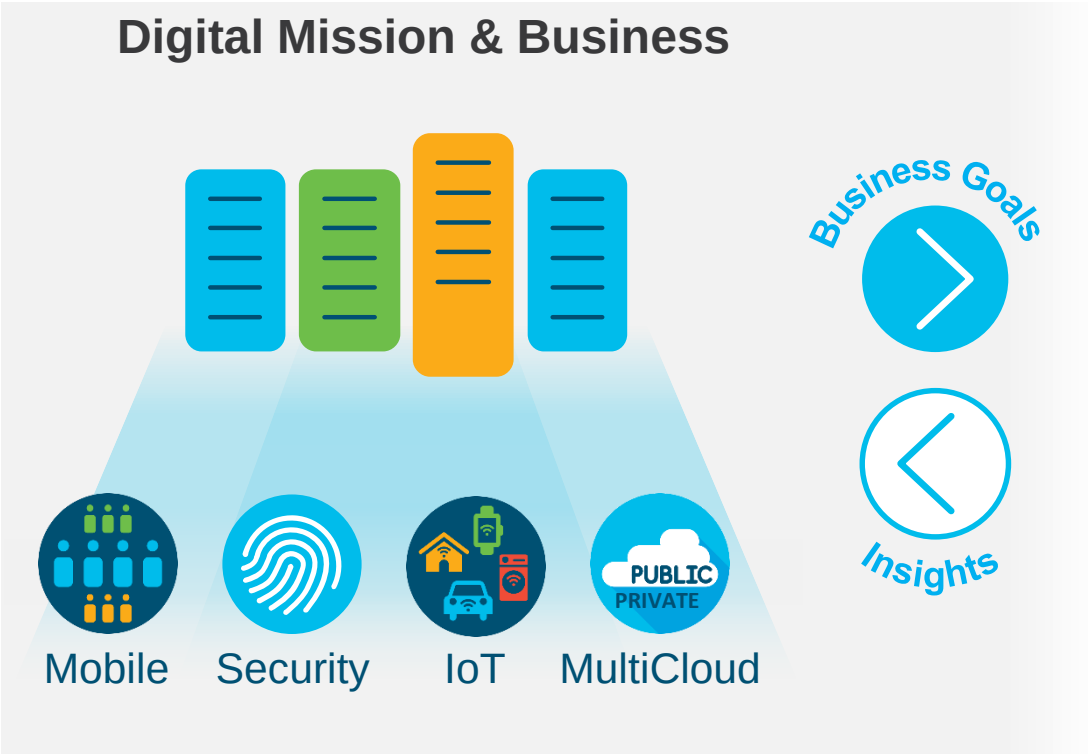
Moving to a Zero Trust World

Steve Vetter and Theodore Gates
Federal Strategist and Services Consultant
November 2019

Key Networking and Security Factors

- **Performance**
- **Scale**
- **Security**
- **Performance at Scale with Security**
  - **The Means:** Visibility / Automation / Intent-Based Networking / AI-ML
    - **SD-WAN / SDA and DNA-C / ACI** --- Cross-Domain Network Integration
    - **Switches** as Network Sensors / Policy Enforcers and Scale Enablers
  - **The Benefits:** Above / Network & Tool Consolidation / Zero Trust

Intent-Based Networking (IBN)



Network

Translation & Validation

Captures business intent, translates to policies, and check integrity

- **The "what" to the "how"**

Activation & Awareness

Orchestrate policies & configures systems automatically

- **Automates the "how"**
- **Real time network status**

Dynamic Assurance

Continuous verification, visibility & corrective / proactive actions

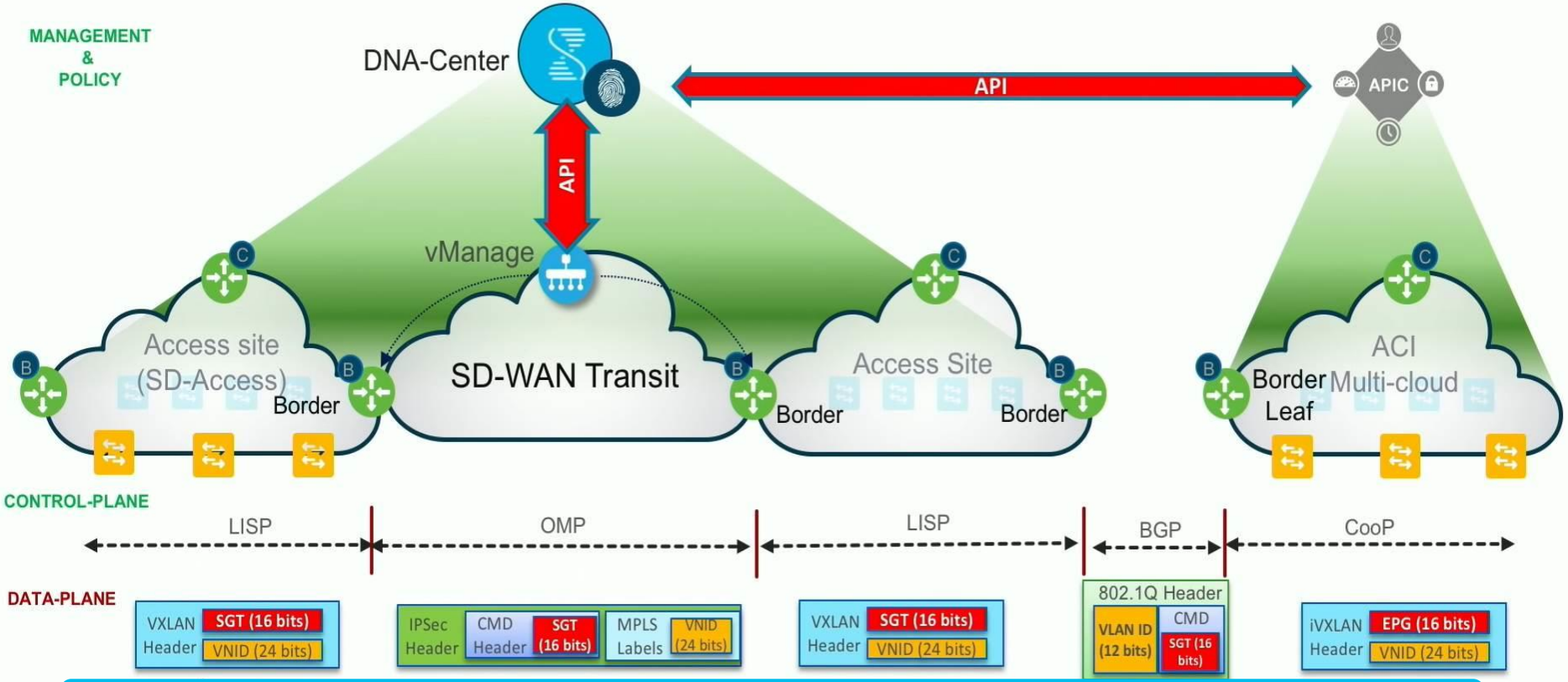
- **The "how" is doing the "what"**

Comprehensive visibility is essential – for both IBN and Security

Cross-Domain Networking Today – single policies!

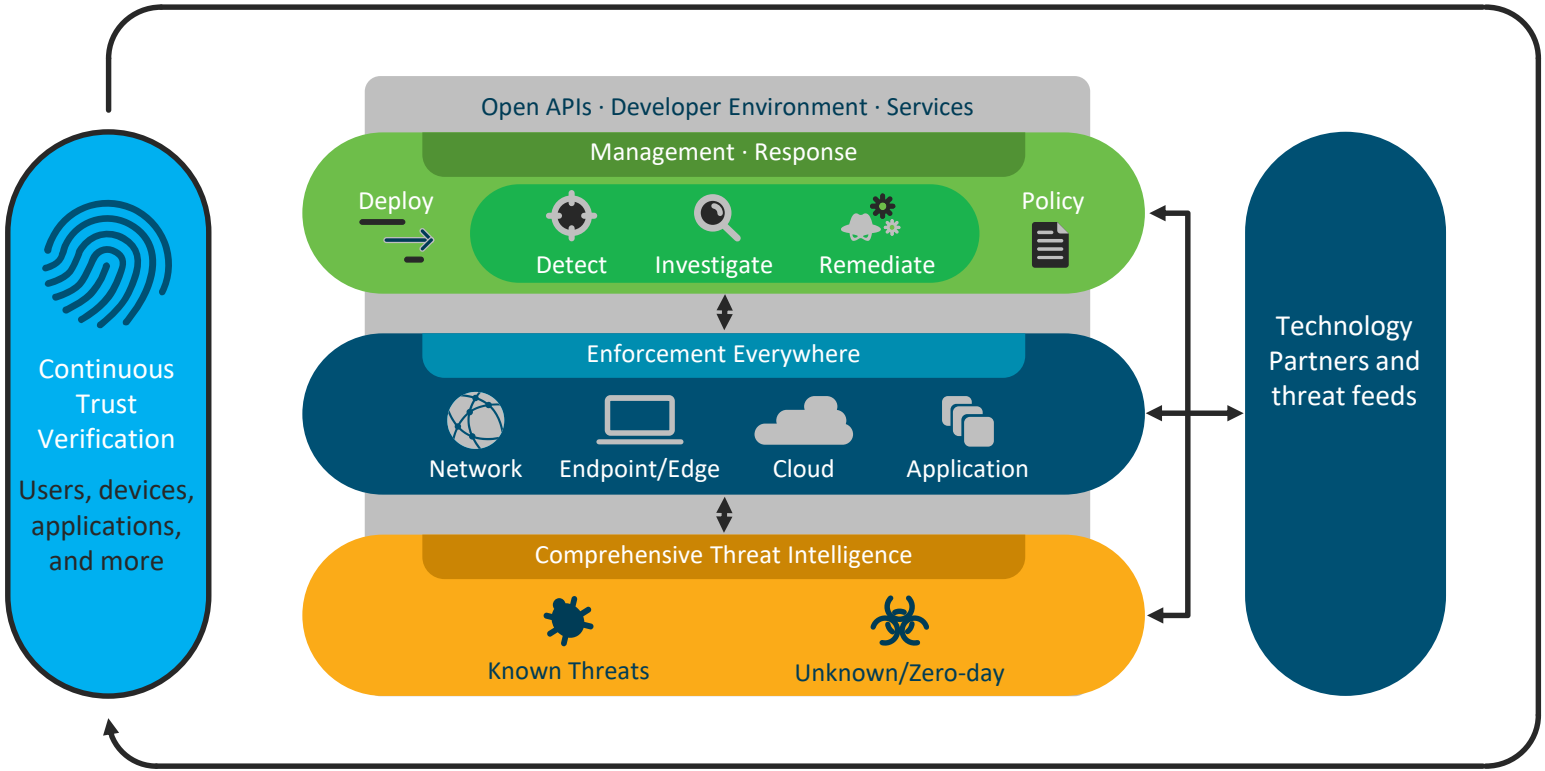
SDA – DNA-C / SD-WAN

Data Center / Cloud



Enables Granular End-to-End Segmentation Today!

Modern Security Architecture

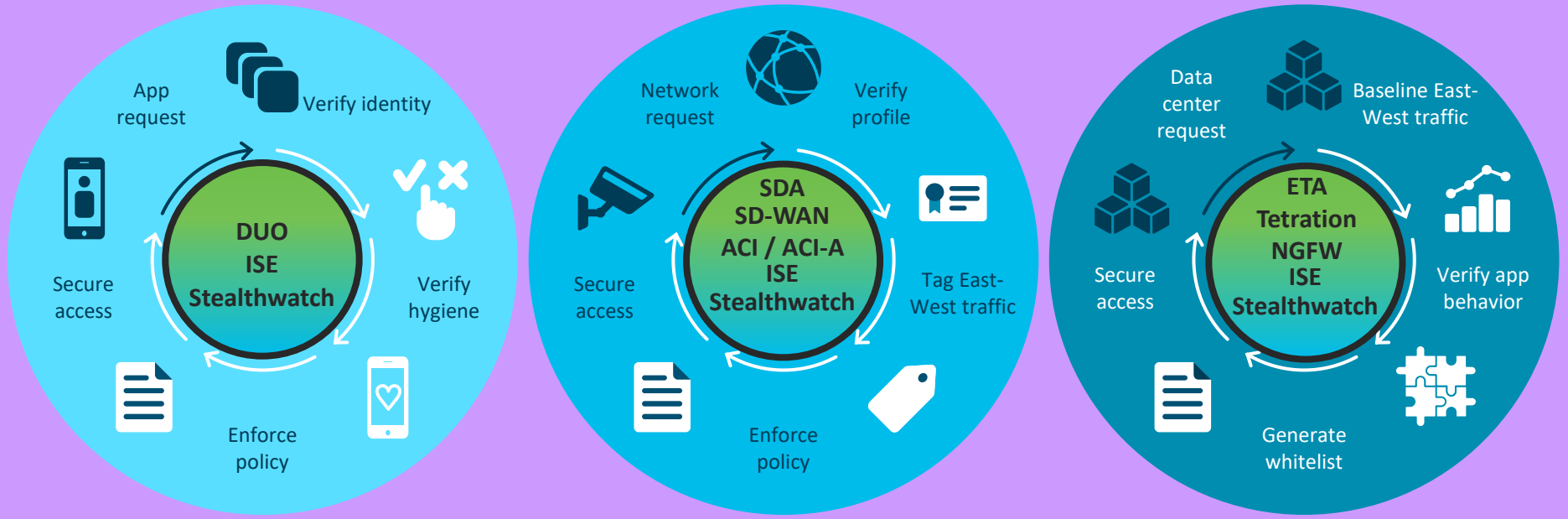


Cisco Zero Trust Recommendations

Trusted Workforce
User and Device Access

Trusted Workplace
IoT, Edge and Sensor Access

Trusted Workloads
App and Data Access



Cisco Talos…for Threat Intelligence and proactive threat defense

An open, scalable foundation supporting all frameworks with multi-vendor tool integration

- Comprehensive, integrated, interoperability (i.e., SIEM, SOAR, MDM, Threat, SDA, etc.)
- Integrated threat defense
- Granular microsegmentation enforcement

NIST Zero Trust Logical Components

From NIST SP 800-207 Draft

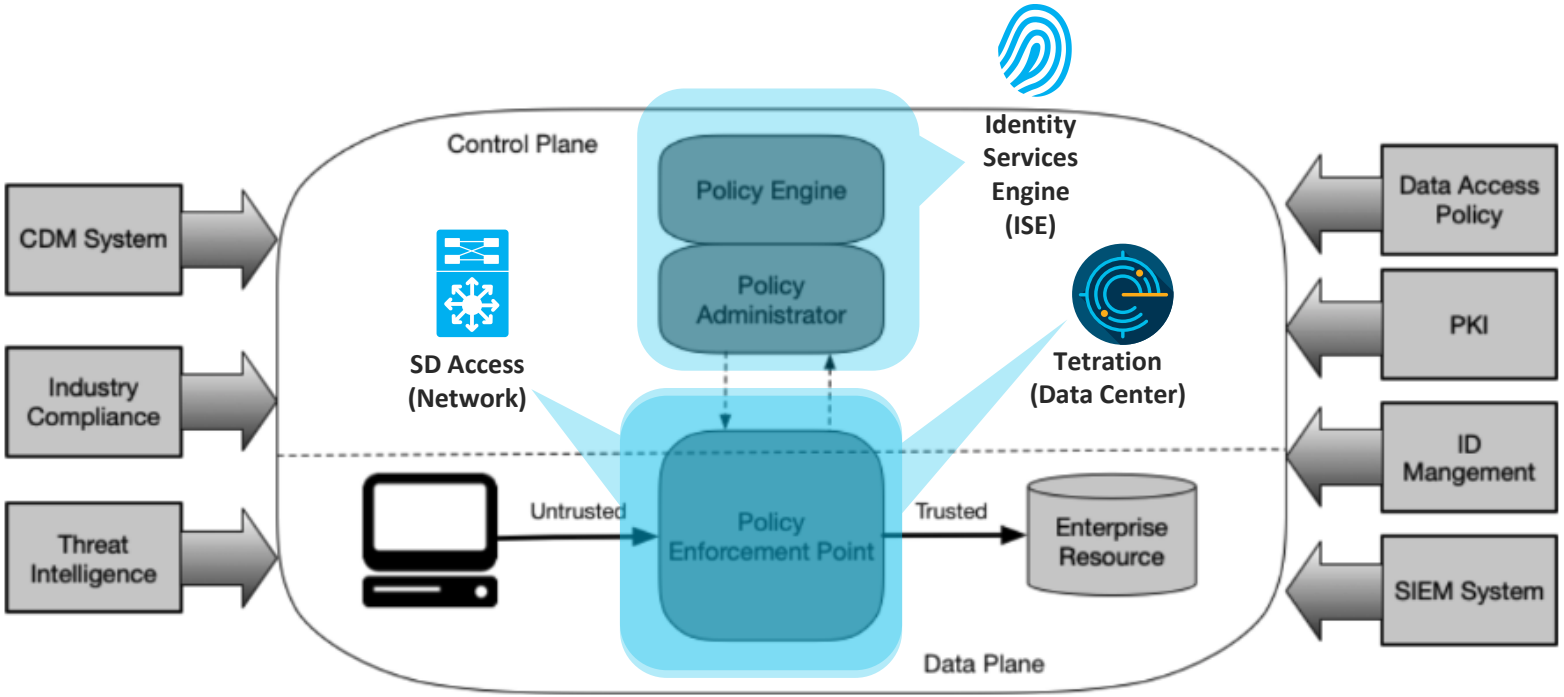


Figure 2: Core Zero Trust Logical Components

Zero Trust architectural approach
A journey with granular-enforcement based on context

Establish Trust Level

Establish SD-Perimeter

Manage Risk Level

1 User-Device Trust

2 IoT Trust — AND/OR — Workload Trust

Inventory · Assess
Authenticate · Authorize

3 Network Access

4 App and Data Access

Authorized SD-Access
Micro-Segmentation

5 Context/Anomalies Determine “Normal”

6 Threat Response

Continuous Detection and Verification

Shift from macro - binary to micro - contextual

Cisco's Zero Trust Perspective

- **ZT Architectural Keys:**
  - Holistic – end-to-end – comprehensive visibility - AI/ML driven
- **Knowledge Gaps? Already being addressed…**
  - Attacker response
  - Network resiliency – integrated IBN
  - User experience / network availability
  - Interface API Standards and standardization
  - Privacy – "decrypting as much as possible"
- **Bottom Line:**

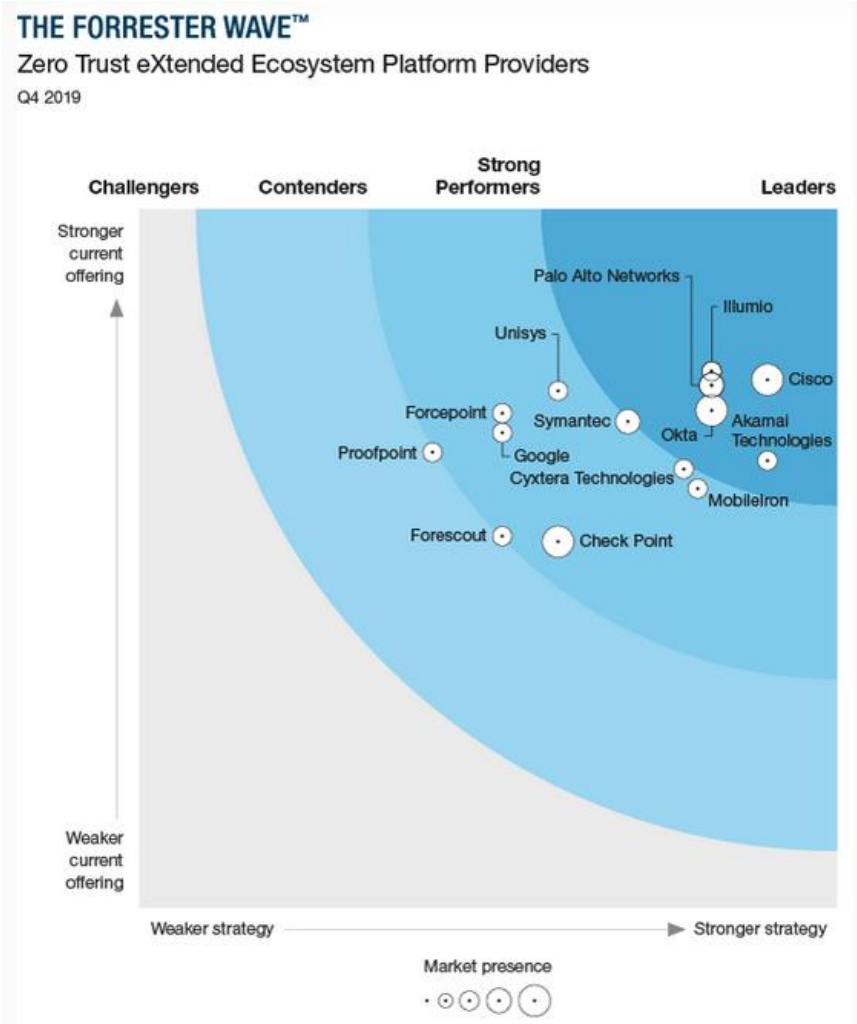
  Zero Trust is really about trusted access to applications and data

AI/ML is a technological game-changer

Zero Trust
– The Latest Rankings…

Cisco excels in Zero Trust, with a renewed and targeted focus. Cisco has been a powerhouse in the networking space for decades, and after a few years of deprioritizing security, it's come roaring back into the sector with Zero Trust as its driving initiative. The company spent significant time and expense to realign much of its security portfolio to enable or enhance Zero Trust for its customers. Cisco has spent the past year working to integrate and operationalize the authentication technology from its acquisition of Duo. The integration of Duo's strong authentication offering and the simplicity of its UIs and tooling have strengthened the Cisco offering considerably.

The interoperability and use for the Duo integration, combined with the other component offerings from Cisco's WWW (Workforce, Workload, and Workplace) approach to Zero Trust, are closely mapped to the ZTX ecosystem. The combination of Cisco's networking and device tooling, new offerings for analytics and cloud workloads, and duo's focus on users and endpoints supports multiple components of ZTX. deployment and ease of use are strengths across the portfolio. Cisco has adopted a Zero Trust strategy and is well positioned as a prominent Zero Trust player.



Zero Trust - Key Constructs - Cisco Perspectives

- **Zero Trust is not a bolt-on security product – must be designed into the full network life cycle**
  - Essential with impending devices / sensors / data explosion – customer experience focus
- **No implicit trust**
  - Must authenticate before being allowed to connect to the network
  - Assume all traffic, regardless of location, is a potential threat – use risk to prioritize actions
- **Provide total visibility, analytics and proactive response across the entire environment**
  - Continuously monitor/inspect/log all traffic, assess threat and automate responses
  - Detect and respond to anomalous activity in real-time
  - Ensure predictive quality of experience analytics to enhance user and mission outcomes
- **Ensure granular network segmentation by user, device and application (down to Layer 2)**
- **Focus on: Security AND Privacy AND Availability**
- **Automation is essential for enterprise management**
- **Open, extensible platforms that integrate with existing investments**
- **Optimize risk management for mission outcomes through real-time response to dynamic threats**


CISCO