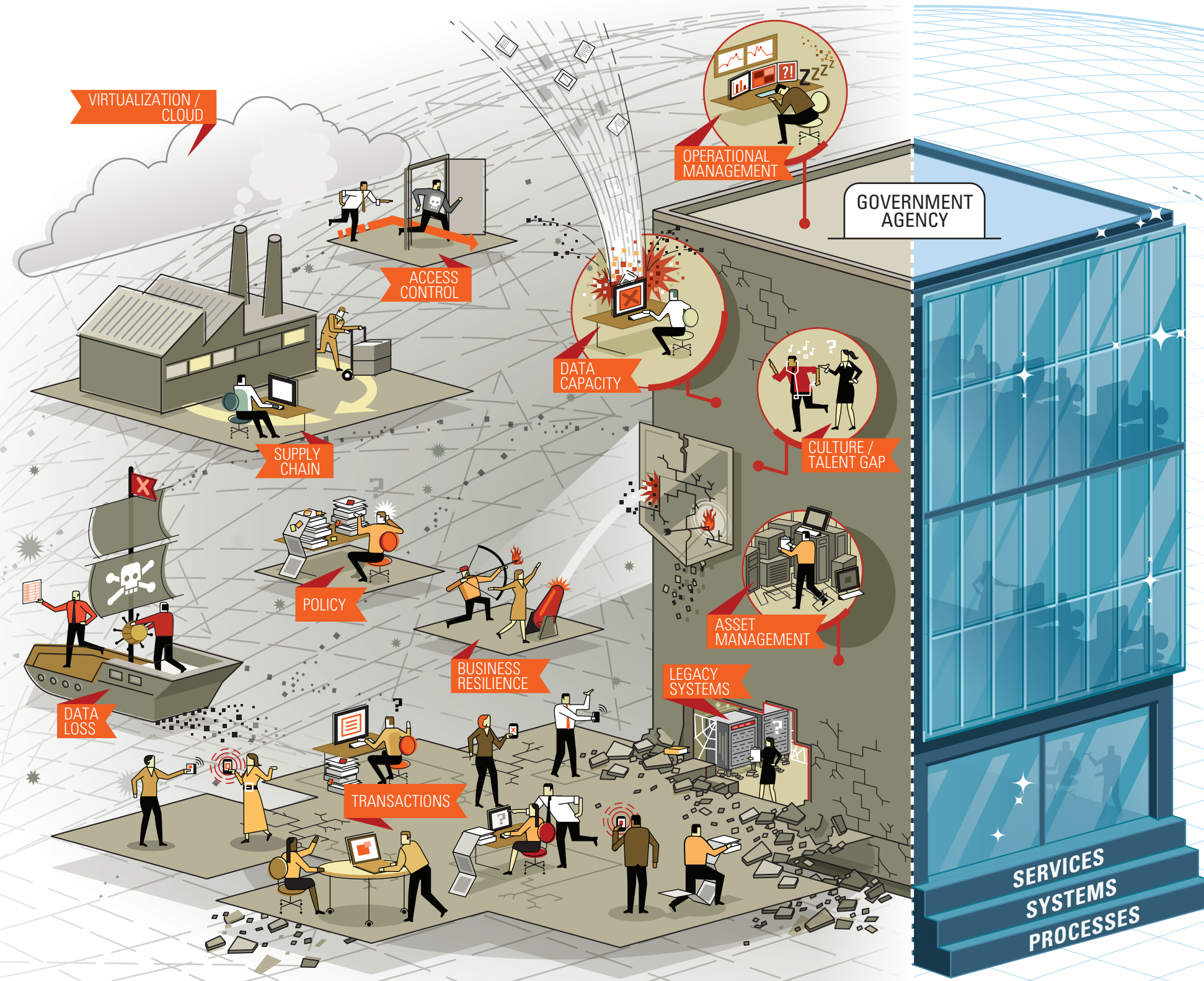


# CYBERSECURITY

TRUST, VISIBILITY, RESILIENCE

In today's dynamic threat landscape, maintaining business resilience while mitigating security risk is a challenge that all government entities face. Partnering with Cisco helps governments travel down the path to secure information and a secure network infrastructure.

No other company delivers the coordination of knowledge, tools and resources, or provides the global visibility and insight that Cisco does. The cybersecurity challenge is complex and pervasive. Don't attack it without Cisco.



## TRUST IDENTIFY AND MANAGE

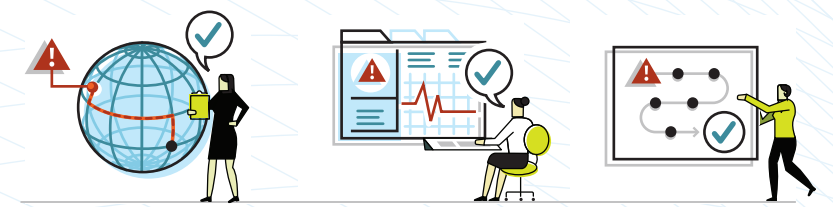


**ASSET DISCOVERY & MANAGEMENT**  
Validating user and device identity at the system's point of entry and maintaining a state of trust.

**CONFIGURATION MANAGEMENT & REMEDIATION**  
Identifying vulnerabilities and misconfigurations, and following this with corrective action to ensure policy compliance and risk reduction.

**ARCHITECTURAL OPTIMIZATION**  
Network design and feature application, combined with best practices to create a threat-resistant and risk-tolerant infrastructure.

## VISIBILITY PREVENT AND DETECT

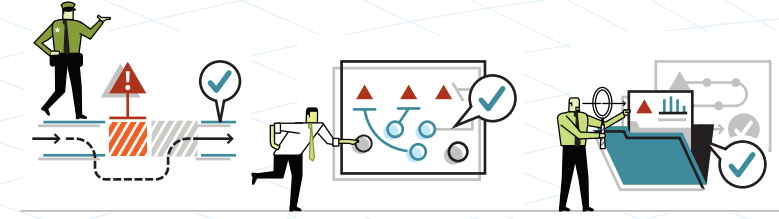


**GLOBAL THREAT ANALYSIS**  
Cisco's global sensor network collects and analyzes threat information that customers can use to reduce the risk of network compromise.

**NETWORK INTELLIGENCE**  
Using the intelligence inherent in Cisco technology to remove uncertainty and understand network behavior.

**SITUATIONAL AWARENESS**  
Providing a systematic approach to support enterprise security decisions.

## RESILIENCE RESPOND AND RECOVER



**POSITIVE NETWORK CONTROL**  
Controlling traffic and maintaining business operations during a cyber attack.

**THREAT MITIGATION**  
Using the network's agility and defense resources to limit the consequences of a threat, attack, or breach.

**INCIDENT HANDLING & FORENSICS**  
Compiling post-incident data for assessment and policy compliance.