Cisco SecureX Architecture

What Is the Value of the Cisco SecureX Architecture?

The Cisco SecureX Architecture™ is a context-aware, network-centric approach to security that enables:

- Greater alignment of security policies with business needs
- Integrated global intelligence
- Simplified security delivery
- Consistent security enforcement throughout the organization

The result is automated security enforcement, from the endpoint to the cloud, that is seamless to the end user and more efficient for the IT organization.

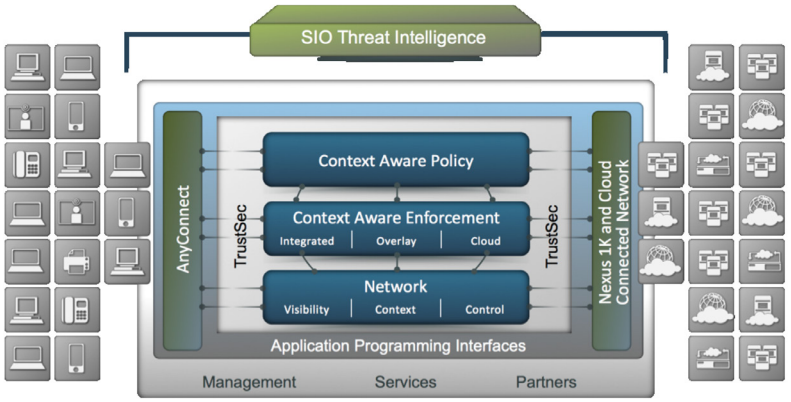
What Problems Does the Cisco SecureX Architecture Help Solve?

The Cisco SecureX Architecture enables organizations to embrace the new network security landscape while protecting their business assets, critical services, and employees. While increased mobility, the influx of consumer devices, and movement of information to the cloud has created tremendous opportunities for organizations, it has also created complexities for securing the IT infrastructure.Deploying piecemeal security solutions can lead to duplicated efforts and inconsistent access policies, and requires increased integration and staffing to support. And with the increasing sophistication and targeting of network attacks, it's more important than ever to have a comprehensive security solution.

How Does the Cisco SecureX Architecture Work?

The Cisco SecureX Architecture blends the power of the Cisco network with context-aware security to protect today's organization no matter when, where, or how the network is used. The architecture is built upon three foundational principles:

- **Context-aware policy** uses a simplified descriptive business language to define security policies based on five parameters: the person's identity, the application in use, the type of device being used for access, and the location and time of access. These security policies more closely align with business policies and are simpler to administer across an organization. They help businesses provide more effective security and meet compliance objectives with greater operational efficiency and control.
- **Context-aware security enforcement** uses network and global intelligence to make enforcement decisions across the network and to deliver consistent and pervasive security anywhere in the organization. Flexible deployment options, such as integrated security services, standalone appliances, or cloud-based security services bring protection closer to the user, reducing network load and increasing protection.



- **Network and global intelligence** provides deep insight into network activity and the global threat landscape for fast, accurate, and granular protection and policy enforcement:
  - Local intelligence from the Cisco network infrastructure takes context such as identity, device, posture, location, and behavior to enforce access and data integrity policies.
  - Global intelligence from Cisco Security Intelligence Operations (SIO) provides full, up-to-date threat context and behavior to enable real-time, accurate protection.

What Are the Benefits?

The Cisco SecureX Architecture:

- Enables organizations to embrace mobility and cloud technology while protecting critical business assets
- Delivers granular visibility and control, down to the user and device level, across the entire organization
- Provides faster, more accurate protection from threats with always-on security and integrated global intelligence
- Increases operational efficiency with simplified policies, integrated security options, and automatic security enforcement
- Provides full security coverage with the industry's most comprehensive security solutions and services

For more information on the Cisco SecureX Architecture and Cisco security solutions, visit www.cisco.com/go/securex and www.cisco.com/go/security.

C45-680225-00 7/11