Intent-Based Network Security

Continuous visibility

Zero-trust access

Constant protection

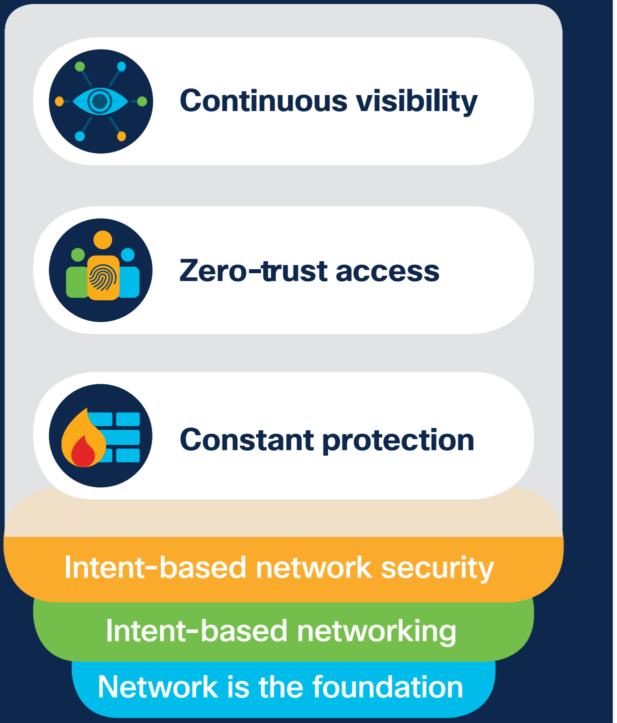
Security built IN, not ON, the intelligent network

A NetOps team empowered with an intelligent network provides a powerful ally to SecOps in the ongoing fight to keep the organization and its data safe. Intent-based network security is how we refer to this convergence of the network and security. It enables IT to enlist the network to automatically and effectively determine what's new, what's important, and what's unusual, regardless of where across the distributed network it exists. It's the process of applying machine learning and analytics to the information generated by the network, users, devices, and applications automatically to confirm the intended behavior. Ultimately this reduces the time to detection and expedites the remediation of threats.

An intent-based network powered by Cisco DNA Center and Cisco DNA software can provide continuous visibility into who and what is on the network, contributing to a complete zero-trust access security model and building threat prevention, detection, and response in, not on, the network fabric for constant protection.

With Cisco DNA Center and its streamlined security integrations, you can:

- **Enable automated access policies** to secure any user, any device, any app, anywhere
- **Stop propagation of data breaches** using dynamic context, not location, for segmentation
- **Ensure fast compliance** by applying security to thousands of locations from one interface
- **Streamline visibility** to the SOC for reduced time to threat detection
- **Automate threat responses from the SOC** to remediate incidents in less time



Continuous visibility

Zero-trust access

Constant protection

Intent-based network security

Intent-based networking

Network is the foundation

Continuous visibility

A full view of our fast-changing mobile-first and cloud-first IT environments is critical to fill the gaps in our traditional perimeter and endpoint-based security solutions. Visibility begins with classifying who and what is on the distributed network. Where personally owned mobile devices, rogue wireless access points, or undocumented cameras are connected. How user or IoT devices converse with services or applications. When application workloads send data to other workloads.

Gaining a baseline understanding of all network communications – even in the cloud – provides a full inventory that a group-based policy can be built around. Cisco DNA Center can help monitor unusual behavior that could represent a threat or policy violation. And the machine learning available in our group-based policy is critical to better classify all types of devices or workloads and more quickly identify anomalies from the baseline.

Zero-trust access

A zero-trust security model provides NetOps teams the ability to secure access regardless of where it originates and minimizes the attack surface. Building on visibility, NetOps can contextually group all users, devices or things, and applications. Then, it can logically segment them throughout the wired and wireless infrastructure to secure the workplace.

As traffic traverses the WAN, a whitelist policy follows applications from the data center to multiple clouds such that micro-segmentation secures your workloads.

And it always verifies trust, such that when any user (employee, contractor, third party) logs into any on-premises or cloud application, notably VPN or email, they must verify their identity with Multifactor Authentication (MFA), which mitigates the risk of stolen passwords. A posture assessment of any device (PC, mobile, personal) runs in the background during MFA to verify device trust, which mitigates the risk of exploitable vulnerabilities.

Constant protection

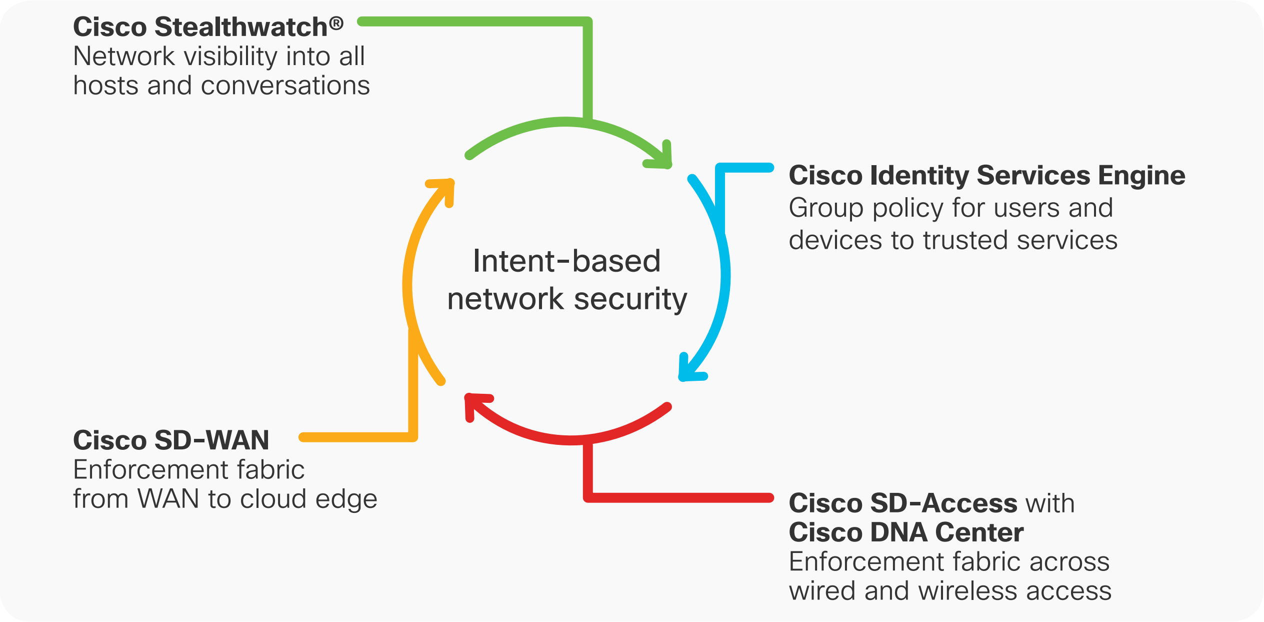
Network transformations, including Cisco SD-WAN and Cisco SD-Access, have resulted in a distributed microperimeter environment requiring security controls in hundreds to thousands of locations. Only by building threat prevention, detection, and response into every network device—from the WAN edge to the campus core—can both NetOps and SecOps be effective.

Not only must these controls be powered by effective threat intelligence to prevent at least 99% of the risk, they must also have effective machine learning algorithms to detect the stealthiest 1% of threats that are still unknown or encrypted. And an open, scalable architecture to push access policy changes from the branch to the data center to rapidly contain threats.

Learn more

Find more details about Cisco Security Solutions that integrate with the Cisco Digital Network Architecture (Cisco DNA):

- Enterprise Network Security – Secure your SD-WAN and campus and branch office networks with routing, switching, and wireless built-in security features
- Cisco Stealthwatch – Detect and respond to emerging threats in your digital business with industry-leading machine learning and behavioral modeling
- Cisco Umbrella™ – Get flexible, fast, and effective cloud security so you can secure your users, even in a matter of minutes
- Cisco Identity Services Engine (ISE)– Enable a dynamic and automated approach to policy enforcement
- Cisco ASA Firewalls – Apply consistent policy to simplify security management across distributed and hybrid networks
- Cisco® Catalyst® 9100 Access Points – Support spectrum analysis for enhanced aWIPS using custom ASICs in these newest Cisco access points



Cisco Stealthwatch®
Network visibility into all hosts and conversations

Cisco Identity Services Engine
Group policy for users and devices to trusted services

Intent-based network security

Cisco SD-WAN
Enforcement fabric from WAN to cloud edge

Cisco SD-Access with **Cisco DNA Center**
Enforcement fabric across wired and wireless access