Cisco's Intent Based Network Security (IBNS)

Continuous Visibility

Zero-Trust Access

Constant Protection

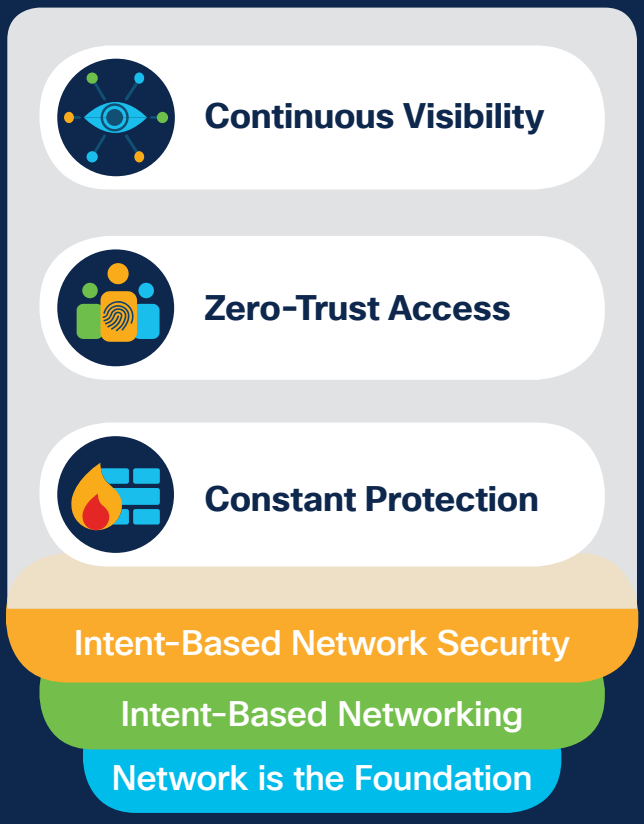
Security built IN, not ON, the intelligent network

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 (IBNS) is how we refer to this convergence of the network and security. IBNS 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.

With IBNS, 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

IBNS includes providing 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.



Find out more about Intent-Based Networking

Learn More

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. It enables unusual behavior monitoring, which could represent a threat or policy violation. And machine learning 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, 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.

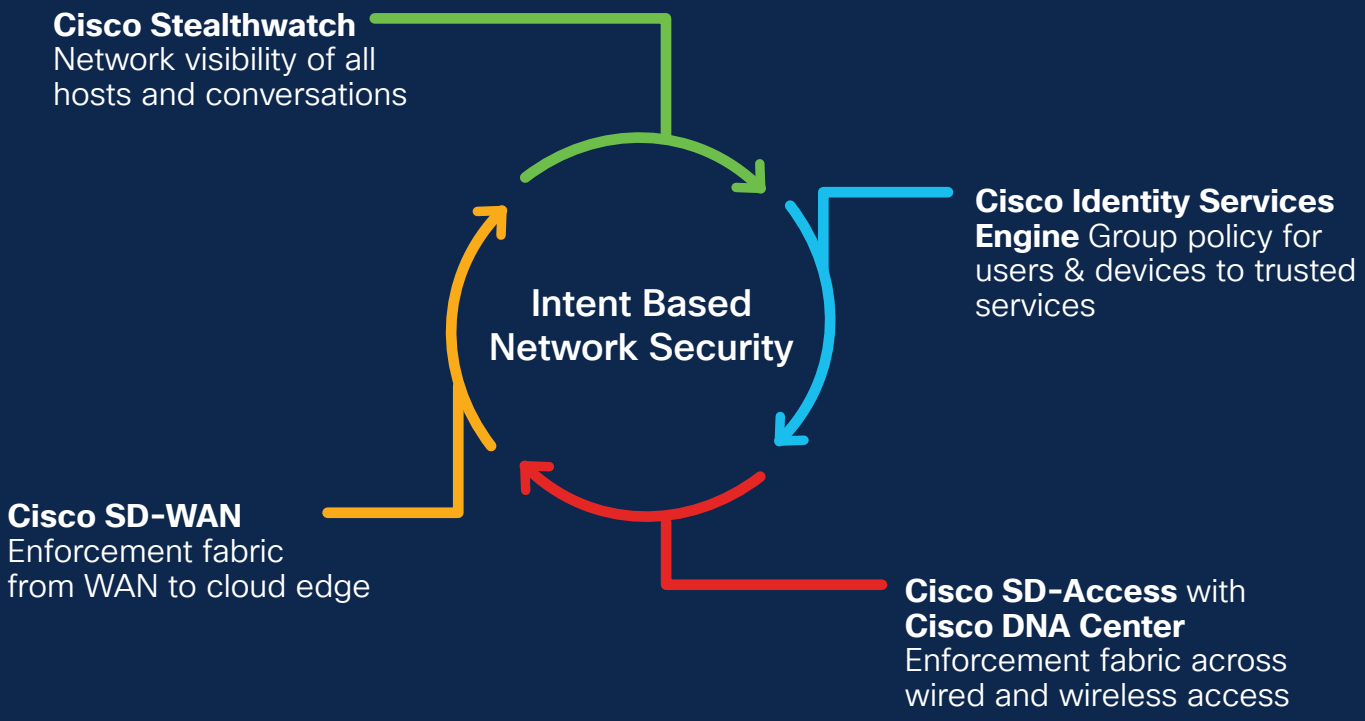
And always verify trust, such that when any user (employee, contractor, third-party) logs into any on-premises or cloud application, notably VPN or email, they must verify their identity with multi-factor authentication (MFA), which mitigates the risk of stolen passwords. A posture assessment of any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

Constant Protection

Network transformations, including SD-WAN and SD-Access, has resulted in a distributed micro-perimeter 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. But 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.

Cisco DNA software subscriptions for switching, wireless, routing and SD-WAN include built in security



Find out more about Cisco DNA software subscriptions

Learn More

As part of, or in addition to, the software subscriptions, **Cisco Umbrella** and **Duo Security** integrate with these IBNS offerings to protect users and devices also when they leave the network.

CXX-XXXXXX-00 XX/XX