Cisco Software-Defined Access

Step up to a new era in networking

What if you had deep visibility into all endpoints on your network and how they were interacting with each other and network resources? What if you could use that information to define and author access control policies? What if you could segment and let the network enforce these policies dynamically and automatically? And what if your network could actively monitor endpoints for any signs of abnormal behavior that might indicate an infection by malware?

Cisco® Software-Defined Access (SD-Access) is a solution within Cisco Digital Network Architecture (Cisco DNA), which is built on intent-based networking principles. Cisco SD-Access provides visibility-based, automated end-to-end segmentation to separate user, device, and application traffic without redesigning the underlying physical network. Cisco SD-Access automates user-access policy so organizations can make sure the right policies are established for any user or device with any application across the network. This is accomplished by applying unified access policies across LAN and WLAN, which creates a consistent user experience anywhere without compromising on security.

Benefits

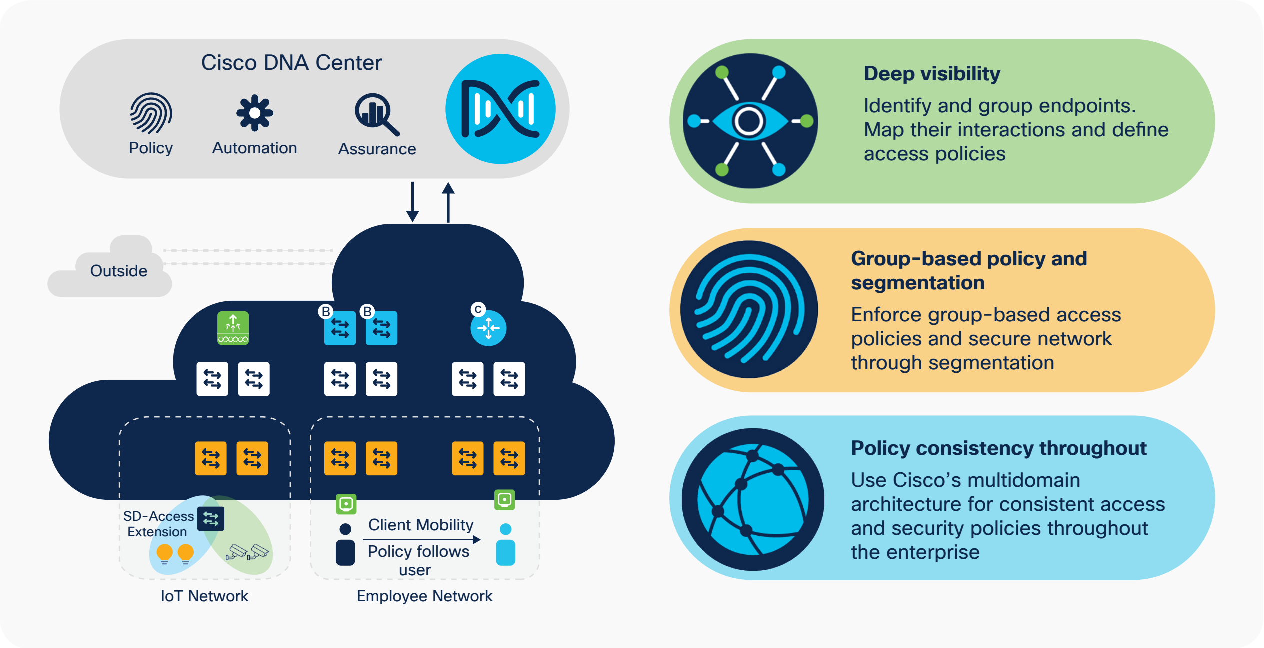
As one of the three pillars of Cisco zero-trust security framework, SD-Access combines security and networking operations. It assists security by enhancing visibility, defining access policies, and improving trust. It improves networking operations by automating network configurations to implement these policies.

- **Identify, profile, and group endpoints:** SD-Access uses AI- and ML-based advanced analytics for endpoint identification and grouping. It analyzes traffic flows between groups and define effective access policies.
- **Segment network based on defined policies:** SD-Access applies group-based access policies for effective multilevel segmentation, leading to zero-trust security.
- **Analyze endpoint behavior and verify trust:** SD-Access continuously scrutinizes endpoint behavior, scans for vulnerabilities, and verifies their trustworthiness for continued access.
- **Rapidly contain threats and prevent data breaches:** SD-Access reduces zones of trust, isolates rogue or compromised endpoints, and enhances regulatory compliance.

Features

- Enhance endpoint visibility by using advanced analytics for user and device identification and profiling. Employ artificial intelligence and machine learning techniques to classify similar endpoints into logical groups.
- Define effective access policies with the help of a thorough analysis of traffic flows between endpoint groups. Enforce these policies through the network infrastructure using a simple and intuitive graphical interface.
- Create virtual overlays to segment both wired and wireless networks uniformly and separate unrelated traffic to provide just the right level of access to endpoints, boosting compliance and reducing business risk.
- Exchange operating policies and ensure consistency by utilizing Cisco's intent-based networking multidomain architecture for enforcement throughout the access, WAN, and multicloud data center networks.

Figure 1. SD-Access overview



Deep visibility
Identify and group endpoints. Map their interactions and define access policies

Group-based policy and segmentation
Enforce group-based access policies and secure network through segmentation

Policy consistency throughout
Use Cisco's multidomain architecture for consistent access and security policies throughout the enterprise

Why Cisco SD-Access?

There are many challenges today in managing the network because of manual configuration and fragmented tool offerings.

Manual operations are slow, error-prone, and are proving to be ineffective due to constantly changing business environments that are adding more and more diverse users, devices, and applications. With the growth of users and different device types coming into the network, configuring user credentials and maintaining a consistent policy across the network – both wired and wireless – is more complex. And as users move around the network, identifying and troubleshooting issues becomes more difficult. The bottom line is that the networks of today do not address today's business needs effectively.

These challenges are deeply rooted within network and security operations as noted below:

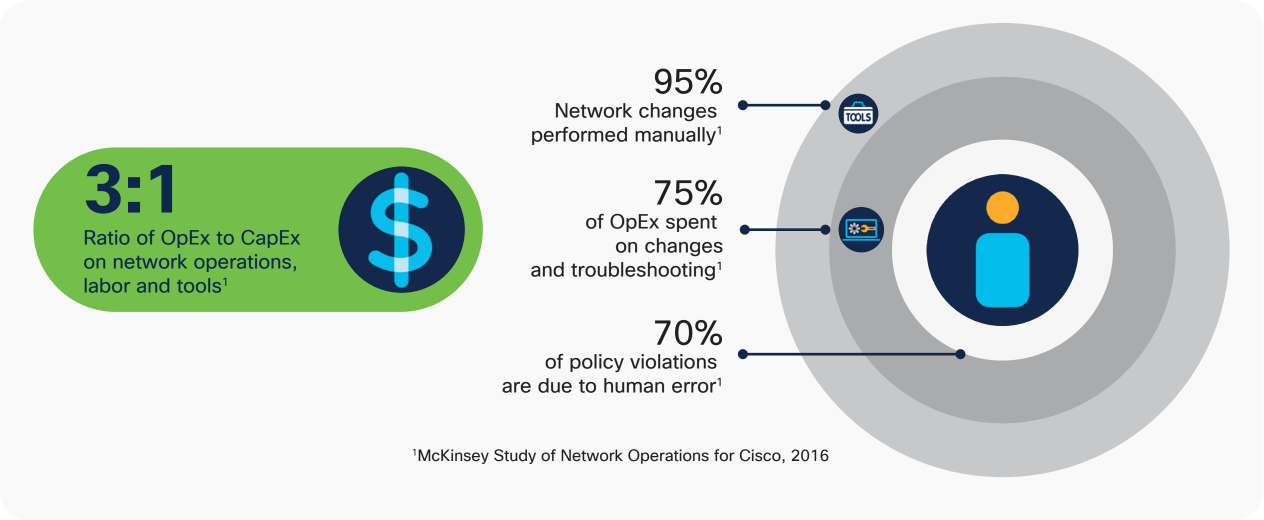
Network operations

- Without adequate knowledge of who and what is on the network and how they are using it, network administrators cannot create endpoint inventories or map traffic flows, leaving them unable to properly control the network.
- Networks cannot respond quickly to evolving business needs if changes need to be done manually. Such modifications take a long time and are error prone.

Security operations

- Securing the network without deep visibility and insights into endpoint identity, composition, location, and behavior, is impossible. Obtaining this level of information on who and what is on the network requires deep analysis of the endpoint and its interactions.
- Effective network segmentation, a well-recognized security best practice, can be exceptionally difficult to achieve in a complex network with a variety of users and devices requiring different access privileges. Traditional IP-address-based methods with firewalls, VLANs, and Access Control Lists (ACLs) do not scale and are not efficient in responding to real-time needs.
- Complying with regulations requires that granular access controls be applied to users and devices and block any unauthorized access. Without an effective segmentation strategy that reduces risk and the scope, cost, and difficulty of compliance assessments and controls, verification of compliance will be extremely hard.

Figure 2. Pace of change exceeds human scale


3:1
Ratio of OpEx to CapEx on network operations, labor and tools[1]
95%
Network changes performed manually[1]
TOOLS
75%
of OpEx spent on changes and troubleshooting[1]
70%
of policy violations are due to human error[1]

[1] McKinsey Study of Network Operations for Cisco, 2016

Cisco SD-Access components and solution overview

Cisco SD-Access enables IT transformation by improving visibility, defining and applying group-based access policies, segmenting network to isolate traffic, reduce risk, and contain threats, and achieving consistency in policy over the entire enterprise, from users to applications. Building this next-generation solution involves some key foundational elements, including:

- Controller-based architecture
- Policy enforcement engine
- Network fabric
- Programmable infrastructure

Controller-based architecture: Traditional networking focuses on per-device management, which takes time and creates many complexities. This approach is prone to human errors. Cisco SD-Access uses Cisco DNA Center, the command-and-control center for the Cisco DNA–based network, to drive business intent into the orchestration and operation of network elements. This includes the day-0 configuration of devices and policies associated with users, devices, and endpoints as they connect to the network. Cisco DNA Center also collects and analyzes network telemetry and data from various sources for deep analytics that identify connected endpoints and associated traffic patterns, and help define access policies.

> **"SD-Access, the software-based solution, opens up new possibilities. The network knows how people work, and this way, service can be more efficient."**

Ester Manzano Peláez
Director-General of Digital Administration, Government of Catalonia

The controller provides a network abstraction layer to arbitrate the specifics of various network elements. Additionally, Cisco DNA Center exposes northbound Representational State Transfer (REST)-based APIs to facilitate third-party or in-house development of meaningful services on the network.

Policy enforcement engine: Policies once defined are stored in Cisco Identity Services Engine (ISE). ISE authenticates and authorizes endpoints based on the security policy – and grants an appropriate level of network access limited on the needs of their roles or functions. It does so by automatically and dynamically configuring network devices as endpoints connect through them to the network.

Network fabric: With a controller and policy enforcement in place, you can start building the network in logical blocks called fabrics. The Cisco SD-Access fabric leverages virtual network overlays in order to support mobility, segmentation, and programmability at very large scale. The virtual network overlay leverages a control plane to maintain the mapping of endpoints to their network location up to date as endpoints move around the network. Separation of the control plane from the forwarding plane reduces complexity and improves scale and convergence over traditional networking techniques. The Cisco SD-Access fabric enables several key capabilities, such as host mobility regardless of volume of moves and size of the network, Layer 2 and Layer 3 segmentation, and wireless integration. Other capabilities include intelligent services for application recognition, traffic analytics, and traffic prioritization and steering for optimum performance and operational effectiveness.

Programmable infrastructure: To build a modern infrastructure, Cisco is equipping its existing and future devices with advanced capabilities to enable full lifecycle management while being open, standards-based, and extensible. These key technologies include (1) automated device provisioning, incorporating well-known functions such as zero-touch provisioning, and Plug and Play; (2) open API interface; (3) granular visibility, using telemetry capabilities such as NetFlow; and (4) seamless software upgrades with live software patching. Cisco Catalyst® wired and wireless networking infrastructure provides all functions necessary for reaping all benefits of SD-Access.

Cisco SD-Access use cases

Building on the foundation of industry-leading capabilities, Cisco SD-Access can now deliver key business-driven use cases that realize the promise of a digital enterprise while reducing the total cost of ownership (Table 1).

Table 1. Cisco SD-Access use cases

Use case	Details	Benefits
Increase visibility	▪ Use Deep Packet Inspection (DPI), telemetry, and other sources to identify endpoints and their attributes ▪ Use AI and ML techniques to classify like endpoints based on shared attributes into logical groups	▪ Build a detailed inventory of previously unknown endpoints ▪ Ensure that endpoints on your network are compliant to policies regarding OS, patch levels, etc.
Determine network policies	▪ Obtain visual representation of traffic flows between endpoint groups with details such as protocols, ports used, etc.	▪ Use the visual flows to get insights into network usage and set policies to permit or deny these interactions or add new ones
Secure through group and policy-based segmentation	▪ Onboard users with 802.1X, Active Directory, and static authentication ▪ Group users with Scalable Group Tags (SGTs) ▪ Automate VRF configuration (lines of business, departments, etc.) and create virtual networks ▪ Use Encrypted Traffic Analytics (ETA) to further enhance analysis of traffic through AVC and NetFlow ▪ Author and enforce granular access and communication policies between groups	▪ Reduce time needed to provision network segmentation and user groups ▪ Segment the network at two levels – a "macro" level that separates larger logical blocks such as lines of businesses, and a "micro" level that permits or denies communication between groups at a protocol and port level ▪ Provide a foundation to enforce network security policies ▪ Be able to detect and intercept threats at line rate (not from samples) from the center throughout the network, including all devices on the network edge
Maintain security by continuous monitoring	▪ Monitor endpoint behavior for suspicious, anomalous, or potential spoofing activity ▪ Collect and analyze intelligence data from endpoints, the security ecosystem, and vulnerability databases ▪ Generate a trust score based on analysis	▪ Determine the trustworthiness of endpoints as they connect to the network and continuously verify it ▪ Guard against malware that might infect endpoints after they are admitted ▪ Flag suspicious behavior and take mitigating steps

Use case	Details	Benefits
Zero-trust security for the workplace	▪ Provide just the level of access required by the user or device according to their role ▪ Protect users and devices against lateral spread of malware	▪ Mitigate the risk of unauthorized access ▪ Proactively contain breaches ▪ Respond to and reduce risks ▪ Enhance regulatory compliance
User mobility	▪ Single point of definition for wired and wireless users ▪ Seamless roaming for wireless ▪ Distributed data plane for wireless access ▪ Simplified guest provisioning for wireless	▪ Management of wired and wireless networks and users from a single interface (Cisco DNA Center) ▪ Ability to offload wireless data path to network switches (reduce load on controller) ▪ Scalable fabric-enabled wireless with seamless roaming across campus ▪ Simplified policy provisioning ▪ Time savings when provisioning policies
Guest access	▪ Define specific groups for guest users ▪ Create policy for guest users' resource access (such as internet access)	▪ Simplified policy provisioning ▪ Time savings when provisioning policies
IoT integration	▪ Segment and group IoT devices ▪ Define policies for IoT group access and management ▪ Device profiling with flexible authentication options	▪ Simplify deployment of IoT devices ▪ Reduce network attack surface with device segmentation
Monitoring and troubleshooting	▪ Multiple data points on network behavior (syslog, stats, etc.) ▪ Contextual data available per user and device	▪ Significantly reduce troubleshooting time ▪ Use rich context and analytics for decision making
Cloud/data center integration	▪ Identity federation allows exchange of identity between campus and data center policy controllers ▪ Share policies between SD-Access, SD-WAN, and multicloud data centers	▪ Administrator can define user-to-application access policy from a single interface ▪ End-to-end policy management for the enterprise ▪ Identity-based policy enforcement for optimized ACL utilization ▪ Flexibility when enforcing policy at campus or data center
Branch integration	▪ Create a single fabric across multiple regional branch locations	▪ Simplified provisioning and management of branch locations ▪ Enterprise-wide policy provisioning and enforcement

Cisco Services

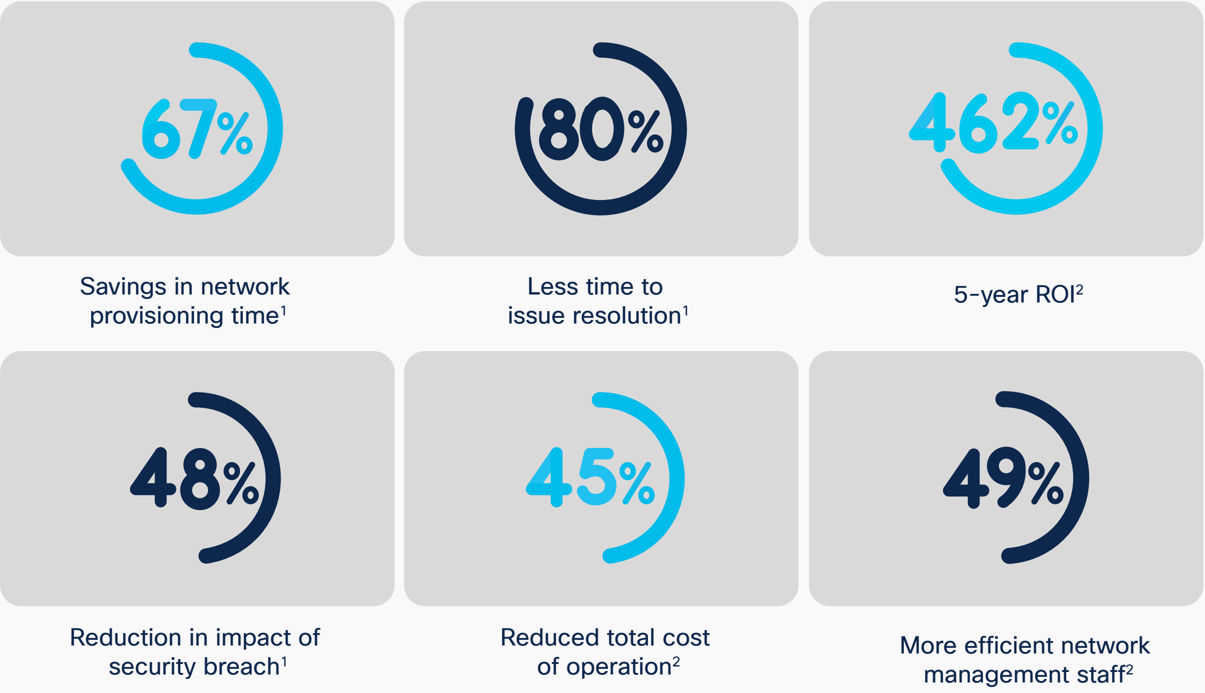
Accelerate your journey to a digital-ready network with Cisco Software-Defined Access services.

Cisco Services provide expert guidance to help you achieve a streamlined operational model across wired and wireless environments at a lower cost. With proven experience, best practices, and innovative tools, Cisco Services work with you to easily manage, scale, and secure your Cisco SD-Access solution. By choosing from a comprehensive lifecycle of services – including advisory, implementation, optimization, and technical services – you can move to a secure and automated unified network with ease and confidence. Learn more.

Giving IT time back with Cisco SD-Access

Cisco SD-Access gives IT time back by dramatically reducing the time it takes to manage and secure your network and improving the overall end-user experience.

Figure 3. Quantitative benefits of SD-Access



67% Savings in network provisioning time[1]

80% Less time to issue resolution[1]

462% 5-year ROI[2]

48% Reduction in impact of security breach[1]

45% Reduced total cost of operation[2]

49% More efficient network management staff[2]

[1] Source: Internal TCO analysis with large-enterprise customer (Actual result may vary.)

[2] Source: IDC business value study of Cisco DNA Center solutions, May 2020

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

Getting started with segmentation through Cisco SD-Access

Network segmentation begins with gaining visibility into what's on the network, but the rapid growth and variety of IoT devices makes that challenging. AI endpoint analytics, a feature of Cisco DNA Center, uses multiple data sources to identify unknown devices based on their state. It then applies AI/ML techniques to intelligently monitor behavioral attributes and group like devices so policy can be applied to the group. This reduces or eliminates the first hurdle in many of our customers' segmentation projects, overcoming a lack of visibility into what and how resources are connecting and applying the right policy that does not prevent the connection, disrupting business objectives.

Next, network segmentation requires knowing the expected, appropriate behavior of devices on the network. Group-based policy analytics, another feature of the Cisco DNA Center, collects and analyzes network traffic flows, models observed behavior based on device types, and then suggests solid segmentation policies. This reduces or eliminates the second hurdle in many of our customers' segmentation projects, which is overcoming complexity in the network to identify and build secure access policies.

Network segmentation then requires some way to "program" the segmentation policy. Historically, this has been through IT engineers writing lines and lines of complex configuration code. But once policy analysis is complete, and you have defined access policies, you may use Access Control Application, running within the Cisco DNA Center, to automatically configure new or update existing policies, dramatically cutting complexity and human error. Cisco ISE then applies these policies in the network infrastructure that enforce them.

Migrating an existing network to Cisco SD-Access

Organizations wishing to convert their existing networks to the simplicity, automation, and security that SD-Access offers, can do so with minimum disruption to their users and connected devices. SD-Access offers several ways for you to evolve your network from where it is now to a state where it can take advantage of all of SD-Access.

How to buy

To view ordering and buying options and speak with a Cisco sales representative, refer to the [Cisco SD-Access ordering guide](#) or visit [www.cisco.com/c/en/us/buy](#).

Figure 4. Simple paths to full SD-Access

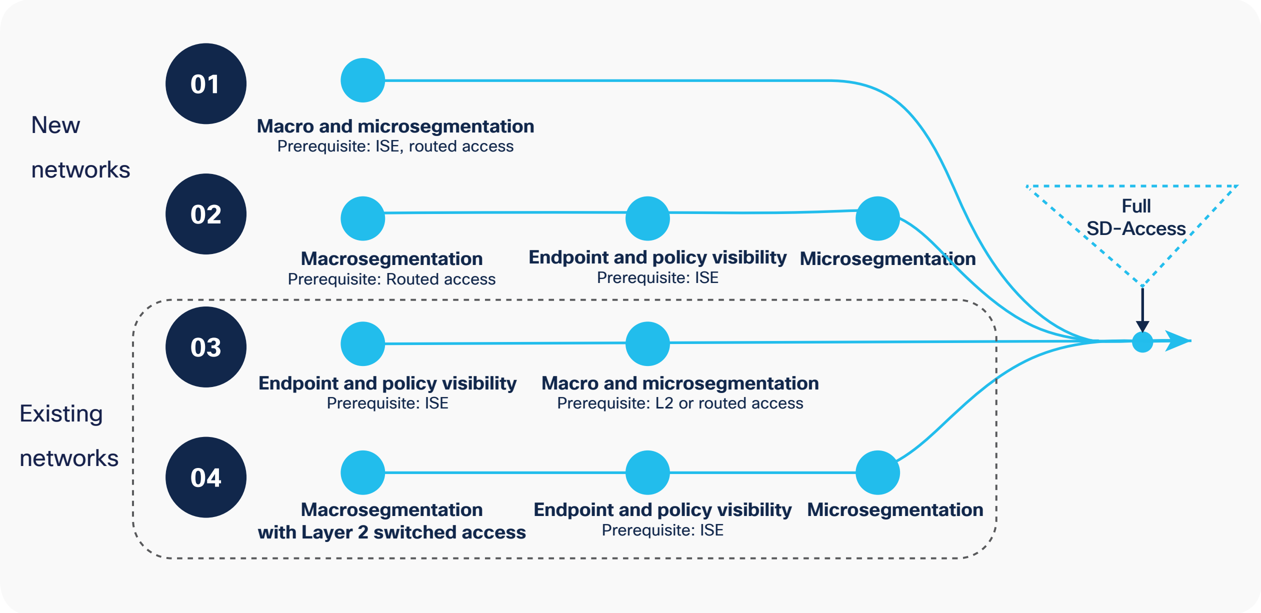

New networks
01
Macro and microsegmentation
Prerequisite: ISE, routed access
02
Macrosegmentation
Prerequisite: Routed access
Endpoint and policy visibility
Prerequisite: ISE
Microsegmentation
Existing networks
03
Endpoint and policy visibility
Prerequisite: ISE
Macro and microsegmentation
Prerequisite: L2 or routed access
04
Macrosegmentation with Layer 2 switched access
Endpoint and policy visibility
Prerequisite: ISE
Microsegmentation
Full SD-Access

Figure 4 shows the small steps that networks, both new and existing, with different starting points, can take to reach full SD-Access while realizing incremental benefits with every step. For example, an existing network without ISE (depicted as #04 in Figure 4) may start by using Cisco DNA Center to create virtual networks to macro-segment. This step does not require any change in existing access layer switches, and hence can quickly and automatically secure the network. As the next step, this network can add ISE to increase visibility, establish policy, and further improve security through microsegmentation to reach full SD-Access status as the access infrastructure is upgraded.

Similarly, an existing network that already has ISE in their network can increase visibility and establish policies using AI endpoint and group-based policy analytics. They can then use Cisco DNA Center to perform both macro- and microsegmentation on their way to full SD-Access.

New installations have their pick of starting points based on their objectives. They can start with a full implementation on day 1 or slowly build their infrastructure and gradually work their way up to SD-Access.

Next steps

- Build your solution with Cisco DNA Solution Builder.
- Follow the Cisco Validated Design guides.
- Register to attend a live SD-Access demo.

While the benefits of segmentation can be realized without a fabric, SD-Access enables the fabric to first be introduced at the distribution layer of the network topology. This is especially helpful to those who have existing Layer 2 access configurations and would prefer not to reconfigure immediately to Layer 3 access. Even without the fabric, SD-Access benefits such as endpoint and traffic visibility through AI endpoint analytics and group-based policy analytics, and Cisco DNA Center features such as Assurance, Automation, and security integrations can be realized.

Access layer switches may connect to the distribution switches as extended or policy-extended nodes. Policy-extended switches perform inline tagging and enforce access policies, but still provide Layer 2 connectivity to their endpoints. Endpoints connected to the access switches do not see any change and continue to function as usual in this hybrid setup.

Once the distribution layer has been migrated, access switches can then join the fabric in a controlled and gradual manner. Devices connected to such switches maintain interconnectivity to the devices and services that are yet to be migrated over, while providing the benefits of the fabric.

Customer success stories

Cisco customers in every industry are changing the way they approach network and security operations in their networks with Cisco SD-Access. Take a look at the latest customer case studies to learn how customers are deploying Cisco SD-Access and the benefits they are experiencing. Read stories.