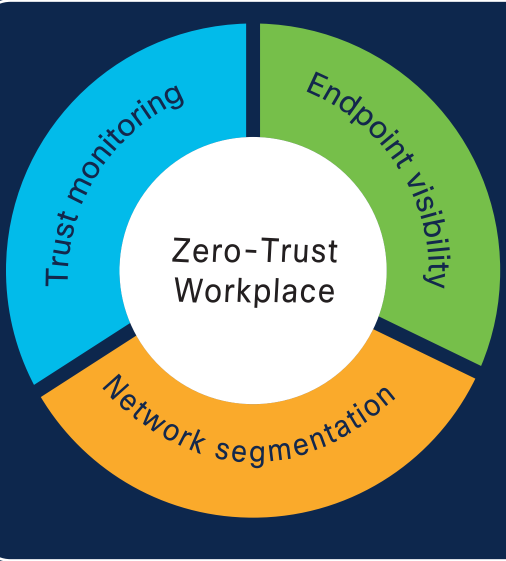
cisco
The bridge to possible

Cisco Software-Defined Access for Zero-Trust Workplace

Zero-Trust Workplace capabilities

Cisco® SD-Access helps streamline the process of providing access to users and devices while mitigating the increased risk of unknown IoT devices. By using network infrastructure and telemetry to inform and enforce security, SD-Access can deliver unrivaled zero-trust workplace capabilities for IoT endpoints and managed user devices while helping ensure continuous trusted access.



Zero-Trust Workplace

Endpoint visibility

Network segmentation

Trust monitoring

Endpoint visibility
Know who is on your network

Segmentation
Define what endpoints can access

Continuous trust assessment
Always-on analysis and enforcement

Why Cisco SD-Access for Zero-Trust Workplace?

- Identify and verify all endpoints and users, including IoT endpoints, that connect to your network
- Establish policy and segmentation to help ensure least privilege access based on endpoint and user type
- Continually monitor endpoint behavior, including encrypted traffic, to help ensure compliance
- Stop threat propagation, including ransomware, by quarantining any endpoint that exhibits malicious or out-of-compliance behavior

For more information

Cisco SD-Access is built upon the robust Cisco DNA Center platform and leverages the security capabilities of Cisco Identity Services Engine and Secure Network Analytics as well as third-party identity and vulnerability management solutions. For more information, visit the Cisco SD-Access, Cisco DNA Center, and Cisco Zero Trust Security pages. Or talk with your Cisco Sales representative.

Cisco SD-Access is uniquely able to support the exponential growth of IoT devices because it analyzes and identifies devices, defines what assets those devices can access, and continually monitors device behavior to help ensure that they continue to operate according to their assigned policy.

This solution can be deployed on your existing network infrastructure yet has flexible deployment options so that it can evolve as your business and technical needs grow.

What it does

Know who is on your network

To truly secure your network, you need to know what is connecting to it. For managed devices, such as laptops and smartphones, Cisco SD-Access provides support for Mobile Device Management (MDM) and other device verification solutions to determine that the connecting device is what it says it is. For IoT devices, Cisco SD-Access uses network-based artificial intelligence and machine learning to identify attributes of the unknown IoT device and compares those attributes to a huge database of known devices. If the IoT device is not part of our known universe of devices, the solution automatically groups it with like devices into a single group.

Define what endpoints can access

Cisco SD-Access lets you easily define segmentation and access policies for individual devices as well as groups of similar devices. These policies define least privilege access to help ensure that the devices have only the minimal level of access—nothing higher—to minimize the potential for lateral movement of threats. You can automatically and continually monitor your established segmentation and access policies, and map what devices are accessing what workloads. You can use this visual information to build more effective segmentation and to identify potential problematic devices. Then it's a quick update to refine and revise your segmentation and access.

Always-on analysis and enforcement

Security threats are always evolving, so SD-Access provides a continuous loop of analysis and enforcement to stay atop intrusions and vulnerabilities. Endpoint activity is continually monitored and mapped to help ensure that each device is acting according to policy and type. This approach can be very effective in controlling ransomware attacks. When ransomware tries to move laterally throughout the organization, SD-Access identifies the out-of-policy traffic and then blocks access and quarantines the device until it can be disinfected. As a result, the ransomware malware is contained so that it cannot impact the entire company.