As the number of connected devices multiplies and demand for data-intensive applications increases, IT is being challenged to provide a fast, reliable, and secure network for branches and campuses. Only Cisco® Secure Network Access helps IT troubleshoot faster, automate network onboarding and management, integrate security, and provide location analytics for the network.





in time for issue detection and resolution.1



in alerts with DNA Assurance AI/ML.¹

Campus network assurance

IT needs to improve network availability and performance as employees and customers demand a high-quality experience every time they connect to the network.

- Identify and solve network issues faster and even avoid issues, using the real-time analytical capability provided by the network.
- Provide network visibility and assurance across the entirety of the campus infrastructure from a single pane of glass.
- Monitor the network and identify unusual behavior for security or performance mitigation with enterprise-scale artificial intelligence (AI) and machine learning (ML).

Network device onboarding

The network needs to move as fast as the business. Automating network deployment and software maintenance allows IT organizations to move faster in designing, configuring, and deploying new services.

- Provide robust automation capabilities for onboarding network devices and maintain consistent software and security versions (LAN and WLAN) throughout the network lifecycle.
- Automate the network with Cisco DNA Center to save time, reduce the potential risks of manual processes, and lower expenses.
- Use a single automation solution for the entire campus infrastructure, both for day-0 deployments and day-1+ changes.
- Design the network before the physical site is up to increase flexibility and agility.









time deploying a server.²





Campus software image management

Network performance and security compliance require up-to-date and consistent network images across the entire network. Cisco DNA Center helps manage the discovery and integration of new software versions and security patches by automatically rolling out software patches and addressing security vulnerabilities with no or little IT staff effort. - Automate network upgrades, software image

- management, and infrastructure refreshes with Cisco DNA Center.
- Maintain consistency in software and features throughout the LAN and WLAN infrastructure.
- Decrease the number of security and configuration incidents and platform vulnerabilities. • Help ensure that the infrastructure is capable of a
- and sufficient memory.

successful upgrade by verifying hardware compatibility

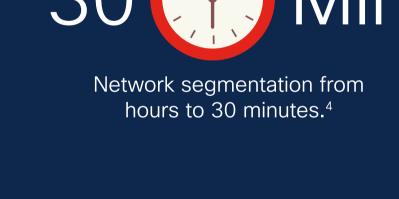
segmentation Design a network that can automatically segment users and devices. The result is a

Campus network

network that can automatically recognize things and provision the appropriate policy. • Provides a single platform that enables enhanced ability to define both macro and micro-segmentation for scalability and flexibility

- A single network fabric the enables a consistent user experience anywhere without compromising security - Combines robust device profiling with segmentation
- policy, enabling automatic security segmentation for IoT devices

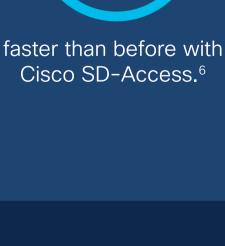








business outcomes.



Scalable access policy Security policies should be different depending

on the user, device they use or thing. A secure access network can automatically recognize and apply policies through the organization.

 Provides the ability to connect an increasing number of device types Create and implement dynamic security capabilities by user, device and application

- These policies can be automatically implemented in conjunction with segmentation capabilities • Dramatically reduce security risk associated
- with network access, both wired and wireless



Location analytics

Eliminate the physical blind spot and understand how people and things interact

in physical spaces. Leverage existing Wi-Fi

deliver contextual engagements, and drive

infrastructure to gain actionable insights,

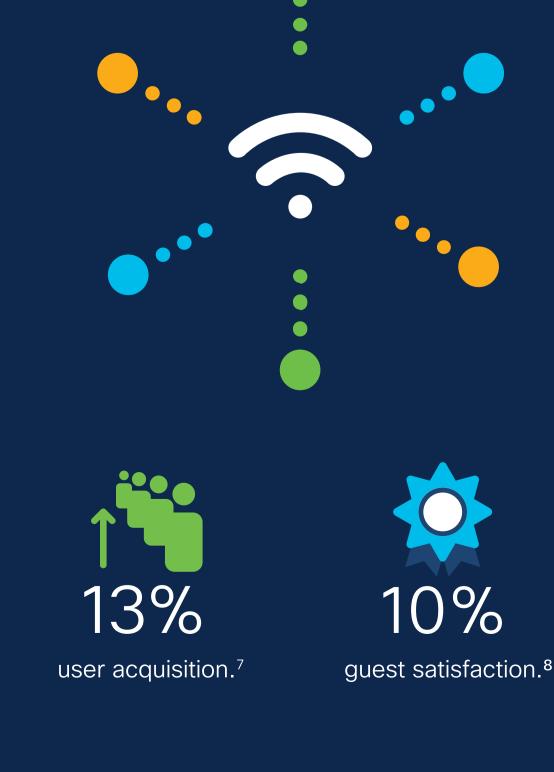
 Gain centralized control over and visibility into location services via a single role-based dashboard. • Enhance customer experiences by gaining insights into people (visitors and employees) and delivering relevant

experiences at the right time and place.

costs through asset management. Increase attachment rates and gain actionable insights

• Improve the efficiency of business operations and reduce

with OpenRoaming, and open up new opportunities for you and your guests.



Read whitepaper



1. Internal Cisco TCO analysis with large enterprise customers. 2. Tromso Kommune case study.

3. The Total Economic Impact™ of Cisco TrustSec Simplified Security Engineering and Reduced Operations Costs Enabled By Cisco, A Forrester Total Economic Impact™ Study 4. Customer: Waterford Institute of Technology.

5. Customer: Children's Hospital Los Angeles 6. Customer: City of Luxembourg 7. Customer: Norwegian Professional Football League

8. Customer: InterContinental Hotels Group

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)