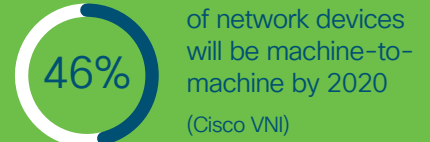
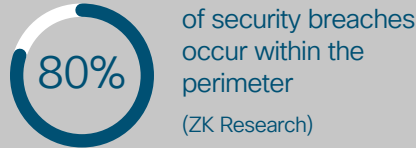
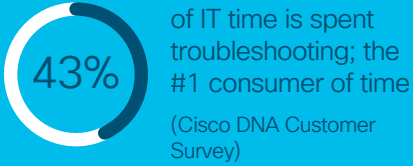


Top 3 Networking Challenges for the DoD

1. Larger networks mean more time and resources to provision and troubleshoot.

2. Defending the network is hard. Attacks continue to increase.

3. Controlling an ever-increasing number of wireless and IoT devices is difficult.



The Solution: Cisco DNA Center



The Benefits

- End-to-end troubleshooting
- Automated provisioning of access switches



- Provision
- Design
- Analyze
- Policy

Reduce device configuration time

Time to configure 50 devices:



Shift IT time to the mission focus

Analysis and testing with customers using SD-Access revealed that:



- Easily click and create virtual networks within the software defined network (SDN)



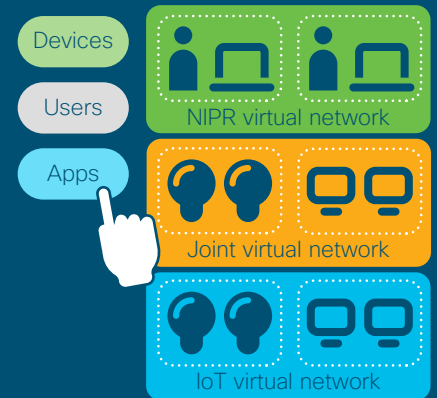
- Simplified microsegmentation
- Stops attacks from spreading
- No VLANs, ACLs to configure

Upgrade to Catalyst 9000 SDA capable switches



- ✓ FIPS approved
- ✓ Common Criteria
- ✓ UC APL Listed
- ✓ Encrypted Traffic Analysis

- Drag and drop groups to apply mission intent and policy



Simplify your IT

- Segment and control wireless and IoT devices
- Policy follows identity wired and wireless



Cisco access points are SDA ready.

- Use the network to enforce security for new wired and wireless applications

To learn more about DNA for government, visit cisco.com/go/FederalDNA

