Compliance Management and Configuration Platform

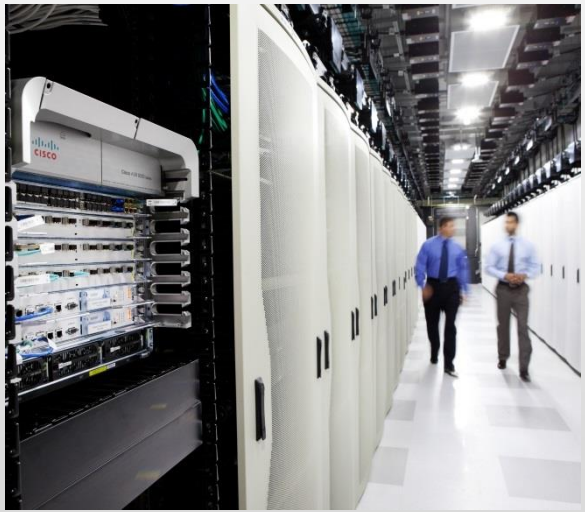
Customer EBC

Date:

Understand, Control, and Maintain Compliance in Your Network

- Avoid Security Breaches
- Automate Change
- Eliminate Manual Errors
- Reduce Operational Expenses
- Protect Your Reputation

Compliance Management and Configuration Platform



A Structured Approach

CMCP helps customers understand and control organizational, commercial, and regulatory compliance across their entire networks by **assessing** and **remediating** outdated and inaccurate software images and configurations **to achieve and then maintain ongoing compliance and configuration standards**.

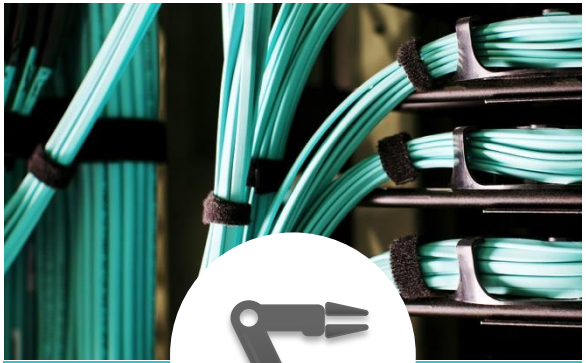
Compliance Management & Configuration Platform

People

- Cisco configuration and compliance management expertise

Processes

- Integrates into customer change processes to provide execution



Tools

- Best –in-class capabilities with intellectual capital updates

Key Benefits

Compliance Management and Configuration Platform Provides...

- Best practices, configuration guidelines, commercial, and regulatory standards embedded in appliance database.
- Workflow management for centralized control increases security and accountability.
- Automation provides a measurable path toward continuous compliance.

Key Outcomes

Compliance Management and Configuration Platform Delivers...

- PSIRT vulnerabilities are mitigated or eliminated based on customer prioritization
- Security policies are implemented, monitored, and remediated, eliminating known issues
- All remediation documented, logged and synchronized with customer change control board

Customer Challenges

Compliance and Change Management

Compliance Management

Usually poorly understood

Measurement is often a “snapshot”

Poor visibility into corporate configuration policy

Configuration Management

Most configuration changes are manual

~70% of network downtime due to human error

Majority of problems detected after deployment

Poor visibility into industry best practices

Workflow Management

No desire to learn new tools, interfaces, or procedures

Poor overall control results in extreme control measures

Change activity occurring by non-entitled individuals

Limited audit trail for changes made

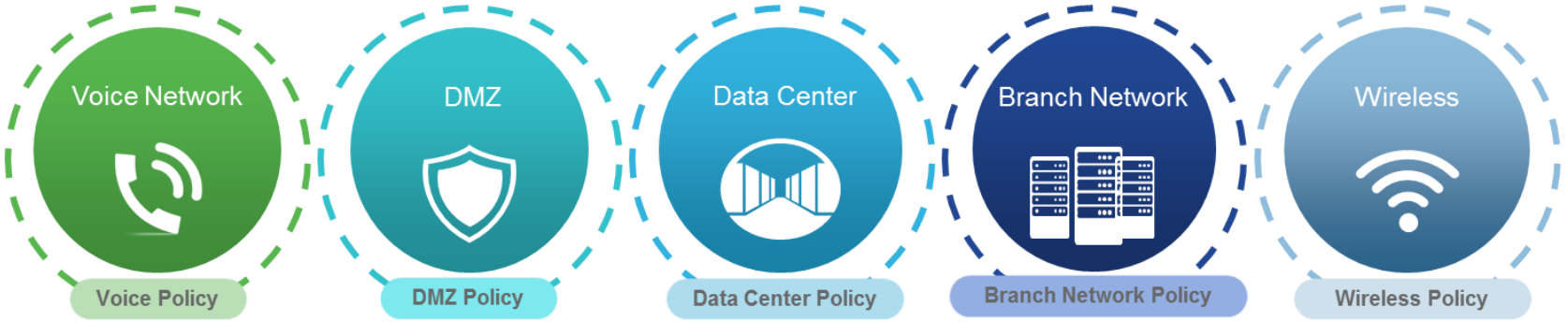
Software Management

Process is often limited to paper-based flow diagrams

Even small errors will cause large issues

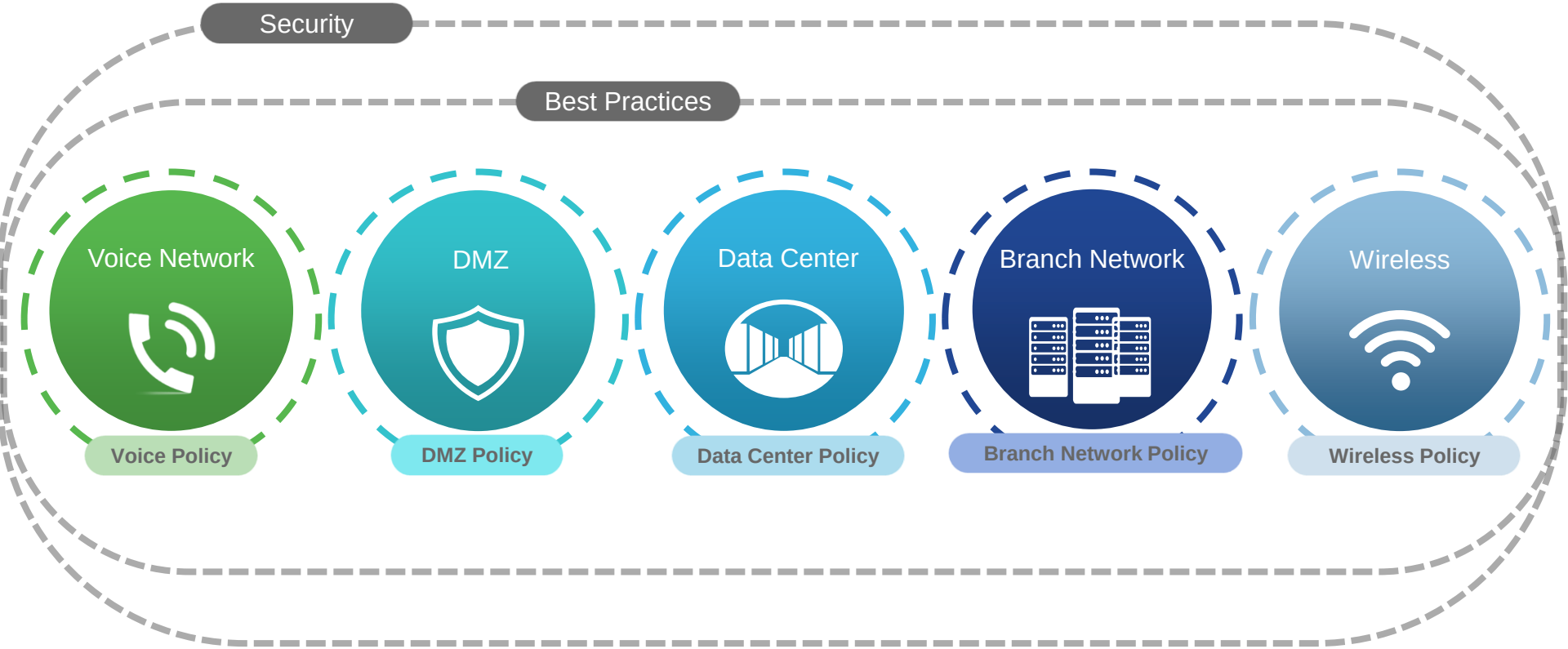
Manpower-intensive

Customer Challenge: Network Policies & Gen1 Tools



- Multiple different network platforms, network OS types and vendors
  - Cisco; Juniper; F5 , Arista, etc.
  - ISR; ASR; Catalyst; Nexus, etc.
- Hundreds of OS versions deployed
  - Multiplies by vendor; OS type, and version (IOS vs. IOS XE and IOS 16.2.21-ert, etc.)
- Fluid organizational - functional needs
  - Configuration by functional area; geography; role; or combination
  - Evolution of company
  - Evolution of threats

CMCP Policy Management



Customer Case Study

Global Financial Services Provider

Customer Issue

- 542 versions of OS deployed across 10,000 network elements. Recommended reduction to 29 versions
- Failure of internal Security & Best Practices configuration audit – bring installation into compliance
- Cost & Timeline bids by internal and external sources: Timeline 36 months+; Cost = $3.6 to $4.2M

8K+ OS SWIM upgrades

~15K Policy Configuration changes

99.2% of changes executed successfully without human intervention

Delivered within 8 months @ 40% of the cost projected by other bids