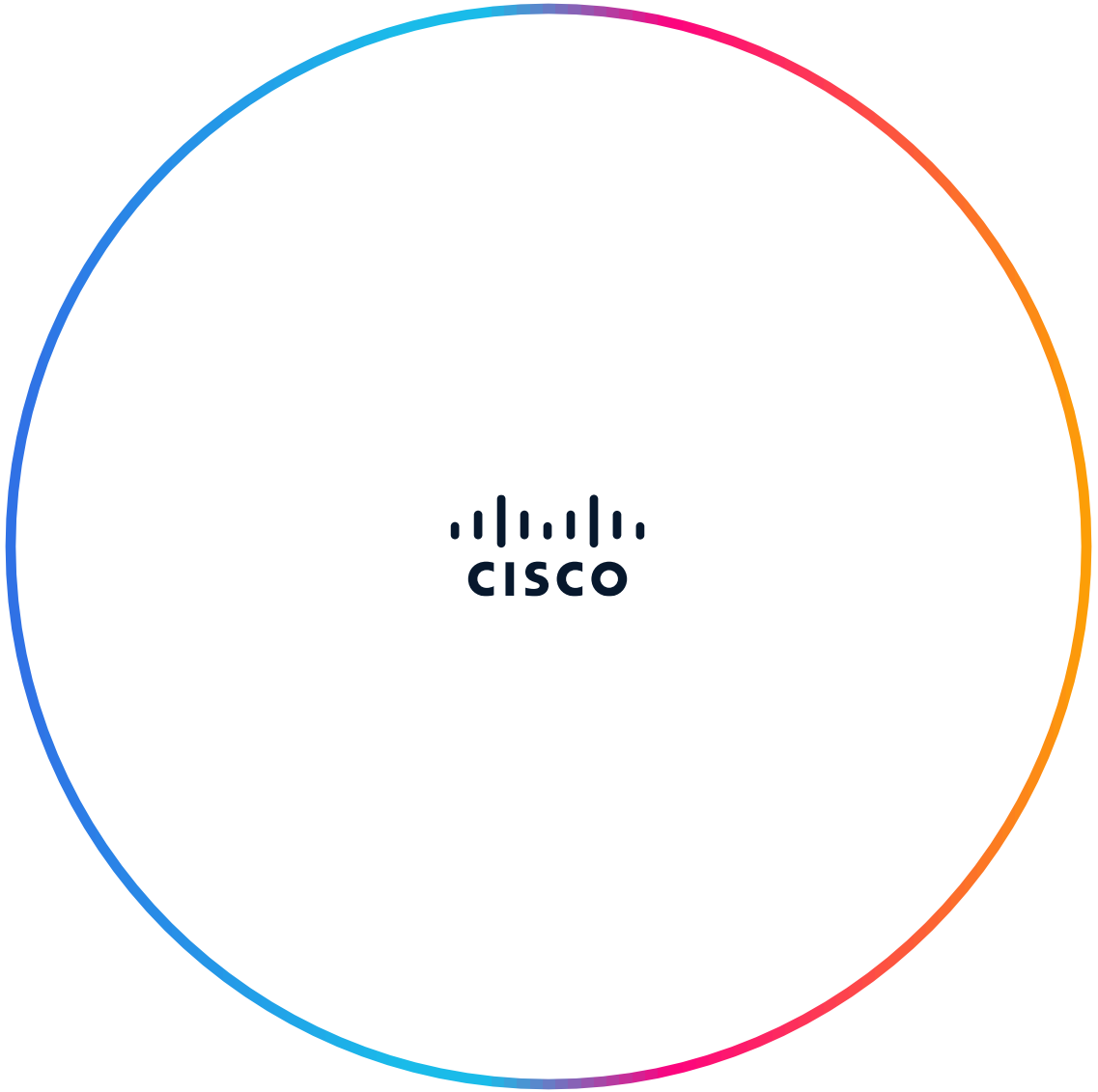
From Manual Audits to Automated Guardrails

Policy-as-Code in Modern Cybersecurity

Loránd Jakab, Cisco
linkedin.com/in/lorand



November 5, 2025

About Me

- NetAdmin/SysAdmin @ UTCN Dorm Campus Building 5 – IPv6 early adoption
- PhD @ BarcelonaTECH
- Cisco
  - R&D / Patents
  - LISP – IETF (RFC 7215, active current draft), Open Source
  - Application Networking, Automation: Infrastructure-as-Code, Policy-as-Code

© 2025 Cisco and/or its affiliates. All rights reserved.

Feel free to interrupt and ask questions at any time



© 2025 Cisco and/or its affiliates. All rights reserved.

Insecure defaults, misconfigurations, oh my!

- Some products still come with insecure defaults (convenience, compatibility, lazyness)
- Human error still the biggest source of misconfiguration errors
- A significant fraction of security incidents stem from misconfiguration, especially in the cloud
- "Through 2025, 99% of cloud security failures will be the customer's fault" (Gartner, 2023)* Primarily due to misconfiguration and mismanagement
  - Survey of 800 IT Leaders:
  - 78% experienced at least one cloud misconfiguration incident in past 12 months
  - 23% experienced data exposure due to misconfiguration
  - Average cost per incident: $620K (median: $380K)
- Forecast: By 2026, organizations with automated policy enforcement will experience **80% fewer security incidents** than those relying on manual processes

- **The gap:** Known best practices exist, but manual processes fail under pressure

* Gartner, Inc. (2023). *Market Guide for Cloud Security Posture Management*. Gartner Research Note G00793595

© 2025 Cisco and/or its affiliates. All rights reserved.

Why Misconfigurations Persist

Insecure defaults in cloud platforms and infrastructure

Human error in manual processes

Changes made under time pressure

Lack of standardized enforcement mechanisms

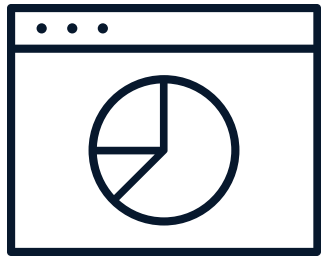
Knowledge gaps and complexity of modern infrastructure

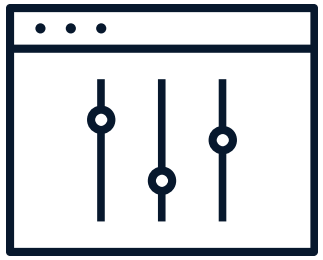
Disconnect between security policies and implementation

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Dashboards and ClickOps







- Still the main modus operandi for a lot of organizations

- If you have clear processes defined → AUTOMATE
- If you repeatedly do some operations → AUTOMATE
- If an operation is complex, write a script, test in staging → AUTOMATE

© 2025 Cisco and/or its affiliates. All rights reserved.

Manual Audits and Their Limitations

- Periodic security reviews and audits, with checklist-based compliance verification
- Post-deployment security assessments
- **Compliance certifications: Point-in-time snapshots**
  - E.g., ISO 27001 audit: Valid for moment of assessment
  - Configuration drift after certification
  - Annual or bi-annual recertification cycles
- Key limitations
  - Reactive rather than proactive
  - Time-consuming and expensive
  - Don't prevent issues, only detect them
  - **Compliance gaps between audit periods**
  - Scale poorly with infrastructure growth

© 2025 Cisco and/or its affiliates. All rights reserved.

OK, Manual Stuff is Bad. Now What?

- Dev(Sec)Ops and Infrastructure-as-Code
  - Automation
  - Declarative infrastructure
  - Version control
- GitOps
  - CI/CD Pipelines
  - Development / Staging / Production
- Shift from "security as audit" to "security as guardrails”
- Policy-as-Code
- Automation as a core security principle

© 2025 Cisco and/or its affiliates. All rights reserved.

What is Policy-as-Code?

- Definition: Codifying security policies into executable rules
- Key principles:
  - Machine-readable policy definitions
  - Version-controlled policy repositories
  - Automated policy evaluation
  - Consistent enforcement across environments
- **The Continuous Compliance Paradigm**
  - Every change evaluated against policies
  - Real-time compliance verification
  - Automated evidence generation
  - **From annual certification to continuous certification**
- Benefits: Speed, consistency, scalability, auditability, **continuous compliance posture**

© 2025 Cisco and/or its affiliates. All rights reserved.

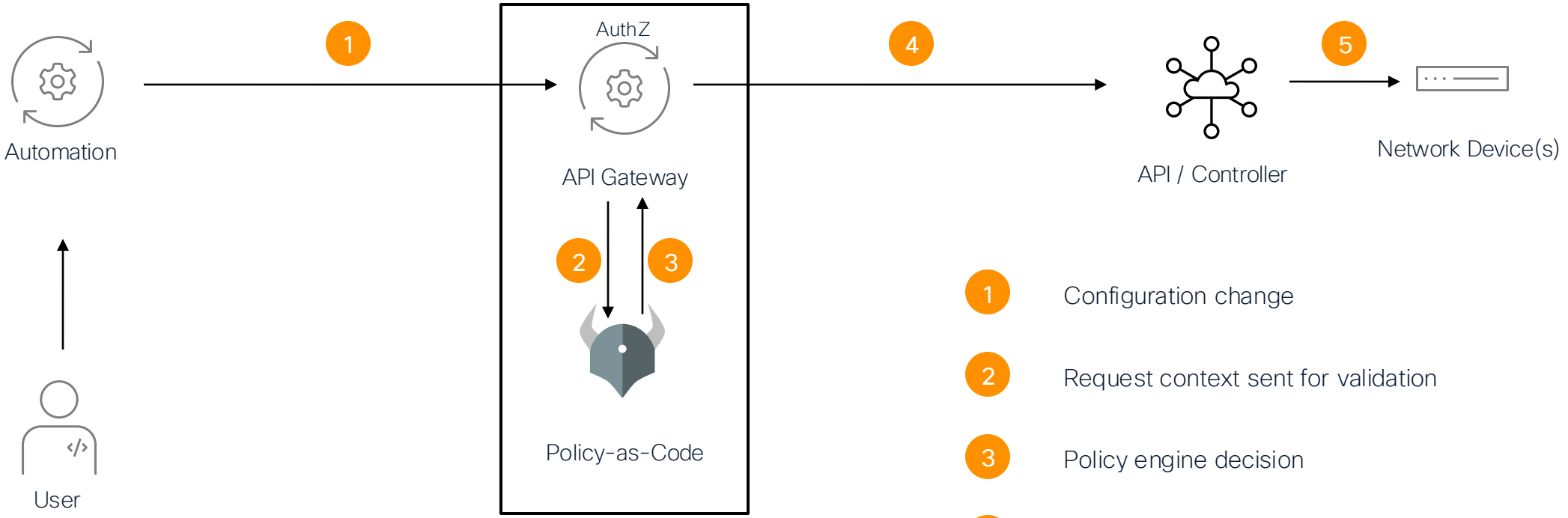
Application of Policy-as-Code

- Check configurations before applying...
  - ... as a component of your (network) infrastructure **automation** suite

- Periodically (and on-demand) poll and check configurations...
  - ... as a component of your (network) infrastructure **monitoring** suite

© 2025 Cisco and/or its affiliates. All rights reserved.

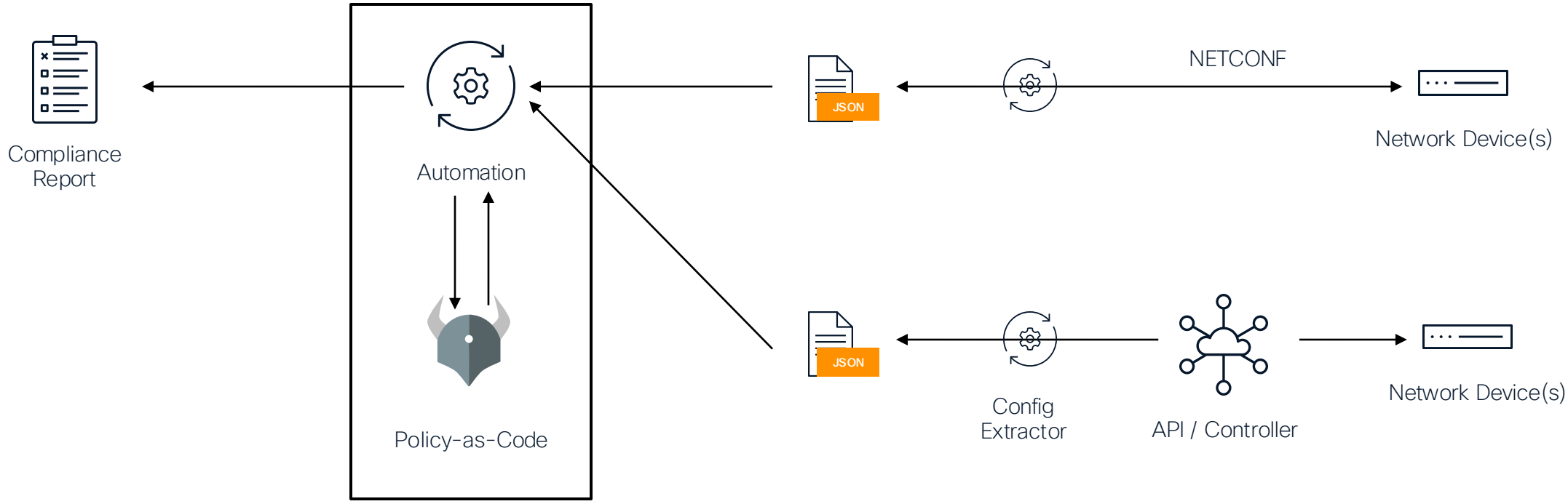
Configuration Change Compliance Check



1. Configuration change
2. Request context sent for validation
3. Policy engine decision
4. Valid change reaches controller
5. Change is applied to device(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

Current Configuration Compliance Check



© 2025 Cisco and/or its affiliates. All rights reserved.

Open Policy Agent

- Open source, **general-purpose** policy engine
  - Unifies rule validation across the stack

- Provides a high-level declarative language (Rego)

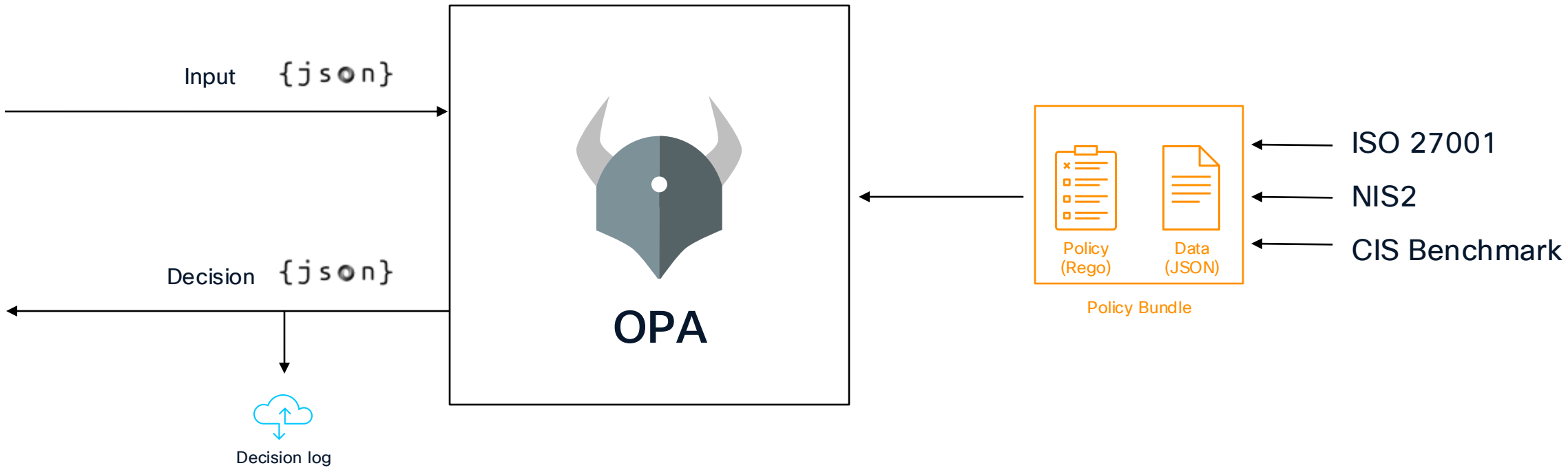
- Exposes APIs to offload policy decision-making from other components

- Graduated CNCF project (Feb. 2021)

- ABN Amro KubeCon presentation

© 2025 Cisco and/or its affiliates. All rights reserved.

Components of an OPA Setup



© 2025 Cisco and/or its affiliates. All rights reserved.

Open Source Considerations

- **Advantages:**
  - Transparency and auditability
  - Community-driven improvements
  - Avoid vendor lock-in
  - Faster innovation
- **Security considerations:**
  - Supply chain risks
  - Maintenance and support
  - Governance models

© 2025 Cisco and/or its affiliates. All rights reserved.

Strengthening Cybersecurity Through Automation

My Recommendation 1: Mandate Automation in Critical Sectors*

- Require policy-as-code for critical infrastructure (NIS2 entities)
- Define minimum automation thresholds
- Enable continuous compliance certification models
- Phased implementation roadmap

My Recommendation 2: Promote Interoperability Standards

- Develop or adopt EU-level policy language specifications
- Certification programs for policy engines
- Cross-border policy sharing frameworks
- Standardize continuous compliance reporting formats (e.g., Open Security Controls Assessment Language: OSCAL)

My Recommendation 3: Support Open Source Policy Development

- EU funding for open policy libraries
- Reference implementations for common controls (ISO 27001, NIS2)
- Open compliance evidence frameworks

** These recommendations are expressing my personal opinion*

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Call to Action

Pretty please, with sugar on top,
avoid manual ops and start automating!

© 2025 Cisco and/or its affiliates. All rights reserved.


CISCO