Solution Brief

anuta networks

Eliminating IT Silos: Pioneering Networks with Cross-Domain Automation

Manage Across Increasing Network Complexity

Finding Control in Commotion

Multi and hybrid cloud connectivity moves the Internet perimeter from centralized control and data planes to a distributed model encompassing many interconnected technologies from different vendors. This domain shift demands diverse skill sets and new tools for effectively managing the planning, installation, analysis, assurance, and security aspects of today's modern networks.

To effectively manage these expansive networks, communication service providers (CSPs) and enterprises have segmented their deployments into domains, often categorized by technology, service, geographical location, or organizational boundaries. This layered infrastructure brings with it the ability to more easily access on-demand services while increasing operational complexities.

The key to enabling a smooth multi-cloud operation is a versatile and cross-domain automation (CDA) platform that integrates necessary functions into a unified experience across all domains.

Key Considerations for CDA

Networks can be characterized by their extensive size, complexity, and a mix of vendor solutions. There are several considerations that must also be navigated:

Heterogeneous vendor landscape: Networks often comprise equipment and technologies from various vendors. Many vendors do not support automation for legacy multi-vendor equipment as they lack standardized interfaces. Each vendor typically has proprietary management interfaces, protocols, and command sets, and a best-of-breed environment makes it difficult to achieve seamless interoperability and automation across multiple vendors.

Presence of numerous control frameworks: A data center might have a separate controller for network virtualization. In contrast, the wide area network (WAN) may have a different controller for routing and traffic management. These controllers often operate independently, leading to fragmentation and limited visibility across the entire network.

Long cycles with adapter delivery: Integrating adapters across domains involves complex integration requirements, stringent security measures, and policy compliance, all leading to extended development timelines. Device adapters must handle various systems, protocols, and data formats to work across domains.

Navigating control for hybrid multi-cloud- Ensuring consistent control and compliance is crucial in cross-domain networking involving hybrid and multi-cloud architectures. Different cloud providers may have varying security protocols, compliance requirements, and data protection mechanisms, necessitating a focus on maintaining compliance for SLA adherence.

Security and access controls: Cross-domain automation requires strict security measures to protect sensitive data and ensure authorized access. Implementing robust security controls across diverse network environments can be complex, as each domain may have its own security policies, authentication mechanisms, and encryption standards.

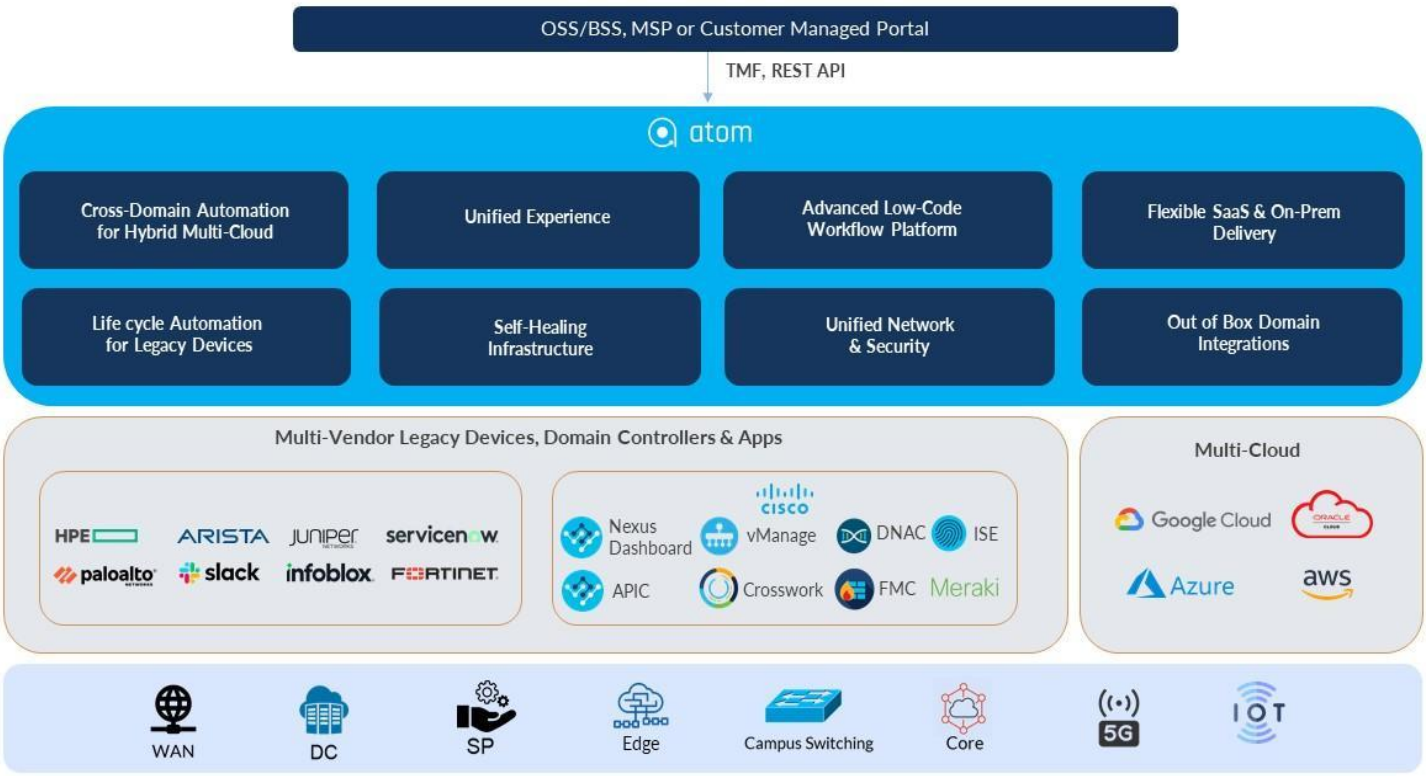
Anuta Networks ATOM Implementation

Anuta Networks has identified APIs as the key to automation across domains within the ATOM platform. It has built a significantly differentiated solution enabled through workflow automation, a modern, cloud-based architecture, and can be deployed in the cloud, on-premises, or hosted.

Solution Brief

anuta networks

Anuta ATOM- Cross-Domain Automation

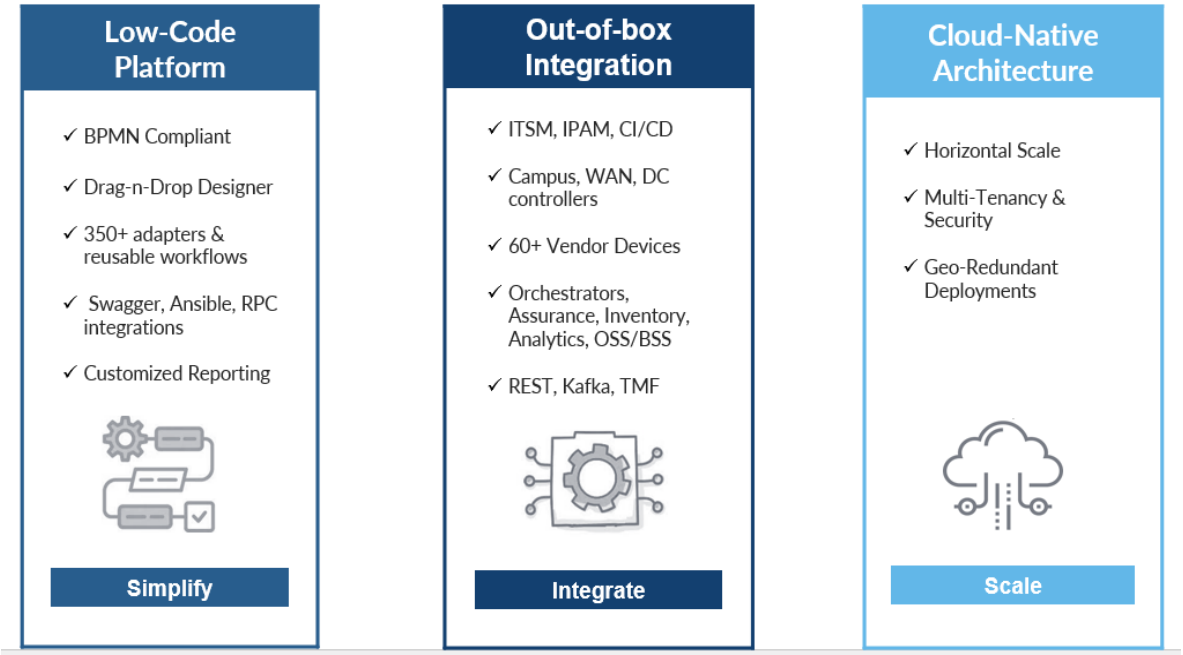


Unified Experience for Networking Cloud with ATOM

Spanning the cloud, the data center to workplace applications, ATOM's technology and services help customers to Simplify, Integrate, and Scale networks with the industry's most comprehensive feature portfolio-

Solution Brief

anuta networks



Workflow: The ATOM framework incorporates an AI-powered Workflow Platform featuring over 350 pre-built libraries and automated adapter integration. Its Visual Designer simplifies the creation of automation workflows, while the Workflow Optimizer optimizes and enhances the efficiency of these workflows. The Planner & Scheduler component allows for effective scheduling and management of automation tasks, while Custom Dashboards offer personalized views and insights.
It also provides a Workflow Co-Pilot feature that utilizes the power of ChatGPT (Generative AI) to provide a Virtual Assistant, acting as a knowledgeable and interactive guide in the automation process.

Architecture: Built on a cloud native architecture, ATOM leverages microservices to auto-scale as per demand, reducing the software footprint through a pay-per-use model. The modular design also supports both SaaS and on-premises delivery models while ensuring massive scaling, disaster recovery (DR), and geo-redundancy with high availability. Additionally, the unified platform architecture with multi-tenancy capabilities is accessed with a Single Sign-On (SSO) for secure access control.

Integrations: ATOM provides best-in-class integration support, with adapters for all the popular IT systems and network technologies to build custom Integrations quickly. The

out-of-the-box controller integration leverages ITSM, IPAM, and CI/CD tools to seamlessly integrate campus, WAN, and data center controllers, supporting over 60 vendor platforms without a hitch. It also integrates with various external systems and tools, including Slack, external scripts, inventory, and assurance systems.

Use Case Examples

Delving deeper into some of the Cross-Domain use cases ATOM supports–

End-to-End Segmentation and Consistent Policy Enforcement Across Campus

Overview: In Cisco SD-Access Fabric Sites, segmentation is achieved using Virtual Networks (VNs) and Cisco TrustSec Scalable Group Tags (SGTs). VNs enable macro-segmentation, while SGTs enable micro-segmentation within the VN.

When SD-Access Fabric sites are connected via SD-WAN fabric, these segmentation constructs must be propagated across the WAN fabric to maintain end-to-end segmentation and enforce policies consistently across multiple sites.

In an Independent Domain Deployment, the SD-WAN controllers and Cisco DNA Center are not integrated. The SD-Access Border Node roles are deployed on one set of network devices, while the SD-WAN Edge functionality is deployed on a separate set of network devices. The SD-Access components are managed independently by Cisco DNA Center, and Cisco SD-WAN components are managed independently by the vManage controller.

In this deployment,

- VNs in the Cisco SD-Access Border devices are mapped to the corresponding service VPNs on the WAN Edge devices to extend the macro-segmentation.
- SGTs are carried from the Cisco SD-Access Border devices to the WAN Edge devices on the Layer 3 handoff interface with additional Cisco TrustSec Inline configuration to extend the micro-segmentation.

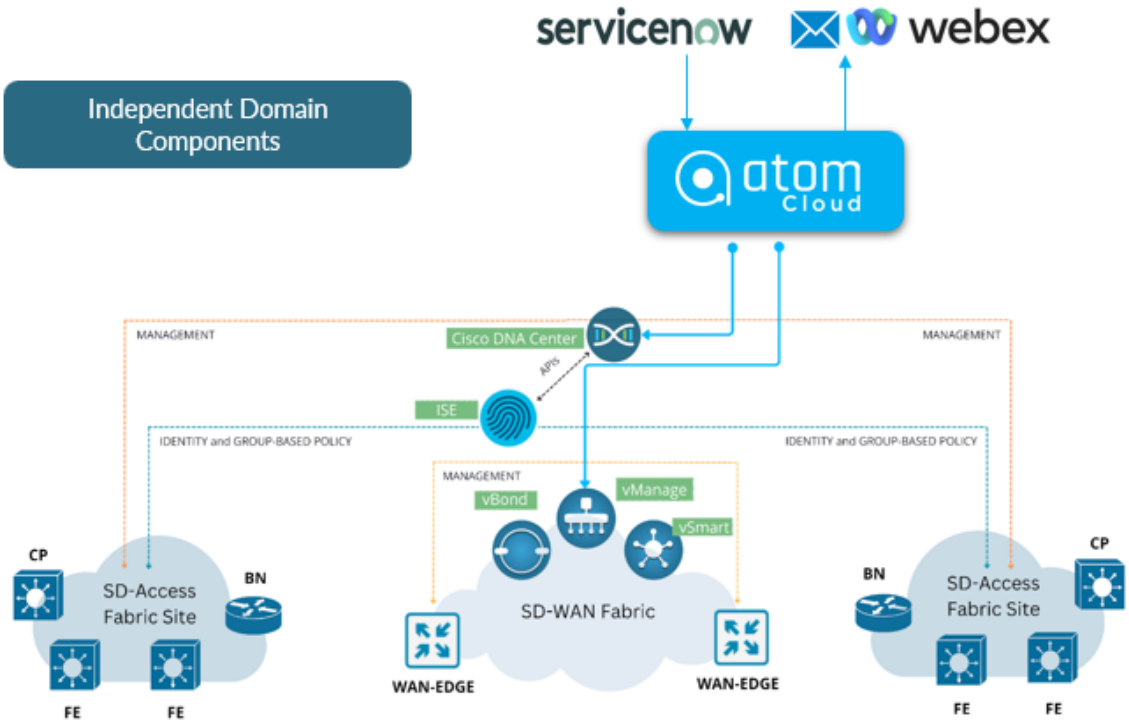
Solution: To enable end-to-end segmentation and thus ensure consistent policy enforcement, ATOM integrates with

- Cisco SD-Access DNA Center to enable TrustSec configs on the SD-Access border nodes L3 handoff interfaces.

- Cisco SD-WAN vManage Controller to enable TrustSec configs on the WAN Edge interfaces.
- Additionally, ATOM can deploy Group Based Access Policy via Cisco DNA Center

ATOM – External Integrations:

- SD-Access Controller: Cisco DNA Center
- SD-WAN Controller: Cisco vManage
- ITSM: ServiceNow
- ChatOps: Cisco Webex Spaces, Email

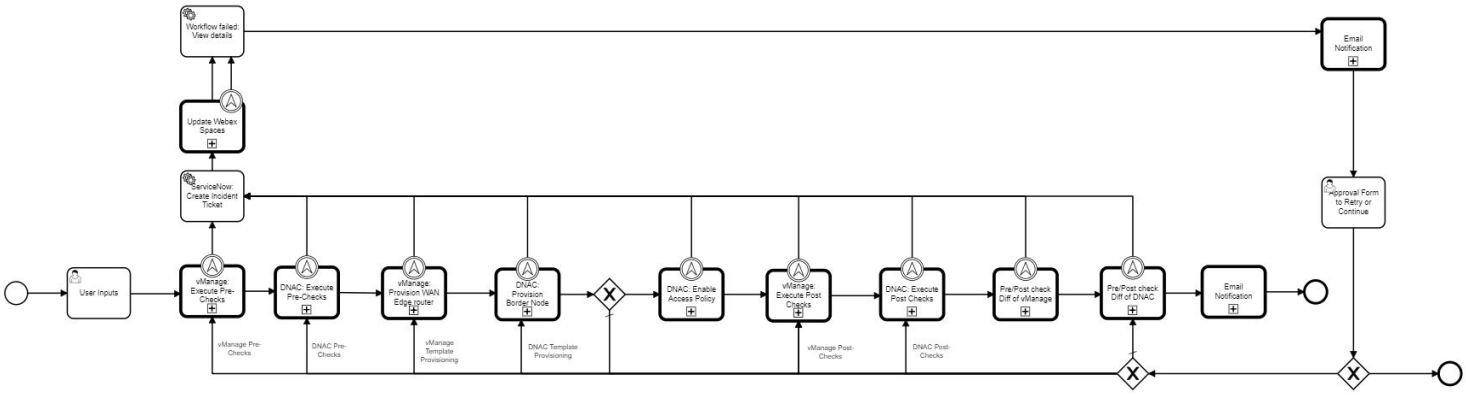


Cross-domain Automation:

Network Operator initiates the process automation in ATOM, and the following steps are executed.

1. Open Change Request in ITSM Tool (ServiceNow)
2. Execute Pre-checks on SD-Access and SD-WAN devices
3. Push TrustSec Configs on WAN-Edges through vManage SD-WAN Controller to maintain end-to-end segmentation

4. Push TrustSec Configs on Border Nodes through Cisco DNA Center SD-Access Controller to maintain end-to-end segmentation
5. Push Group Based on Access Policies through Cisco DNA Center
6. Execute Post Checks on SD-Access and SD-WAN devices
7. Perform Pre / Post check validations
8. Notify Change status through Email and Cisco Webex Spaces
9. Update and close Change Request in ITSM Tool (ServiceNow)



ATOM Value Add: A single-pane-of-glass for SD-Access (Cisco DNAC) and SD-WAN (Cisco vManage), providing a consolidated and real-time view of all devices.

Automated Policy Update for SD-WAN from ITSM

Overview: Cisco SD-WAN centralized control policy is a policy that manipulates the route and Transport Locator (TLOC) information that is exchanged between the vSmart controllers and the vEdge devices in the Cisco SD-WAN overlay fabric. It can also influence the overlay topology of IPsec tunnels and the routing paths through the fabric.

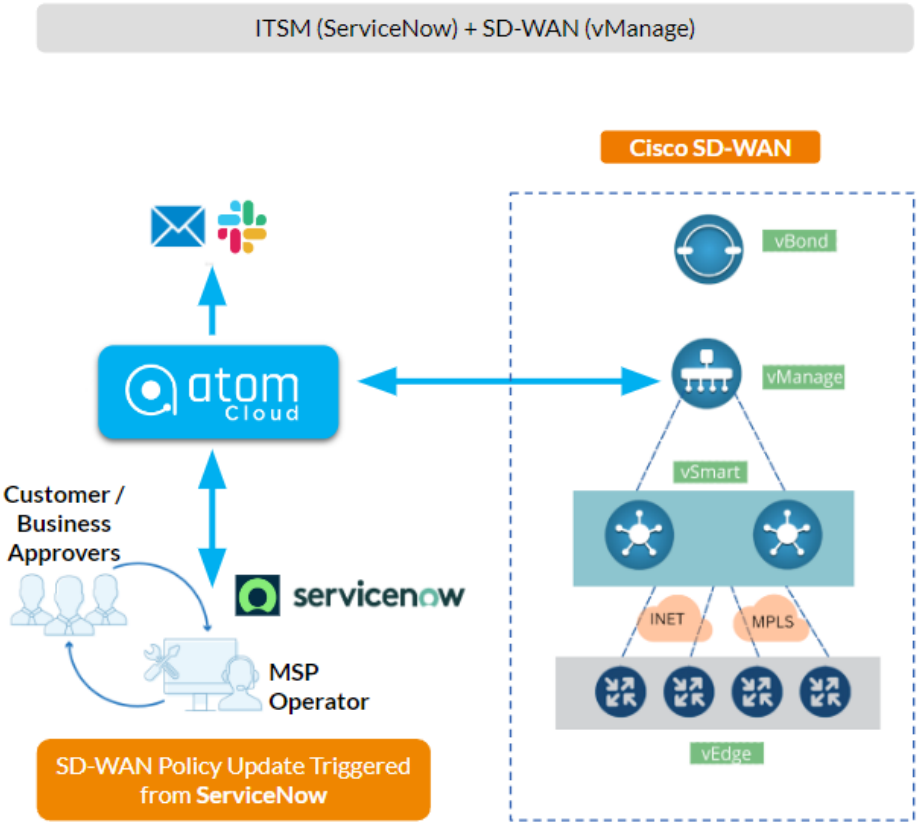
In the event of a network brownout or software failure, the traffic policy can be manipulated to divert the traffic to another path.

Solution: In this use case, the network operations team receives an alert about a network outage, and an incident ticket is opened in the ITSM system - ServiceNow. The incident

ticket in ServiceNow invokes ATOM process automation flow. ATOM integrates with Cisco SD-WAN Controller - vManage to update the routing policy to influence the traffic flow.

ATOM - External Integrations:

- SD-WAN Controller: Cisco vManage
- ITSM: ServiceNow
- ChatOps: Slack, Email

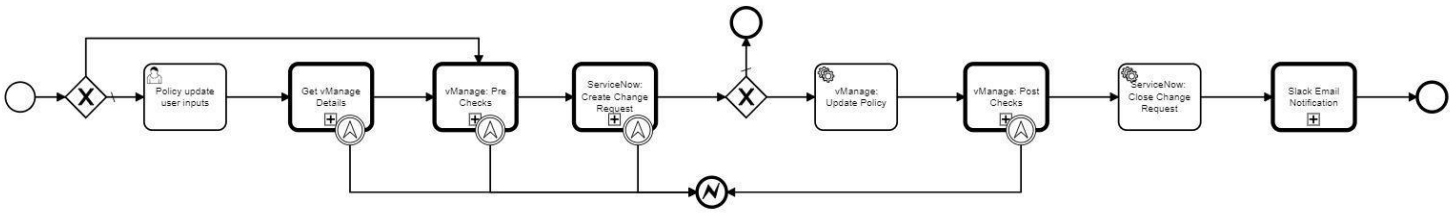


Cross-domain Automation:

Network Operations team Invokes ATOM Policy Automation from ITSM (ServiceNow) as part of an Incident Ticket, and the following steps are executed.

1. Open Change Request in ITSM Tool (ServiceNow)
2. Change Request is approved by Stakeholders
3. Execute Pre-checks on SD-WAN Fabric

4. Push Policy update to the Fabric via vManage SD-WAN Controller
5. Execute Post-checks on SD-WAN Fabric
6. Perform Pre / Post check validations
7. Notify Change status through Email and Slack
8. Update and close Change Request in ITSM (ServiceNow)
9. Update Incident Ticket in ITSM (ServiceNow)



ATOM Value Add: Streamlining the ServiceNow UX with powerful automation, ATOM can expedite new requests and services. This results in faster time to revenues, reduced operating expenses (OpEx), minimized manual errors and decreased associated network downtimes.

Accelerated Application Access across Campus and Data Center

Overview: Cisco SD-Access sites use Scalable Group Tags (SGTs) to enable granular access policies. Similarly, Cisco SDN-Data Centers use End Point Groups (EPGs) to enforce isolation and granular policy enforcement.

Solution: When Cisco ISE in SD-Access is integrated with the Cisco APIC controller in SDN-DC, the SGTs in SD-Access are propagated to the Data Center and will be visible as External EPGs to APIC controllers.

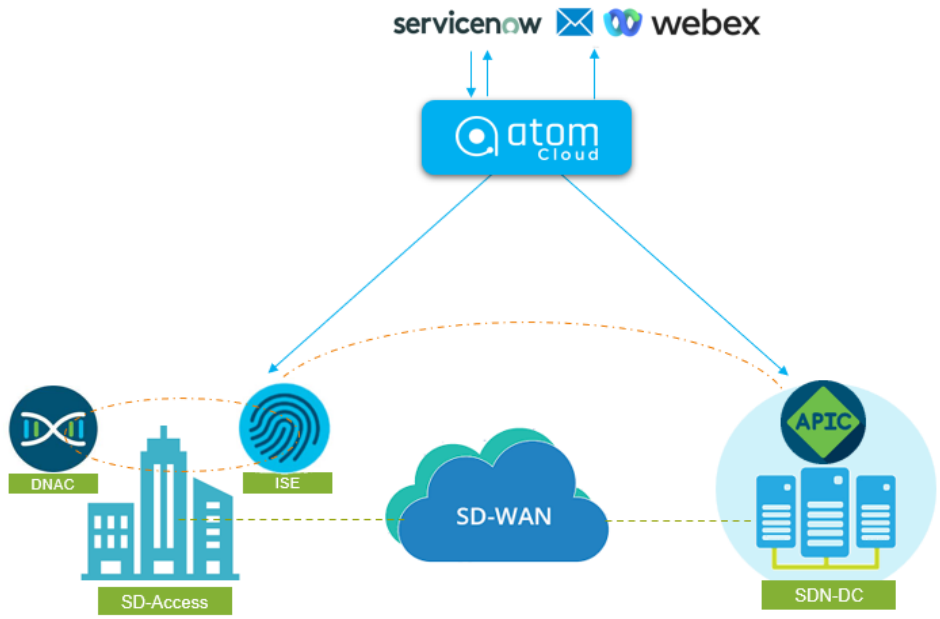
Data Center Application access to new user groups (i.e., new SGTs) can be provided using the SDN-DC APIC controller by mapping these user SGTs (visible as External EPGs) and Application EPGs.

To enable the creation of new user groups and provide access to applications in Data Center, ATOM integrates with:

- Cisco SD-Access DNA Center to create new user groups (SGTs). Cisco ISE is integrated with Cisco DNA Center. SGT creation on Cisco ISE can be achieved through Cisco DNA Center
- Cisco SDN-DC APIC controller to deploy policies to enable application access to the new user groups

ATOM - External Integrations:

- SD-Access Controller: Cisco DNA Center
- SDN-DC Controller: Cisco APIC Controller
- ITSM: ServiceNow
- ChatOps: Cisco Webex Spaces, Email

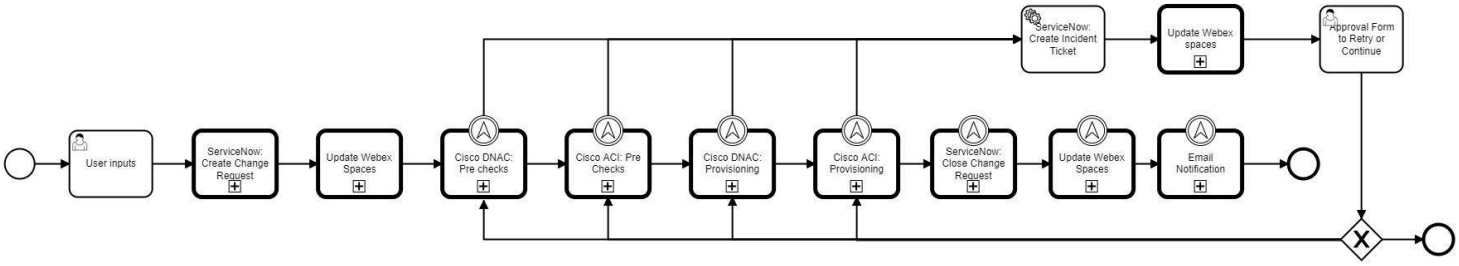


Cross-domain Automation:

Network Operator initiates the process automation in ATOM, and the following steps are executed.

1. Open Change Request in ITSM Tool (ServiceNow)
2. Execute Pre-checks on SD-Access and SDN-DC Fabrics
3. Create a new user group (i.e., SGTs) on Cisco ISE via Cisco DNA Center
4. Create an application policy to enable access between the user group (External EPG) and Application EPG via Cisco APIC Controller

5. Execute Post Checks on SD-Access and SDN-DC Fabrics
6. Notify Change status through Email and Cisco Webex Spaces
7. Update and close Change Request in ITSM Tool (ServiceNow)



ATOM Value Add: ATOM's ability to allow administrators to manage both SD-Access and SDN-DC environments from one location reduces complexity and improves productivity.

Rapid onboarding of SD-WAN Branch (Cisco Meraki)

Overview: On-boarding SD-WAN involves configuration steps, centralized cloud-based management, and automatic provisioning of network devices. Ensuring stable and reliable connectivity between the branch office and the central management system can be challenging, especially if network misconfigurations or hardware issues exist.

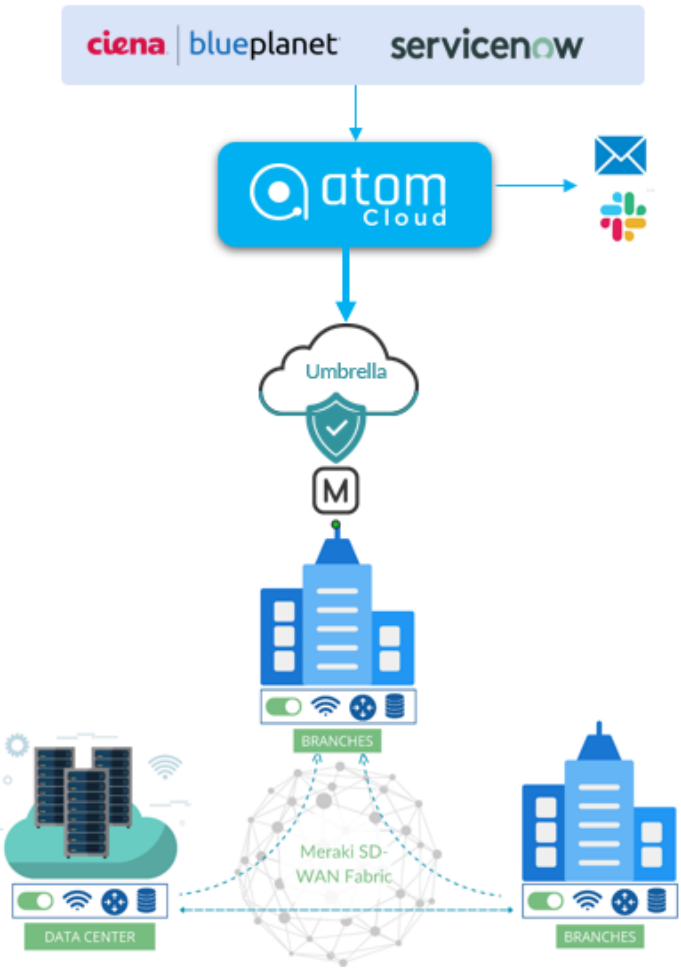
Solution: ATOM automates the complete SD-WAN Branch onboarding process. Its integration ensures that the branch router is delivered onsite. IP addresses for the branch are reserved in the NetBox IPAM system. After completing these steps, it is integrated with the Cisco Meraki SD-WAN controller to onboard the branch.

ATOM - External Integrations:

- SD-WAN Controller: Cisco Meraki
- ITSM: ServiceNow
- IPAM: NetBox
- Asset Inventory: Blue Planet Inventory
- ChatOps: Slack, Email

Solution Brief

anuta networks

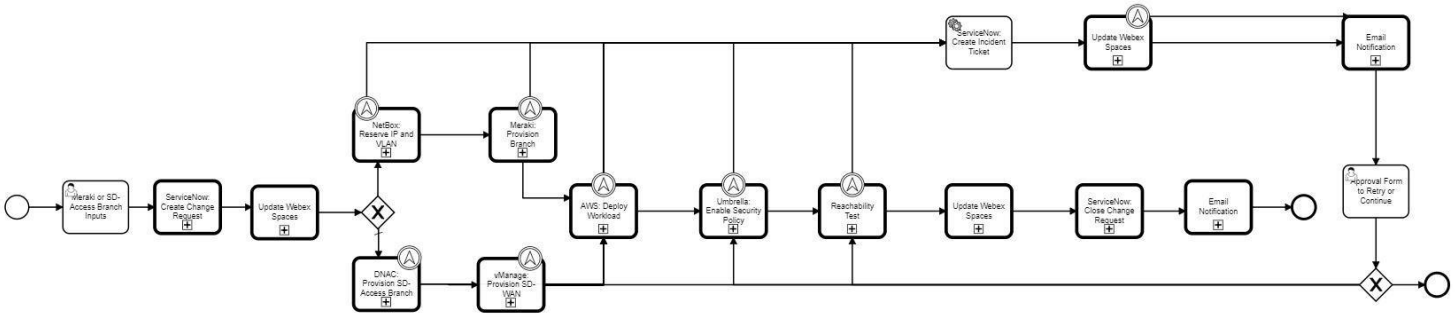


Cross-domain Automation:

Network Operator initiates the process automation in ATOM, and the following steps are executed.

1. Opens ITSM Change request ticket on Service now
2. Identify the Physical asset tracking in FedEx
3. Reserves Branch IP subnet from NetBox IPAM
4. Change start notification (Slack, Email)
5. Pre-Check policy
6. Branch onboarding provision via Meraki Controller
7. Post Check the policy
8. Trigger Branch Monitoring
9. Change complete notification (Slack, Email)

10. Close ITSM change request ticket on Service now



ATOM Value Add: ATOM provides complete, end-to-end automation for the SD-WAN branch onboarding process involving integration with multiple systems, branch network configurations, and pre & post-check verifications.

Conclusion

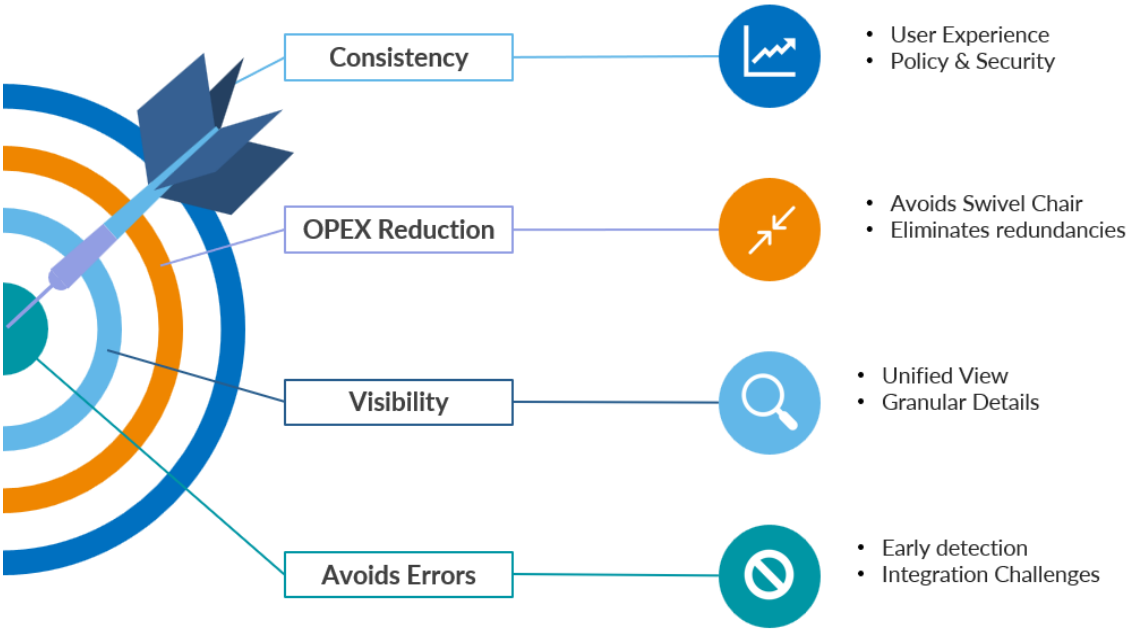
ATOM, a flexible Cross-Domain Automation (CDA) platform, delivers high value and agility to enterprises of all sizes. It effortlessly integrates with existing infrastructure and can be deployed in the cloud, on-premises, or a combination of both.

ATOM extends its automation capabilities to legacy devices, offering features like Active Assurance, Config Management, Compliance, and Service Orchestration. It also includes Network Management capabilities with distributed collectors, observability, and closed-loop automation for effective infrastructure monitoring and remediation.

The ATOM framework provides unified network and security management, incorporating features such as SASE (Secure Access Service Edge), centralized policy management, and a unified user experience.

Solution Brief

anuta networks



ATOM is a powerful automation tool that can be used for complex scenarios, enabling the rapid and effortless integration of diverse systems. By reducing the need for multiple management tools and interfaces, organizations can save on licensing costs, reduce the overall IT infrastructure footprint and save money.

With ATOM, the focus shifts from building domain-specific solutions to constructing cross-domain use cases with organized network infrastructure management and efficiency. That is a powerful consideration, given the challenges tied to managing IT silos in the past.