SALTSTACK | IBM Cloud

IBM Cloud Customer Spotlight

Event-Driven Security & Control for Network Infrastructure at Scale

SUMMARY

IBM uses SaltStack as a global command and control layer that provides comprehensive audit, remote execution, automation, patch, and security detection and remediation for the IBM Cloud network.

RESULTS

Global network control from a single platform

19 work years saved on first project alone

75% reduction in manual tasks with security automation

SOLUTION

- Global SDN principles applied through SaltStack command and control layer
- firmware updates to 70,000 physical network devices via event-driven orchestration
- Automation of significant compliance workflow bottlenecks.

CONTENTS

Introduction

While SaltStack is best known as an IT infrastructure automation platform, it is also a powerful solution for controlling and securing network infrastructure at scale.

Network engineering and operations teams are turning to SaltStack because of its ability to abstract away underlying network device components and manage all data center infrastructure with a single platform. SaltStack also provides constant visibility and control (with or without an agent) and provides remote execution of commands, configuration management, and automated security and continuous compliance at scale.

This paper will explore how the network engineering team at IBM Cloud uses SaltStack to control and secure a diverse collection of more than 75,000 network devices across 80 sites world wide.

IBM Cloud Network Use Case Overview

Challenge: Outdated legacy networks and constant growth

The IBM Cloud network team is a relatively small group of highly-skilled network engineers who are responsible for supporting a large, high-growth digital environment. In 2018 alone, IBM Cloud grew its network by more than 20,000 unique devices.

Due to this explosive growth the IBM Cloud network team was constantly building up and out, unable to spend sprints updating and improving older data centers.

In order to maintain the resiliency and security the business demanded, they needed to use automation to amplify their engineers' abilities and bring their diverse network portfolio under centralized control.

Solution: Automated network control and security with SaltStack

After an intensive search, the network team at IBM Cloud decided to use SaltStack to update all of their legacy data centers and then automate the ongoing security and control of all 75,000 physical network devices.

The remainder of this paper will detail the steps they took to achieve this, the outcomes for both the team and the business as a whole, and what's next for IBM Cloud and SaltStack.

> "SaltStack gives us the ability to centrally manage all of our devices and programmatically configure them. Now we can get out of the business of having network engineers log in to devices individually to make changes and possibly make mistakes that are damaging to our customer experience."
>
> **Nathan Newton**
> *Network Development Lead at IBM Cloud*

Applying SDN to Physical Networks

One of the primary goals for the IBM Cloud team was to apply a software-defined network layer over their existing physical infrastructure. Doing so would allow them to centrally manage, programmatically configure, quickly audit, and easily update all of their physical infrastructure.

However, like many large enterprises with expansive hardware investments, the IBM Cloud network was built on a wide array of physical devices. Approximately half of IBM Cloud's 75,000 devices were various generations of Cisco NX-OS. The remaining half consisted of mostly Arista and Juniper devices, with a mix of Fortinet, Array, Palo Alto Networks, and others sprinkled in.

In order to apply SDN control over an environment so diverse, IBM Cloud needed a platform that was extremely flexible and massively extensible. Enter SaltStack.

Flexible control options

SaltStack offered multiple control options that IBM Cloud networking could use in unison to achieve global network control.

The first control method was running a SaltStack agent—called a Salt Minion—directly on box. Arista EOS already offered a native Salt Minion on box. The lightweight nature of the Minion allowed deployment on virtually anything that could run a Linux distribution.

Still, many of IBM Cloud's devices had hardware and software limitations that did not allow a Minion to be installed locally.

The next method was to use Salt-SSH to connect to and make changes on the device without an agent. While this method was helpful for certain ad hoc jobs, the temporary nature of an SSH connection and the fact that it required ports to remain open on the device disqualified it as a ongoing management option.

The final method, which proved to be the most effective for broad control, was through an API-driven Salt Proxy Minion.

Abstracted control for all

The Salt Proxy Minion operates by designating a single server (VM or cloud instance) to act as a proxy agent for thousands of network devices and communicates with them through an API powered by the NAPALM Python library. In addition to standard NAPALM support for EOS, NX-OS, and JunOS, SaltStack includes additional out-of-the-box network modules that deepen and enhance network device control.

The IBM Cloud network team used the SaltStack Enterprise API framework to control all Salt Masters from a single location. This meant, from an operational standpoint, Salt Proxy Minions could be controlled in exactly the same way as traditional Minions. This allowed the team to control all devices centrally and combine the full benefits of an agent with the flexibility of agentless.

Orchestrating Firmware Updates

One of the main SaltStack differentiators over legacy automation tools is its ability to perform event-driven automation and orchestration.

The IBM Cloud network team used this functionality to update firmware across tens of thousands of outdated legacy devices while minimizing disruption to live customer environments.

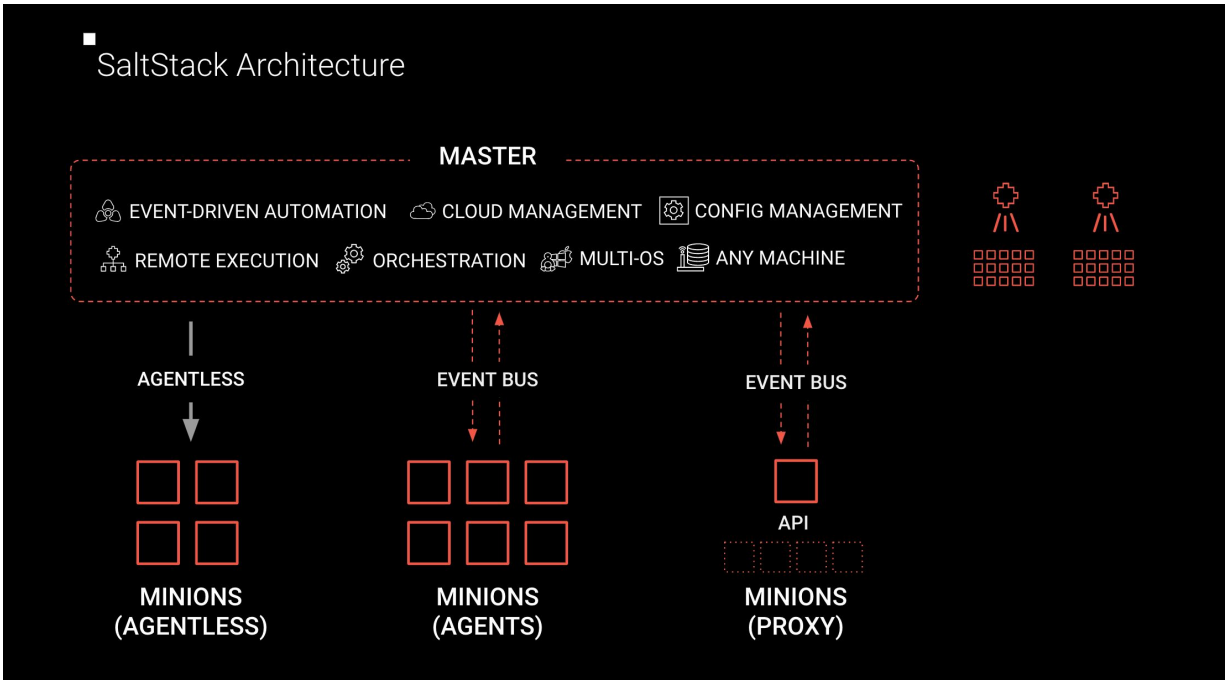
One does not simply upgrade to the latest version

In order to upgrade legacy switches and routers, certain key firmware versions had to be deployed in sequence.

To add to the challenge, this had to be done with minimal impact on production traffic. To accomplish this, the IBM Cloud team worked with SaltStack professional services engineers to create an event-orchestrated sequence that would coordinate upgrades between A/B pairs. In some cases 13 individual steps needed to be performed to bring a device up to the appropriate code level.

Event-driven testing and execution

Rather than set the upgrade orchestration sequence loose on a production network, the network team used SaltStack native, event-driven automation capabilities to build careful testing into the upgrade sequence. These tests would run within a controlled environment between each phase of the A/B upgrade.



Event-driven testing and execution (continued)

As each test passed, SaltStack software detects the event and deploys the next firmware upgrade automatically. While almost the entire process was performed autonomously, the SaltStack event bus allowed network engineers to monitor the process in real time and intervene if ever a test failed or a sequence timed out.

The results

By harnessing SaltStack event-driven automation and orchestration capabilities to perform upgrades, critical networks were secured in just a few weeks. The network team saved more than 40,000 hours of labor (19 work years) and the need for customer notifications, midnight maintenance windows, and customer downtime were all eliminated.

> "SaltStack forms the basis of a comprehensive audit, remote execution, configuration management, patch, and baseline enforcement suite for the IBM Cloud network. This has replaced several disparate legacy tools with a single command and control layer that allows us to automatically roll out new security policies and quickly react to any new security threats. Problem scoping, mitigation, and audit is done in hours rather than weeks across our network."
>
> **Brian Armstrong**
> *IBM Cloud Network Executive*

Driving Efficient Governance with "NetSecOps"

Once the IBM Cloud network team had proven the power of SaltStack, they immediately began to look for the next area of the business where it could make an impact.

Automating continuous compliance

The IBM Cloud network governance team is a small group responsible for investigating and remediating approximately 1,000 compliance and vulnerability issues that were discovered every day by network security scanning tools. Specifically, when the team received a notification from the monitoring tool they would open a ticket in Jira, investigate the issue, determine legitimacy, assign a priority, remediate any critical issues, and disposition the ticket. This process took about 90% of the team's dedicated time.

The governance team attended a two-week SaltStack introductory training and, immediately following, started using SaltStack to automate their governance processes.

They used the robust SaltStack third-party integration library to automate the creation of Jira tickets, then they deployed SaltStack SecOps, an add-on module for continuous compliance and vulnerability remediation, to detect validity of the issue. When a deviation from the predefined policy is detected, SaltStack SecOps remediates the issue automatically.

Automating continuous compliance (continued)

If the issue required more human involvement, then SaltStack would send a notification to the team, allowing them to explore and address the issue directly. Finally, SaltStack kept a complete data record and pre-built dashboards used by leadership to audit current compliance levels and network changes.

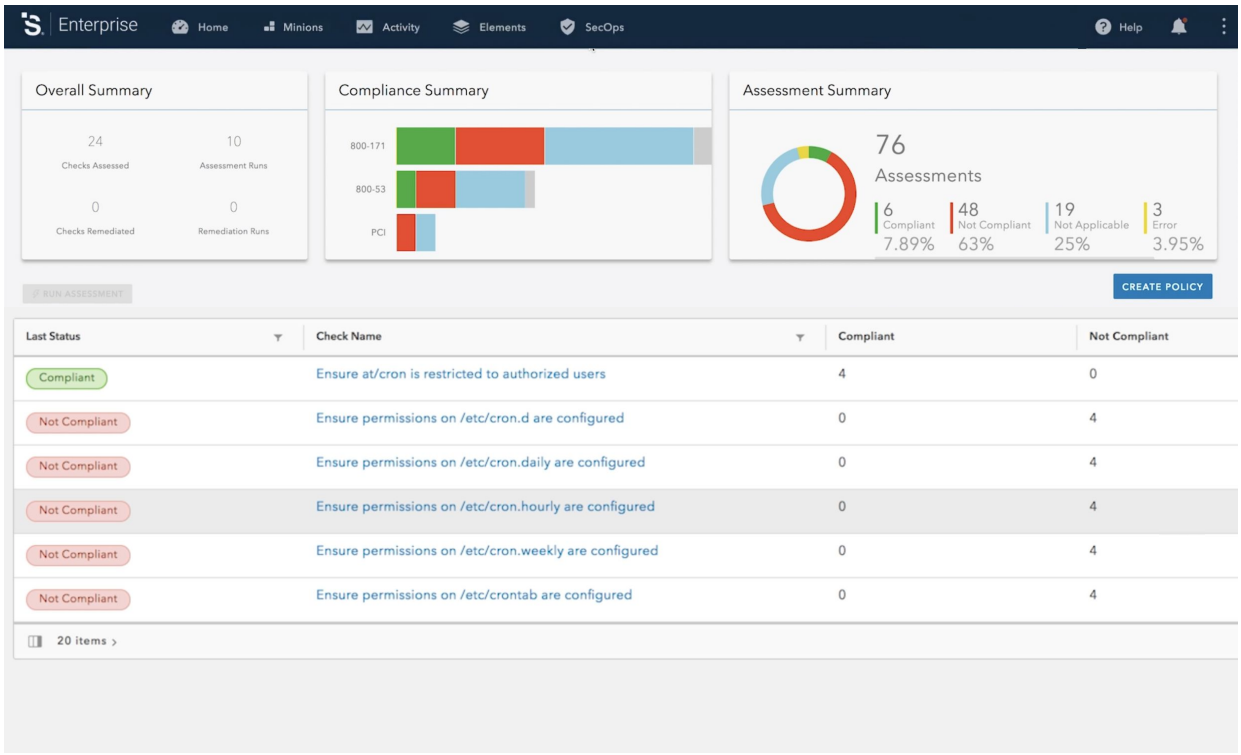
The results

By applying SaltStack intelligent orchestration and utilizing SaltStack SecOps, the governance team reduced their workload by 75%. This allowed them to automate away reactionary, repetitive work and, instead, focus on preventative strategic projects to improve the company's network security posture.

"After applying SaltStack SecOps automation and orchestration to our existing governance processes we are seeing dramatic improvements in team and tooling efficiency.

"For example, we've seen a 75% reduction in the work simply needed to coordinate priorities between our security and IT operations teams. SaltStack SecOps will be the catalyst to helping IBM Cloud achieve the goal of continuous compliance while optimizing collaboration and output between our global security, IT, and governance teams."

Stephen Dumesnil
IBM Cloud Network Engineering Governance Manager



SaltStack + Cisco for Event-Driven Data Center Automation

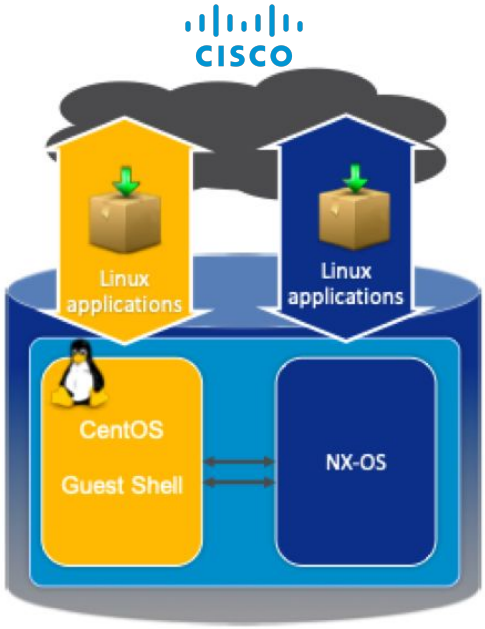
While the SaltStack Proxy Minion architecture provided the IBM Cloud team with powerful flexibility to manage their diverse device landscape, there are certain considerations for managing Proxies at large scale. Since many of the IBM Cloud network devices were provided by Cisco they reached out to the Cisco NX-OS development team to see if they could help provide a solution.

Cisco realized the obvious benefit of providing a native Salt Minion for IBM Cloud, along with many of their other customers, and partnered with SaltStack engineering to create a solution.

> "Cisco is working closely with customers to optimize IT infrastructure uptime and simplify operations through intent-based network fabric automation. Support for SaltStack event-driven automation with Cisco NX-OS provides customers an option to manage large-scale Nexus fabrics in a programmatic way, from defining configurations to monitoring and remediating issues."
>
> **Thomas Scheibe**
> *Vice President, Cisco Data Center*

Cisco NX-OS provides an open abstraction layer that allows Salt Minions to be hosted on Nexus switches within the guestshell, or as part of an off-box solution, leveraging the Salt Proxy Minion.

Joint SaltStack and Cisco customers can now manage the entire Nexus portfolio through a common SaltStack interface, enabling end-to-end automation. By providing a common simplified solution, IT teams can focus on innovating and optimizing network up-times, minimizing downtime and increasing end user satisfaction.



Conclusion

SaltStack is a powerful automation platform for the entire, modern data center. As the digital business landscape continues to evolve, it is critical for organizations of every size to harness automation to manage and secure their business-critical networks and the infrastructure and applications they support.

SaltStack, Inc.
2801 N. Thanksgiving Way, Suite 150
Lehi, UT 84043
USA

+1 801.207.7440
info@saltstack.com
www.saltstack.com
Produced in the United States of America