anuta networks

Master Network Compliance

The Easy and Thorough Way

A Snapshot of key steps to comprehend Network Compliance:

anuta networks

Network Compliance:

In the current age of agile business services where customers have got used to the push-thumb speed and frictionless experiences, it is hard to find any enterprise that is not considering investments into faster and more robust networks. But these investments cannot be merely about speed, invisibility, and customer outcomes. These new changes have to dovetail well with the compliance side of network IT as well. Brace up on the inevitable needs of network compliance by understanding its reasons and areas of action.

What is regulatory compliance?

Regulatory compliance lists out specific guidelines to ensure security, reduce risk, and improve governance. It is an essential part of bolstering the safety aspects of lightning-fast networks. Organizations have to adhere to compliance standards strictly. Any violation here can have monetary and reputation implications.

Some commonly-followed compliance mandates that intersect with network ambit due to the industry-context are:

HIPAA

HIPAA, the "Health Insurance Portability and Accountability Act," is the governing standard for all medical facilities dealing with patient information. It is designed to fight discrimination based on health status and to ensure that sensitive medical data is protected and well-under the patient's control.

PCI

PCI (Payment Card Industry) 's primary goal is to create a compliance standard to ensure any company that is accepting credit cards is properly securing the data collected on customers. Any merchant accepting credit cards is required by law to adhere to PCI compliance and is susceptible to audits by the PCI governing body

SOX

The SOX (Sarbanes-Oxley Act) requires corporations to create internal standards and procedures for handling and reporting financial information. From an IT perspective, the configuration of the entire demonstrates compliance with every aspect of SOX.

Organizational Compliance

In addition to the above, organizations may also define policies for better management of risk. All units within the organization must follow the organizational compliance policies that are applicable and relevant.

Let's now ask - What is network compliance?

Ensuring consistent configuration and security of the network while it meets various compliance standards constitutes a proper stance of network compliance. The high-level compliance policies have to be broken down into multiple granular network policies. The network should always adhere to the network compliance policies by fixing any non-compliance automatically. Network compliance deals with monitoring network policies, alerting non-compliance, and automatically remediating violations. It may look like an area of additional effort, but it is a very critical part of today's business environment.

Why is non-compliance not an option? Why can it not be cursory?

Many companies have detailed data and network compliance policies, but are these enough? Even with a well-defined process, services and devices often become non-compliant for a variety of reasons. An improper change in a router or firewall can trigger a non-compliant network policy and could result in unauthorized access to sensitive data. A change in ACL (Access Control List) or opening of ports in a firewall to accommodate a new application can be non-compliant to application onboarding policy and enables invisible backdoor access to your network. Non-compliance with security policies by failing to upgrade your software or firmware to the latest release versions creates a security gap and increases the likelihood of massive data thefts. Such issues are adequate to cost your enterprise enormous damage even if one error backfires or one loop-hole accommodates bad actors. Other red flags, of course, envelope this aspect.

Severe fines and penalties

Penalties form another deterrent that can be a strong reason for making sure that networks comply well with the rules and caution they need to embrace. Based on the severity of the violation, non-compliance can cost the organization anywhere from hundreds of dollars to millions of dollars. Not just that, the service provider in question may be banned from providing services for many years. Depending on the severity of breach fraud, strong and punitive criminal actions can also be undertaken. Additionally, the authorities may even confiscate the infringing products.

Loss of reputation and revenue

According to a study, the average cost of non-compliance to an organization is around $14.82 million. Failing to comply with regulations not just causes financial losses but also wrecks reputation, which is very difficult to rebuild. Loss of reputation leads to a domino-effect - loss of profit and market share and more. Plus, it personally affects those in charge of the business. The reputation of not only the business but also the CEO or CRO (chief risk officer) could be at stake in light of the new and evolved regulatory environment that has come up.

The ever-slippery customer confidence

Consumer trust in business is extremely critical. Customers need to feel confident that their financial and sensitive details are safe when parting with them over the phone and online. The bottom line is that if the public does not trust your brand, the customers you yearn aren't going to give you their trust. Compliance with regulatory bodies instills trust and confidence in customers towards the brand and company. It is not just an extra pile of paperwork but the building brick of ultimate customer loyalty and reliability of your enterprise.

Barriers to achieving network compliance

As much as you dream of it or as much as some iffy providers deceive you into believing it – network compliance is not a one-push magic switch. It takes perseverance, clarity, workforce, strategic planning, and patience. A lot can go wrong on this path. A lot has to be anticipated and pre-empted while designing and executing rigorous network compliance.

Manual, error-prone audits

Network administrators use a variety of tools to monitor their environments. They wield these for quick alerts on policy violations. However, most of these tools lack any interoperability. In most cases, administrators have to, still, manually collect data from various tools, analyze data relations, identify non-compliance, and take remediation- steps with their own hands. It's ok to do the audit as a one-time exercise, but it is difficult and exhausting to maintain the compliance status eternally. Automation helps. A lot.

Lack of standardization

Network operations are complex. Upgrading an OS on a network device, for e.g., is a long and tedious process. Though organizations have written proper methods of procedures for every network operations, they are not following these as sincerely and comprehensively as they should. Mistakes while following MOPs (Method of Procedures) are bound to spill over. Typically, configuration scripts are stored in various IT workstations. But critical configurations may be missed out while copy-pasting from older config files. Which is why it is critical to have adequate standardization in this realm.

Lack of critical insights

Too many compliance tools bring in too many dashboards. Network administrators have to look through numerous tools, correlate and analyze to identify issues and monitor the network.

If something goes wrong, a correlation between various events across a vast expanse of tools is bound to turn into a nightmare. A single-pane-of-glass is necessary for any enterprise to identify non-compliance swiftly and avoid delay and network fiascos.

Tedious manual configurations and monitoring

Manually configuring devices one by one is time-hogging and difficult. With ever-changing policies, this process becomes even more challenging to manage in an ideal way. The same struggles apply to monitoring. Decentralized monitoring doesn't provide a complete picture as well. Automated config mgmt and monitoring become the key ways here to address these complications and unnecessary interruptions.

Difficult to keep up with the standards

Hackers are smart and persistent. They keep finding new innovative ways to breach security and steal data. That's why the standards have to evolve to mitigate any threats continuously. But keeping track of rapidly-evolving standards is stressful and tedious. Even if standards are followed, it's often difficult to report the compliance activities. By continually updating templates, automation solutions help in keeping up with the standards. Automated reporting helps in maintaining compliance-logs.

Lack of motivation

Highly-skilled network architects and engineers are more interested in performing higher policy-level tasks rather than constantly monitoring compliance-logs. Lack of motivation not only leads to disgruntled employees but also puts the network and business at risk. Automating such tedious, yet critical, tasks is essential for enforcing compliance effectively. It keeps your workforce fresh, excited and spared for the tasks they genuinely enjoy and add value in.

Essentials requirements to achieve compliance

Now that we have an overview of the quintessential need and role of network compliance, let us see how simple the process can be made by deploying the right tools and steps at the right point.

Automated configurations

Eliminate manual and tedious configurations as much as possible. They introduce costly human errors and make trouble-shooting difficult. Automation solutions should push configurations to the network devices automatically.

Low-code policy builder

An essential first step towards holistic compliance is about building effective policies. Heavy coding deters administrators from creating complex policies. They prefer to monitor compliance manually, that leads to further, and riskier, non-compliance. Low-code interactive intuitive frameworks are essential to creating even the most complicated of policies with ease. This irons out the issue of waste time as well as monotony for the human resources who can now save their time and skills for better goals.

Continuous monitoring & in-depth insights

A network has to be monitored continuously for inconsistencies. A single solution answer that is capable of monitoring the entire network and providing intuitive dashboards with collected network data – now that becomes extremely useful to detect non-compliance in a faster manner. In-depth analytics combined with AI/ML may give administrators a prediction edge on future non-compliance as well.

Quick alerts and event correlation

Organizations must address non-compliance immediately. There is no room for laxity or procrastination here. A single issue is potent enough to generate many alarms and events. Searching for the issue within numerous alarms is as complicated and tedious as looking for that proverbial needle in a haystack. Event correlation helps in reducing the number of alarms and pinpointing issues with precision. Alerting, as a process, needs to be quick and immediate. Delay in alerts may lead to significant losses in revenue and reputation.

Segment-Rule enforcement

Various elements of network and business differ in compliance requirements. E.g., compliance in a finance department is different from that of an engineering department. Compliance could also differ by geography or business SLAs (Service-Level Agreements). It should be possible to enforce different rules for different segments of the network.

Clear separation of duties

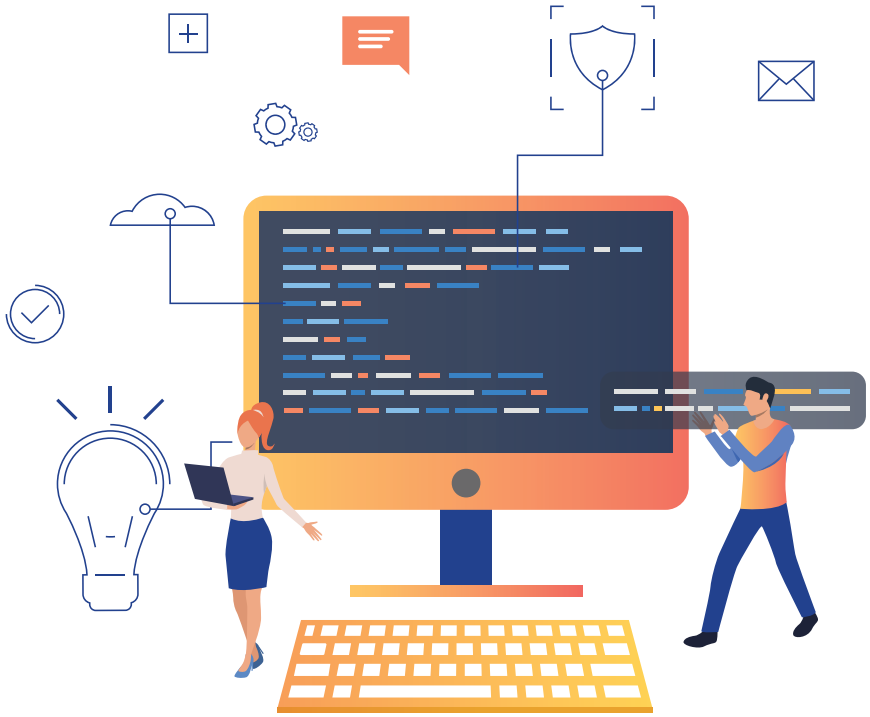
Compliance rules are created with the utmost care and keeping in mind the business efficiencies that need to come into play for an agile environment. Once a network architect creates appropriate rules, operators and network engineers should not have access to modify the policies. Separation of duties across various stakeholders in organizations is an essential but often-neglected area.

Scale and performance

Compliance enforcement should be holistic. The entire network should be monitored with similar policies. It should encompass all network devices. At the same time, compliance checks should be quick to report violations and remediate with appropriate measures. Automated compliance that takes longer than manual checks is useless to the organization.

All the above areas are very critical and need to be addressed with the right solution – something with the capabilities, stronghold, and sharpness that a difficult space like network compliance can use a lot.

Anuta ATOM - The perfect compliance solution

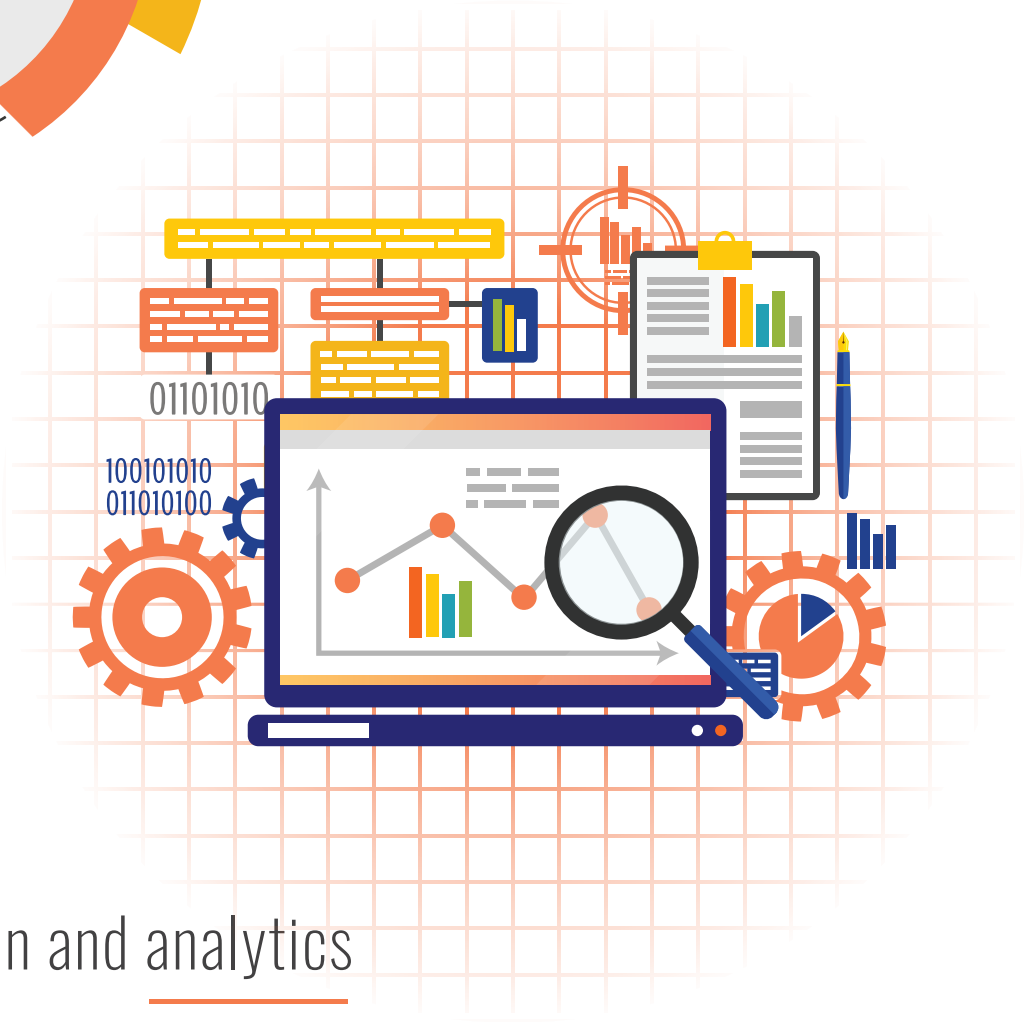


Intuitive-interface to build compliance policies

Intuitive interfaces with low-code automation contribute heavily to define even the most complicated compliance policies with ease. An intuitive graphical user interface to design, deploy, and execute complicated or straightforward network operations is imperative for a right compliance solution. ATOM's low-code designer allows the administrator to configure pre-checks, post-checks, and approval flows. This area plays out in a powerful way when one is dealing with the actual groundwork of compliance and interfaces.

ATOM's compliance solution is not limited to device and service automation. It automates the entire Method of Procedures (MOPs). MOPs include not only network operations but also business processes such as approval flows, operation sequence, and time-of-day executions. The low-code designer utility should enable administrators and architects to incorporate all these features and create an end-to-end business policy.

As such, the low-code framework integrates with north-bound entities such as ticketing, billing, and ITSM solutions like Service Now, BMC Remedy, Jira and others, and south-bound entities such as devices, SDN/SD-WAN controllers and cloud technologies such as AWS, GCP. An excellent low-code framework has exhaustive open APIs to integrate with any north- or south-bound elements. The framework is bi-directional, so it can be triggered by the operator or via the alerts from the infrastructure.



Collection and analytics

ATOM has a robust collection and monitoring framework. Operational and performance data from multiple data sources such as SNMP, Streaming telemetry, SNMP traps, and syslog gives deep insights into the network behavior.

An effective collection engine ingests multiple data sets to provide a foundation for a useful monitoring framework. It allows NetOps teams to choose the right data-source based on network requirements such as latency and throughput. A modern stack with a provision to queue messages to meet any contingencies helps to maintain a high availability and ensures THAT NetOps teams do not miss out on any vital information.

The presentation of collected information is vital but challenging as well. Using Grafana and ATOM dashboard, ATOM presents a unified view of alarms, performance-related data derived from multiple data sources; and offers NetOps teams with a single-pane-of-glass to meet all their monitoring requirements. An intuitive and customizable user-interface with the dashboards offering insightful data at a region, network, device, and even interface-level details offers NetOps an opportunity for initial triage as well as deep-troubleshooting.

Continuous and useful feedback from the network is essential to enforce compliance effectively. A lot hinges on the ability of a network to get swift feedback and to wield it in a nimble-footed way to avert major issues and imminent incidents with smart planning.

Alerting/Reporting

Non-compliance has to be detected and remediated instantly. A delay could potentially lead to security breaches of massive consequences and data-theft. Non-compliance to regulatory standards has the potential to not only cause massive financial losses but also reduce organization reputation. There have been many cases in the last two to three years, where despite having a good arsenal of defense, an enterprise suffered business loss because it could not spot a security threat or network issue before it worsened.

Alert-routing capabilities help to alert responsible individuals quickly. ATOM's CLA framework helps detect non-compliance and route alert through email/slack and other means to the correct people.

Non-compliance reporting is a very robust advantage of ATOM. It is what gives it the distinction in a crowded marketplace. Anyone can sell and promise to report, but the speed, coverage, and actionability value of that reporting are paramount. ATOM continuously monitors the entire network for any non-compliance to the predefined policies. It presents a comprehensive report to the network administrators as to which devices are non-compliant and to what policies. ATOM enables network administrators to take quick actions and be on top of their game.

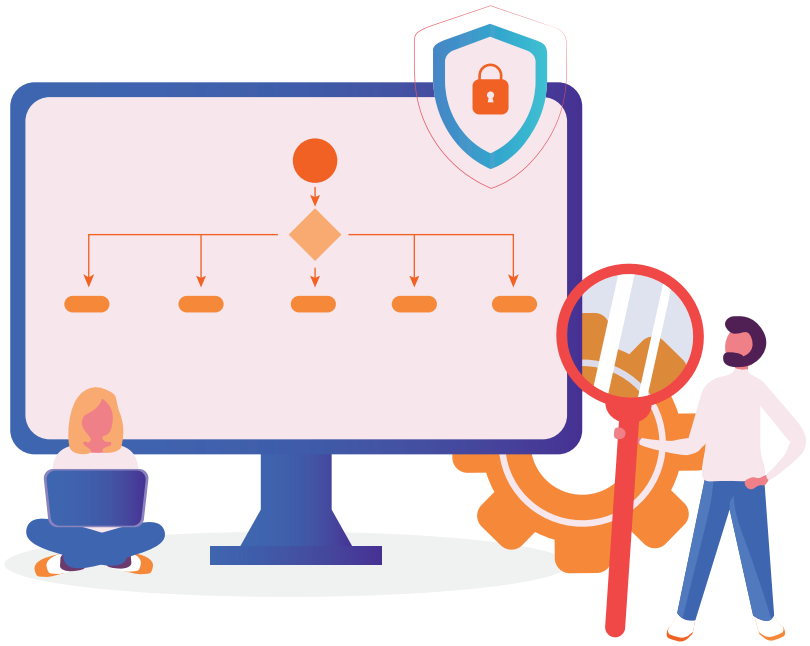
Horizontally-scalable functionality

Networks today are bolstered, and also challenged, by fast-paced technologies such as 5G and IoT serving digital transformation. Organizations are looking to improve service velocity, but are struggling to do so due to the scale and the cost of manual changes to implement service offerings, from installing & provisioning of new network equipment to upgrading an existing one.

Networks have to scale rapidly to keep up with the ever-increasing demands. A monolithic network automation software fails to meet this growing demand from the network. A compliance platform should have the capability to scale horizontally to meet the breadth of any network.

ATOM features a modern software stack packed into micro-services that allows each feature within ATOM to have its lifecycle, so that it can be upgraded without affecting other features, and can be scaled independently. A distributed architecture leveraging cloud-native technologies helps in the placement of ATOM modules closer to the target networks addressing remote-site use-cases without latency issues.

ATOM is a flexible platform that can suit the different scenarios and purposes of various operator environments - A platform that is highly reliable, scalable, secure, and easy to manage.



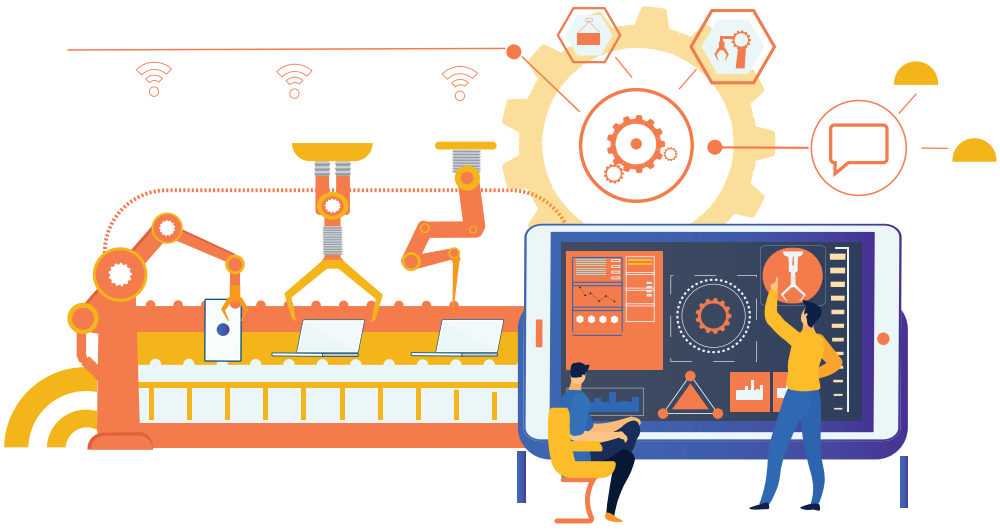
Automated remediation

Another very critical aspect of ATOM is in the remediation area. Enforcement of policies and ensuring the network is always at the desired state is enabled by ATOM's closed-loop automation (CLA) framework. Traditional automation solutions take action based on initial inputs. They do not consider network feedback. The administrator may have specialized tools to monitor the network and get alerted on specific issues. However, the response to the alerts is manual. This process not only causes delays in action but also introduces human errors. It dilutes all the investment and speed that has gone into fast alerts. These areas are pointless if swift action does not follow a red-alert.

Closed-loop automation bridges this gap. ATOM CLA continuously receives feedback from the network and takes appropriate remediation actions – in an automatic and timely way. ATOM CLA works in conjunction with the collection and monitoring framework. The monitoring framework provides real-time metrics indicating the state of the network to CLA. CLA compares the current state to the desired state and, in case of any violation, takes appropriate action automatically.

E.g., say a policy is defined which prescribes that CPU of any device should not exceed 70%. CLA continuously receives feedback from the collection and monitoring framework on the current CPU utilization of all devices. If any device exceeds the set baseline behavior, CLA triggers remediation actions - like say blocking a particular port, or redirecting traffic to another network - automatically.

CLA is an essential component of the right compliance solution. To always enforce the policy defined by the intent, ATOM has a powerful CLA at its core.



Multi-vendor support

Gone are the days of homogenous IT environments. Today's IT infrastructure stacks are anything but amorphous. They entail a broad array of solutions and vendors. Having a diverse IT stack is almost a reality, even for the most old-school enterprises and CIOs. Whether intentional or accidental, the network infrastructure tends to be a multi-vendor one these days. While some organizations try to standardize on one vendor, they often end up with at least 3 or 4 vendors because of business or technical reasons. Being in a multi-vendor scenario avoids the dreaded vendor lock-in and results in enormous savings to the business. ATOM provides robust multi-vendor compliance solution that can support various formats to communicate with devices such as CLI, NETCONF, API, REST CONF, and YANG models.

Network compliance requires a speedy collection and quick interval across various protocols. ATOM is proficient at collecting operational metrics using many formats such as SNMP, SNMP Traps, Syslogs, sFlow, NetFlow as well as Streaming Telemetry. The robust ATOM compliance solution supports the legacy vendors as well as new and upcoming vendors with their new protocol innovations to continue the organization's advantage.

Out-of-box templates

Understanding complex standards and creating policies adhering to those standards may not be a simple task for all organizations. Many enterprises have dedicated compliance teams that set the standards for various departments, but many others just get lost in the complexities.

ATOM provides detailed compliance templates in 'out of the box' strengths, which can be readily deployed and immediately executed. ATOM uses jinja variables within templates to enable architects to reuse templates for various compliance requirements.

RBAC

ATOM's role-based access control helps to arrest business risk and enhance compliance. RBAC helps to segment responsibilities across various stakeholders. Every element in ATOM can be access-controlled and, thus, provides a very in-depth segmentation.

Compliance Use cases with ATOM

Now that we have an overview of the quintessential need and role of network compliance, let us see how simple the process can be made by deploying the right tools and steps at the right point.

Service and device compliance

Preventing unwarranted configuration changes to devices and services either by some third-party application or manually is critical to ensure security and compliance of the network. CLA framework helps detect unauthorized modifications and reverts to the desired configuration automatically. Constant monitoring for changes prevents fraudulent activities and enhances network security. The execution alacrity and surety that a useful tool allows – it merely lifts the entire situation from an evasive one to something where an enterprise can proceed with utmost confidence. Because it is not looking over its back all the time.

Any out-of-band change to the configuration of the device is detected immediately by the ATOM platform. ATOM flags the change and requests for reconciliation. The operator can decide to either accept the changes or reverts them by pushing the original config. ATOM helps to maintain compliance with zero-touch provisioning.

Configuration versioning and comparison

ATOM's Network Configuration Manager is capable of automatic version configuration on any change. This strength of comprehensive data versioning equips an enterprise to keep track of any small or large modifications made to configurations. When users are assured of this ability to identify configurations from the oldest to the latest based on its version number – they acquire a new velocity and grip on their networks. Network Configuration Manager makes it easy and quick to view the configuration changes made in a particular version. It also garners better visibility into details like - who made the change along with the exact time of change.

In the Network Configuration Manager, it is possible to study two configuration versions of the same device or different devices with a sharp comparison lens. This is why, when a configuration version of a particular device may start to jump into bad performance abruptly, the users can compare it with the old configuration versions by deploying the "Diff View" option. Now, the admin can have a good view of all the changes. They are better armed to identify undesirable changes and resolve them. All this happens at an unprecedented speed and depth. Another advantage of configuration data versioning is when there is a sudden network outage - here, the users can instantly roll back to the previous configuration version. They don't waste time in starting a configuration from scratch. ATOM arms the enterprise well in the RMA situation too.

Let us also look into how Labelled configurations play out. These are normal-device configurations with a name (label) assigned to them. They help let the users distinguish configurations from one another. They make it easier to find a particular configuration. Any-device configuration can also be attained now for future reference or if one desires a fall-back option. So now, if something goes wrong, it can be associated with a label and consequently acted upon.

For example, we can label a stable configuration as 'Stable' before making a critical change in the configuration. Finding the labeled device is easy in case a mishap occurs. It can be addressed with a quick solution. In the case of multiple configuration backups for a particular device, labeling a configuration also gives the ability to identify a particular configuration among the hundreds of configurations for a specific device quickly.

OS version and update check

Software defects and issues in OS comprise a significant security threat. For network administrators, it is essential to upgrade the device OS to the recommended versions at all times. However, not only monitoring all devices in the entire network is highly demanding, but the upgrade procedure itself is quite laborious. CLA can periodically analyze the OS versions in all devices in the network and notify or even automatically upgrade violated devices. To prevent downtime hassles, CLA can have the flexibility to schedule OS upgrades during off-peak hours with minimum impact on the network.

OS upgrades and RMA have complicated procedures. The workflows comprise not just network devices but also mandate integration with surrounding network elements such as ITSM, ticketing, billing, and other solutions. ATOM's low-code workflow automation makes it easy for the operators to define complicated MOPs and helps in streamlining processes.

Compliance to standards - HIPAA, PCI, SOX

Most companies must follow strict standards, which may include HIPAA, PCI, SOX, and organizational compliance policies. They have to set up baseline configurations and remediate violations. E.g., SNMP strings have to follow a specific format for all devices. With ATOM, it's easy to create templates and not only mandate the presence of specific configurations but also define the formats for those configurations. If a certain configuration/ CLI becomes non-compliant, one can define remediation actions to fix this. ATOM remediates the issues automatically.

Enforce compliance today!

Compliance is essential, and as is evident from the information above. The ATOM platform has rich features to define and enforce network compliance. Do not leave this critical area on the back-burner. Embrace the right toolkit for effective and sincere compliance without wasting any more time or business edge.

Learn more on Anuta networks at

www.anutanetworks.com

Contact Anuta Networks today
for a **FREE DEMO** on network compliance.