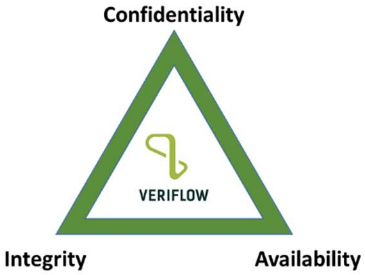
VERIFLOW

Veriflow Enables Continuous and Comprehensive Network Security Compliance

Organizations in all industries implement various information security standards and regulations, such as PCI-DSS and HIPAA, to mitigate financial and reputational risks. These standards include guidelines for implementation of policies to ensure confidentiality, integrity, and availability of information, which also apply to computer networks. Current approaches to verify regulatory and standards compliance include resource-intensive sample-based periodic audits, which fall short of truly mitigating the business risks. Veriflow enables continuous and comprehensive network security compliance using automated mathematical network verification.

Modern businesses rely heavily on information systems to scale their products and service offerings, and to maintain competitive edge. Organizations, both private and public, maintain huge amounts of sensitive data about their intellectual property, business processes, inventories, financials, employees, customers, and market intelligence. Many of these organizations are part of the essential social infrastructure, where business continuity is critical, such as healthcare, law enforcement, banking, transportation, and utilities. Thus, securing the information and systems against breaches and outages is of paramount importance to protect against financial and reputational risks.

Several industry standards and government regulations provide guidelines for information security management relating to confidentiality, integrity, and availability of information, also known as the CIA triad. Confidentiality ensures that only authorized access to information is allowed; integrity ensures that only authorized modification of information is allowed; and availability ensures that information is always available when needed. These guidelines apply whenever information is created, stored, accessed, processed, transmitted, or disposed, both in physical and electronic formats. Organizations define and implement policies to ensure compliance with information security standards and regulations, typically requiring multiple layers of defense, including measures in applications, databases, computers, storage systems, and networks.



The Information Security CIA triad

Challenges of Network Compliance

Communication networks are at the heart of today's technology dependent business infrastructure and operations. The financial and reputational losses due to outages and breaches are astronomical. Thus all security standards place utmost importance on securing the network and ensuring high availability for business continuity.

Organizations need to define and implement policies to comply with the relevant information security standards. These policies must be periodically updated to meet the ongoing business needs and protect against new threats. However, the reality is that most organizations do a poor job of maintaining a pervasive policy repository.

ISO 27001
PCi Security Standards Council
HIPAA Health Insurance Portability & Accountability Act
SOX
FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Well-known Information Security Standards and Regulations

> The true spirit of compliance to information security standards is to always be compliant, not just at the time of audit; and to be holistically compliant, not just in a sampled audited portion.

To validate an organization's readiness to combat threats, and to ensure regulatory compliance, both internal and external audits are performed. The current processes of any compliance audit are time-consuming and resource-intensive, thus very costly. The manual collection and documentation of evidence, even on a sample of a network, is challenging and prone to mistakes.

Modern networks are large and complex, posing great challenges for information security and compliance. They consist of disparate devices from multiple vendors, each with their own anomalies. These network devices run millions of lines of operating system and protocol code that is prone to software defects. They are configured by multiple individuals at different times, causing yet another dimension to the potential of errors, which is the human factor. Since compliance audits are based upon samples, they are not a comprehensive solution to business risk mitigation.

The threat landscape is constantly changing for the worse. In parallel, organizations continually need to modify networks to meet on-going necessities of the business. These changes can be architectural or device specific; at macro level or micro level. Since compliance audits are a periodic process, they are not enough to mitigate business risk at all times.

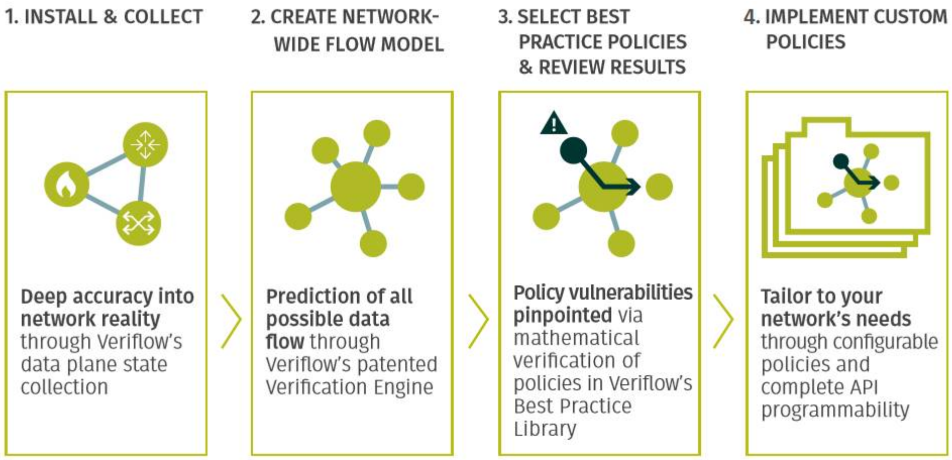
The true spirit of compliance to information security standards is to always be compliant, not just at the time of audit; and to be holistically compliant, not just in a sampled audited portion. Veriflow provides a unique solution that enables continuous and comprehensive network security compliance using automated formal mathematical verification.

The Veriflow Approach

Veriflow has developed a fundamentally new approach to network protection, one based on rigorous, real-time understanding of the network's behavior. By applying mathematical principals of formal verification to complex networks, the company's technology enables enterprises to prevent the outages and breaches that lead to astronomical losses. The core technology emerged from a research breakthrough by a team of computer science professors and Ph.D. students at the University of Illinois at Urbana-Champaign. The resulting technology, now productized by Veriflow, has demonstrated strong success in multiple deployments.

Analyzing data-plane state is fundamentally necessary to provide accurate, comprehensive insights regarding the network's operational correctness, and Veriflow provides the only solution in the market that performs analysis with this level of depth at large scale.

Veriflow's patented approach (US Patent 9,225,601) is unique in its design and scope, unlike legacy techniques such as penetration testing, traffic analysis, or configuration checks. Veriflow solution performs mathematically exhaustive analysis of the entire network's state against a set of broadly-defined policies, and does so proactively before vulnerabilities can be exploited. This approach enables comprehensive insights regarding the network’s operational correctness: if there is a vulnerability in the network, the Veriflow solution will find it and provide precise examples that reveal how to fix the flaw. The underlying technology provides millisecond-level analysis of security policies, enabling real-time alerting and policy enforcement.



1. INSTALL & COLLECT

Deep accuracy into network reality through Veriflow’s data plane state collection

2. CREATE NETWORK-WIDE FLOW MODEL

Prediction of all possible data flow through Veriflow’s patented Verification Engine

3. SELECT BEST PRACTICE POLICIES & REVIEW RESULTS

Policy vulnerabilities pinpointed via mathematical verification of policies in Veriflow’s Best Practice Library

4. IMPLEMENT CUSTOM POLICIES

Tailor to your network’s needs through configurable policies and complete API programmability

Veriflow's patented approach performs a “deep data-plane analysis” of the network, constructs a rigorous formal model, and enables mathematical verification against flexible policies via a simple and intuitive user interface.

The Veriflow solution consists of multiple components. Initially, Veriflow's Collector gathers a real-time situational awareness of the network's data-plane state, the lowest and most foundational information in the network devices. Analyzing data-plane state is fundamentally necessary to provide comprehensive insights regarding the network's operational correctness, and Veriflow provides the only solution in the market that performs analysis with this level of depth at large scale.

Then, Veriflow's Verification Engine processes this information into a predictive model of all possible network-wide data flow. This breakthrough required sophisticated, novel reasoning algorithms and compact data structures that are amenable to high-speed real-time analysis of the exponentially large number of possible packets. This solution works for both traditional networks and software-defined networking (SDN) environments.

Finally, Veriflow's Policy Explorer performs a real-time and rigorous analysis of security policies to detect vulnerabilities and policy violations. This technology enables a level of understanding of the reality of the network never previously attainable.

Using Veriflow for Network Security Compliance

Network Policy Repository
Information security standards and regulations broadly provide guidelines for defining and implementing policies and procedures related to network design and operations.

Veriflow provides a set of policy packs relevant to these standards, such as PCI DSS or HIPAA. In addition, users can define their own policies to meet the organizational needs, making it easy to document and maintain a policy repository.

Vulnerability Risk Assessment

Vulnerability risk assessment is an integral part of all information security standards and regulations. For example, the guest WiFi network should have access to the internet but not to the data center. Veriflow provides an in-depth automated assessment of all possible packet flows throughout the network. It can validate the intended behavior, as well as reveal unexpected vulnerabilities as compared to the defined policies. Network operators can take appropriate action to protect against impending threats.

Network Segmentation Verification

One of the most important network security policy is network segmentation, and it is used to contain the threat landscape. For example, an organization may want to protect finance and human resource departments differently as compared to sales and manufacturing. As network engineers design and implement such segmentation policies, Veriflow can validate whether those policies are actually realized or not (e.g. VLAN leaks).

Organizations can use Veriflow to greatly reduce time and resources required to maintain continuous and comprehensive compliance through automation.

Failover Verification

Business continuity requires availability of mission-critical information and systems at all times. Organizations invest heavily in building redundancy in the form of active high availability as well as disaster recovery sites, and networks play an important role in achieving this functionality. Veriflow validates if the desired failover behavior is in place. The same mechanism can be used for multipath validation, such as ECMP or link aggregation (LAG).

Service Outage Response

Because networks are complex multi-vendor, multi-protocol, and multi-layered environments, network operators typically struggle to identify the root cause of service outages. Veriflow can deeply and broadly analyze the network at software speeds to pin-point the source of outage, such as break points, loops, and black holes. This helps to greatly minimize the service outage duration.

Rapid Incident Response

In case of a security breach, an important part of all information security standards and regulations is incident response and reporting. Incident responders need to quarantine infected machines, but determining how to do so may involve an hours-long manual process of investigating the state of multiple network devices to determine how an infected host obtains connectivity to parts of the network. Veriflow can identify the network vulnerabilities, such as unintended back doors, immediately and interactively – so that network operators can rapidly contain the threat. Analysis of the network state before, during, and after an incident also makes it easy to complete the required documentation and reporting.

Accelerated Network Troubleshooting

Networks can face many challenges other that outages and breaches, such as poor performance, where both internal and external users complain about degraded services. This can be due to several reasons, for example, CRC errors and MTU mismatch. Veriflow has a broad and deep view of the network, thus saving time and effort required to find these anomalies.

Compare Network State "Before & After" a Change

Network topology changes, device re-configuration, and software upgrades are integral parts of managing a network of any size. Occasionally, network operators may upgrade device software without making any change in the configuration, and wonder if the network behavior has changed due to unexpected software defects. Veriflow allows engineers to compare the network state before and after any change to ensure that the network is behaving as expected and is still compliant.

Validation of Security Configuration

The information security standards and regulations require general controls to be implemented in all IT systems, including network devices. For example, implementing user access control and authentication through directory services, instead of vendor default usernames and passwords in the devices. Similarly, configuring encrypted community string for SNMP, or MD5 authentication for OSPF. Veriflow collects this device metadata, and can validate its correctness.

Improved Audit Response

Responding to a compliance audit is a costly and daunting task, because it takes significant time and resources to produce accurate and acceptable documentary evidences. Network administrators can interact with the Veriflow's graphical interface for ease of use, or leverage the extensive open APIs for integration in large scale deployments. Veriflow's output is fully searchable, simplifying a broad spectrum of operational tasks. Results are used (directly or through API) to assist in audits, greatly simplifying the audit process.

Conclusion

Network security compliance is an important component of overall information security standards and regulations. Veriflow provides continuous network-wide mathematical verification of compliance policies to protect against financial and reputation risks. Organizations can use Veriflow to greatly reduce time and resources required to maintain comprehensive compliance through automation. It enable ease of compliance via "policy packs" for various information security standards. Network administrators can easily generate evidence for audits without reliance on manual periodic sampling.

How To Contact Us

To learn more about the Veriflow platform and how it can address the enterprise security needs, or to request a demo, please contact us at info@veriflow.net.

Veriflow's mission is to apply mathematical verification to complex networks, preventing outages and breaches which lead to astronomical losses.

VERIFLOW

2665 N. First St, Suite 206
San Jose, CA 95134
(408) 809-1790