tufin The Security Policy Company.

Best Practices for GDPR Compliance: Network Security

The Four Articles for Network Security Policy Management

Abstract

The introduction of GDPR and the steep penalties for non-compliance requires organizations to redefine their corporate security policy. In particular, the definition of what constitutes personal data is significantly broadened by GDPR and requires a more granular view of applications and the users that have access to them. Network Security Policy Management (NSPM), already a standard to meet PCI and other compliance mandates, will enable organizations to meet and exceed GDPR requirements by mapping the network topology and establishing a unified security policy across the entire hybrid network. NSPM is the solution for providing visibility, monitoring to not only manage policy but automate and orchestrate network security.

About GDPR

The General Data Protection Regulation (GDPR) is a regulation that the European Parliament, Council of the European Union, and the European Commission passed to improve how corporations protect and handle personal data of EU citizens in and outside of the EU Understanding and incorporating GDPR into corporate network security policy is necessary to avoid the penalties of violation, up to €10,000,000 or 4% percent of a firm's global turnover (whichever is higher). It's not just European or multi-national companies who face fines. Through the Privacy Shield Frameworks and the Judicial Redress Act of 2015 any organization that handles personal data of EU citizens, including the United States are required to include GDPR into their security policy and face penalties and class action lawsuits for not doing so.

GDPR Enforcement

Each member state of the EU appoints a Supervising Authority that is an independent public authority who receives direction from the European Protection Board, and businesses are required to work with. The Supervising Authority conducts audits, reviews certifications, issues warnings of possible failures, orders compliance, imposes limitations or bands on processing, imposes administrative fines, and suspends non-compliant data flows.

Understanding and Incorporating GDPR in Network Security

GDPR has broadened the definition of personal data to include identifiers such as device, IP address, cookie identifiers, or location – data fields commonly collected by applications and utilized by a single team or multiple teams. As a result, organizations must reconsider processing personal data in its new and wider context, and also reconsider how they design security policy to ensure a proactive review and improvement of security processes.

The following four articles specify GDPR mandates that impact network security policy:

- Section 1, Article 25: Data Protection by Default and Design
- Section 1, Article 30: Records of Processing Activities
- Section 2, Article 32: Security of Processing (Personal Data)
- Section 3, Article 35: Data Protection Impact Assessment

This document will dive into best practices for each of these articles and will specify how network security policy management (NSPM) can be used to achieve and maintain GDPR compliance.

About Network Security Policy Management (NSPM)

Network Security Policy Management tools enable network security operations to proactively manage firewall policy across heterogeneous networks, implement complex policy-driven controls to monitor and track all change requests, and ensure continuous compliance with internal security policies and external industry regulations. These advanced network security management tools accurately map network topology and provide complete visibility for multi-vendor, multi-platform, and hybrid cloud environments. By managing a unified security policy NSPM solutions operationalize true network segmentation and aggregated risk reporting. A policy-based approach to network security provides the means for efficient change management analysis and design to automatically provision changes in minutes instead of days without violating security policy with fewer resources.

Data Protection by Default and Design (Section 1, Article 25)

Organizations that handle personal data of EU residents must deploy the appropriate organizational and technical measures that protect data by default.

GDPR broadens the definition of what constitutes as personal data leaving organizations to reassess their infrastructure, applications, and access of users and groups. In addition all business units must be surveyed to understand the applications used to collect and store customer data.

Once it's understood where sensitive data resides and which business units or user groups require access to the data, processes and mandatory reviews can be put in place to ensure that data is protected. While many organizations have firewalls in place to protect network access, the complexity introduced by a multi-vendor, multi-platform, environment makes it difficult to consistently enforce security policy. This challenge is complicated by the adoption of the next generation network, now comprised of legacy and next generation firewalls (NGFW), and hybrid cloud platforms.

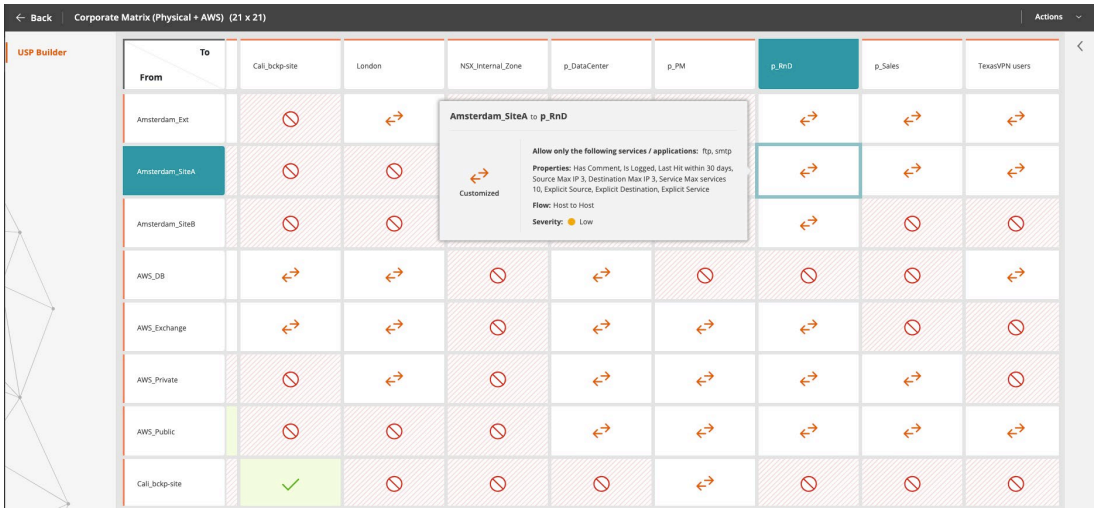
Organizations required to meet GDPR compliance mandates will find utility in several simplified protection solutions of NSPM:

Capability	**Compliance Enablement**
Zone Creation and Management	Design network zones by IP ranges, subnets, or network object groups to enable effective access management between zones as the first step to effective network segmentation.
Multi-Vendor, Multi-Platform Management	Effectively monitor and manage all network vendors and platforms through a single console, regardless of network complexity and diversity.
Policy Enforcement and Monitoring	Enforce network segmentation policy between security zones to enforce compliance. Proactive risk analysis identifies gaps between the current and desired state of compliance and ensures the design of new access changes is aligned with the policy.
Automated Risk Identification	Proactively identify risky and/or unused rules for removal to ensure a minimally-required rulebase.
Automated Policy Improvement	Identify overly permissive rules and tighten them based on advanced traffic analysis.

<u>Manage Zones and Monitor Compliance</u>

Segmentation of the network and monitoring of access against regulations and standards proactively identifies risk and non-compliance. Network zones are designated based on the sensitive nature of the data and applications stored within. Further permission or restriction of

access between the zones is managed across all platforms through IP ranges and network object groups (e.g. user groups). Zones can be further segmented as an iterative approach to microsegmentation while ensuring ongoing manageability.

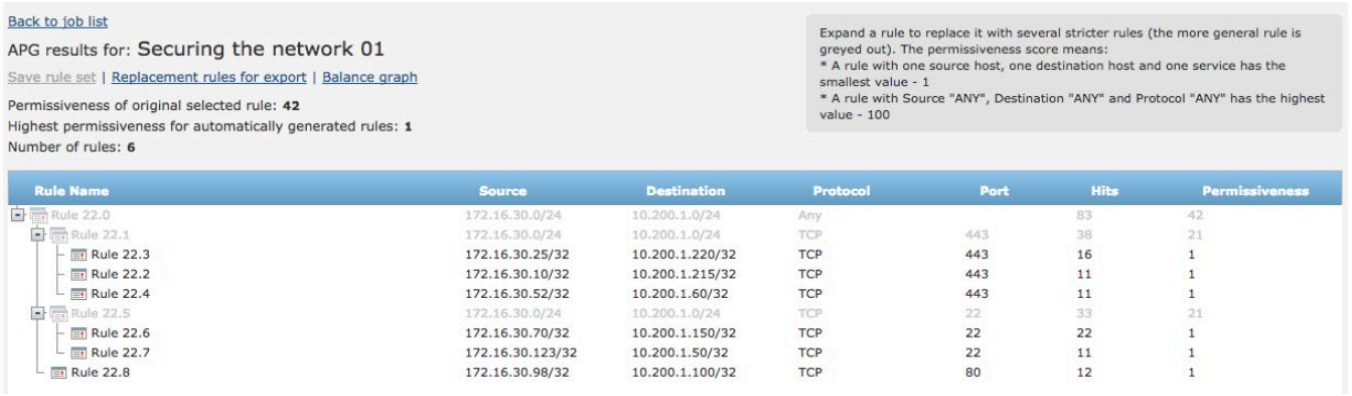


Data Protection by Design with the Tufin Orchestration Suite™

The Unified Security Policy is a matrix-based dashboard showing your organization's adherence to the desired network segmentation policy.

Automate Risk Reduction

Compliance is achieved when the minimal level of acceptable risk is determined. However, even acceptable risky rules that are unused require proactive identification and removal to ensure that only the appropriate access controls are in place. NSPM solutions empower network security professionals to monitor traffic and generate recommendations to develop rule modifications to reduce overall risk by tightening overly permissive rules. Deploying an automated risk identification process enables proactive risk mitigation and ensures organizations meet or surpass both internal security policies and GDPR compliance mandates.



Data Protection by Default with the Tufin Orchestration Suite

The Automatic Policy Generator proactively monitors traffic flows to provide recommendations to reduce the permissiveness of existing access rules.

Records of Processing Activities (Section 1, Article 30)

Any organization that handles personal data of EU citizens must maintain a record of processing activities in writing and make the record available to the supervising authority.

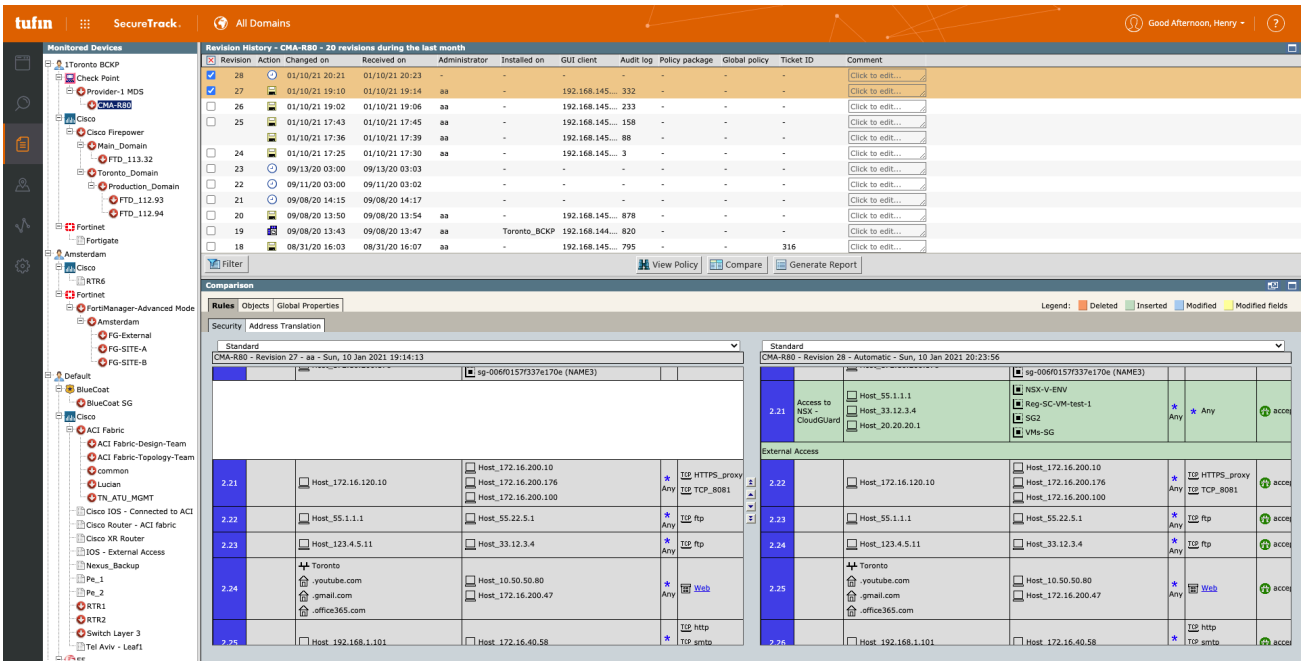
The requirement to track and report on changes to the network is a critical requirement for all common regulatory mandates, including GDPR. But, many organizations struggle with the requirement to design, deploy, and document access changes and risk much more than violation of a single regulatory mandate. In the course of network expansion and contraction – especially through the adoption of private and public cloud – common in-house solutions like documenting changes in Excel become unmanageable and unreportable. It is impossible to meet compliance without a central solution to manage, automate and orchestrate security policy change requests.

Organizations required to meet GDPR compliance mandates will find utility in central change management provided by NSPM:

Capability	**Compliance Enablement**
Automated Change Tracking	The automation of change tracking makes it easy to produce granular compliance reports on a regular basis or ad hoc.
Auditable Change Workflow	To align with the policy changes are processed through an auditable workflow with full history recorded for each change.
Multi-Vendor, Multi-Platform Management	Consolidated access changes across every network device ensures an accurate and readily retrievable data set.
Reporting	Out-of-the-box reports as well as custom reports are produced across vendors and platforms in the hybrid network.

Consolidate Change Tracking

Automated change tracking ensures audit preparedness and enables comprehensive compliance report generation. Change data is normalized across network devices and virtual networking platforms and enriched with metadata throughout the change approval process. Changes processed through the auditable workflow can be proactively checked for security violations and monitored for automatic recertification upon expiration. All changes are searchable in a consolidated change tracking dashboard to ensure audit readiness.



Records of Processing Activities with the Tufin Orchestration Suite

Simplified and aggregated change tracking and comparison of changes to access rules.

Security of Processing (Personal Data) (Section 2, Article 32)

Organizations that handle personal data of EU residents must ensure the ongoing confidentiality, integrity, availability, and resiliency of processing systems and services, and restore availability and access to personal data in a timely manner in the event of a physical or technical incident.

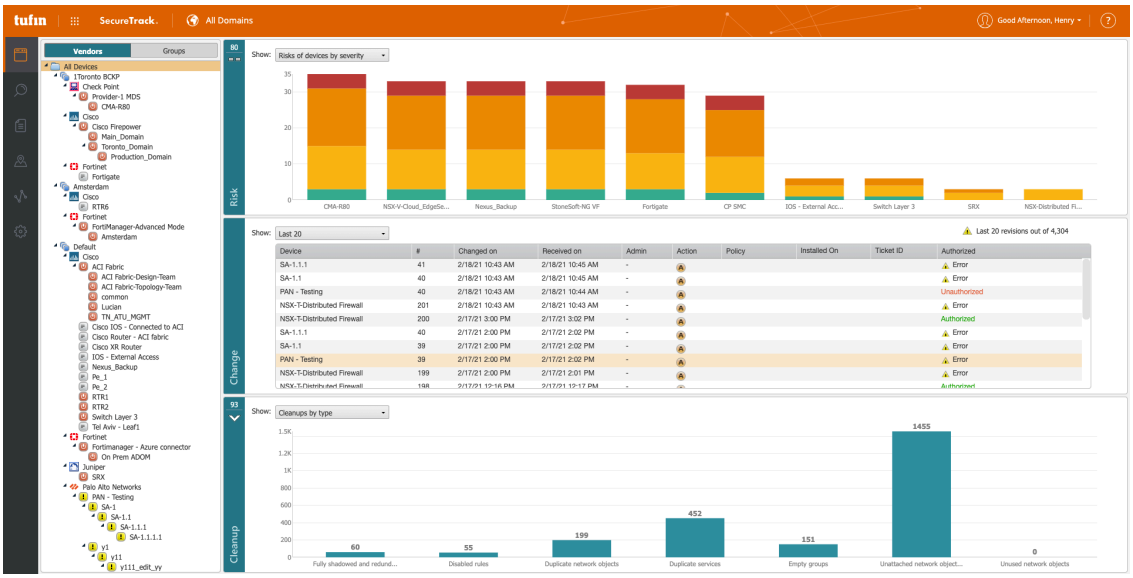
Designing a network policy that limits access to personal data processing systems is a critical step to ensuring confidentiality. Developing a consistent access change process that ingrains confidentiality and integrity requires a rigid and enforceable step-by-step change process. Ensuring availability of applications and systems requires connectivity monitoring and rapid troubleshooting to quickly resolve any issues that arise.

Organizations required to meet GDPR compliance mandates will find utility in network security and application connectivity solutions from NSPM:

Capability	**Compliance Enablement**
Operationalized Network Segmentation Policy	Easily design and deploy network segmentation that ensures only authorized access to applications.
Auditable Change Workflow	Consistent adherence to an access change management process ensures that new risk is not introduced to the network.
Connectivity Monitoring and Troubleshooting	Accurate network topology mapping across the hybrid network helps identify and troubleshoot connectivity issues
Application-Driven Connectivity	Rapid identification of disruptions in application connectivity and automated connectivity requests for quick resolution.

<u>Ensure Confidentiality of Services</u>

Effective network segmentation is a foundational pillar of network security. The design and deployment of network zones ensures that only authorized access is allowed to data processing applications. Modifications of – or new requests for – access are subject to automated proactive risk assessment against corporate security policy to identify and control potential violations. Access requests that violate security policy are automatically flagged for review and recertification by security operations. An enterprise-wide view of risk, independent of compliance, provides consistent monitoring and efficiency to rule review and elimination.

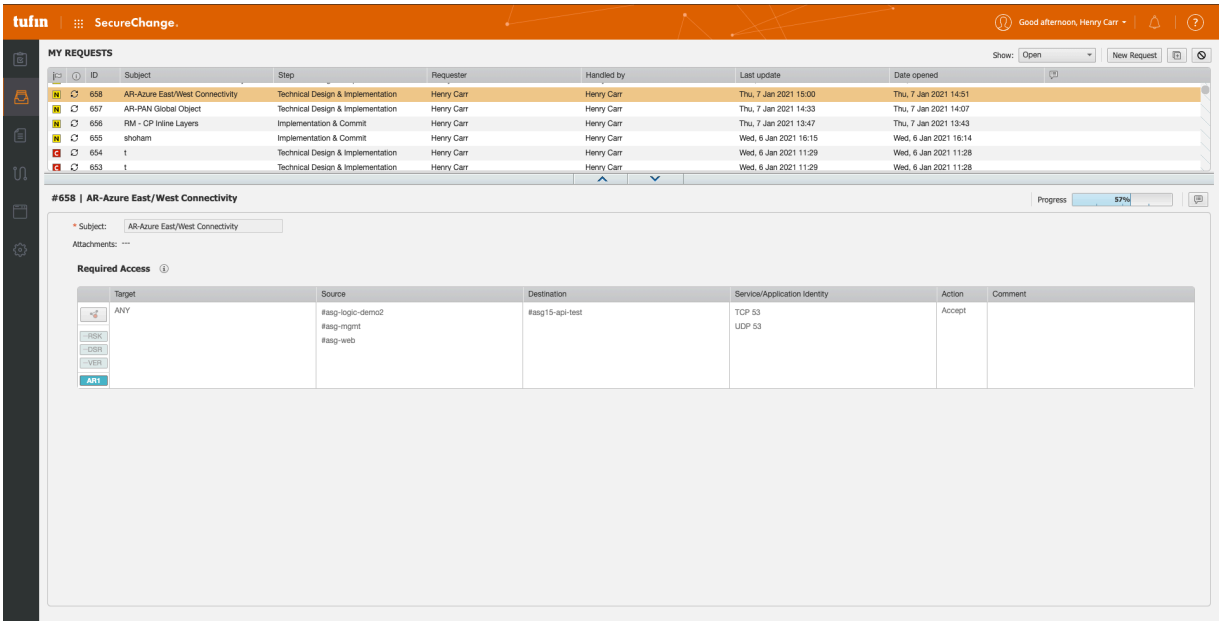


Ongoing Confidentiality with the Tufin Orchestration Suite

The interactive dashboard provides an overview of risk across your network access rules.

Ensure Access Integrity

Workflows provide the ideal solution for a zero-trust access change management model that is consistent with security policy. The separation of duties for risk assessment, access design, and provisioning of changes eliminates the likelihood of granting risky or overly permissive access. The automated workflow solution routes requests along a consistent approval chain and eliminates human errors and misconfigurations.

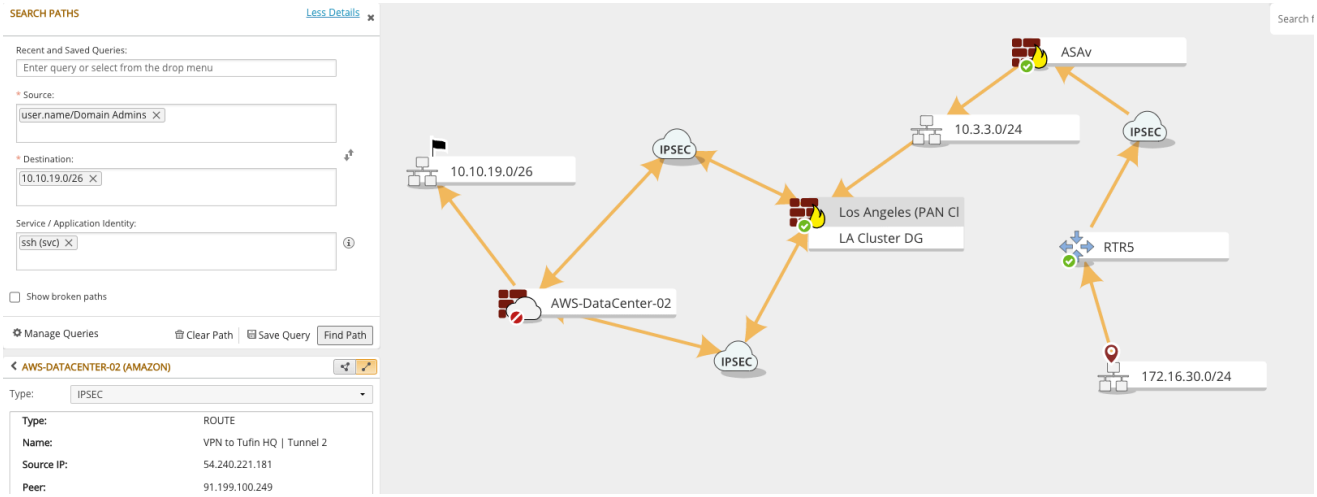


Ongoing Integrity in Access with the Tufin Orchestration Suite

Workflows are customized to match your internal process, and changes are provisioned through policy-based automation.

Monitor and Troubleshoot Application Connectivity

Restoring access to data is critical for the business and for compliance with GDPR. The ability to model network topology and application connectivity ensures that your network team is alerted to a disruption even before it affects end users or customers. Application-driven policy-based automation proactively identifies network disruption, provides instant path analysis to simplify troubleshooting, and implements connectivity requests to restore application connectivity and ensure business continuity.



Restoration of Access with the Tufin Orchestration Suite

Retain technical and business requirements for access design to ensure rapid resolution to unexpected network outages.

Data Protection Impact Assessment (Section 3, Article 35)

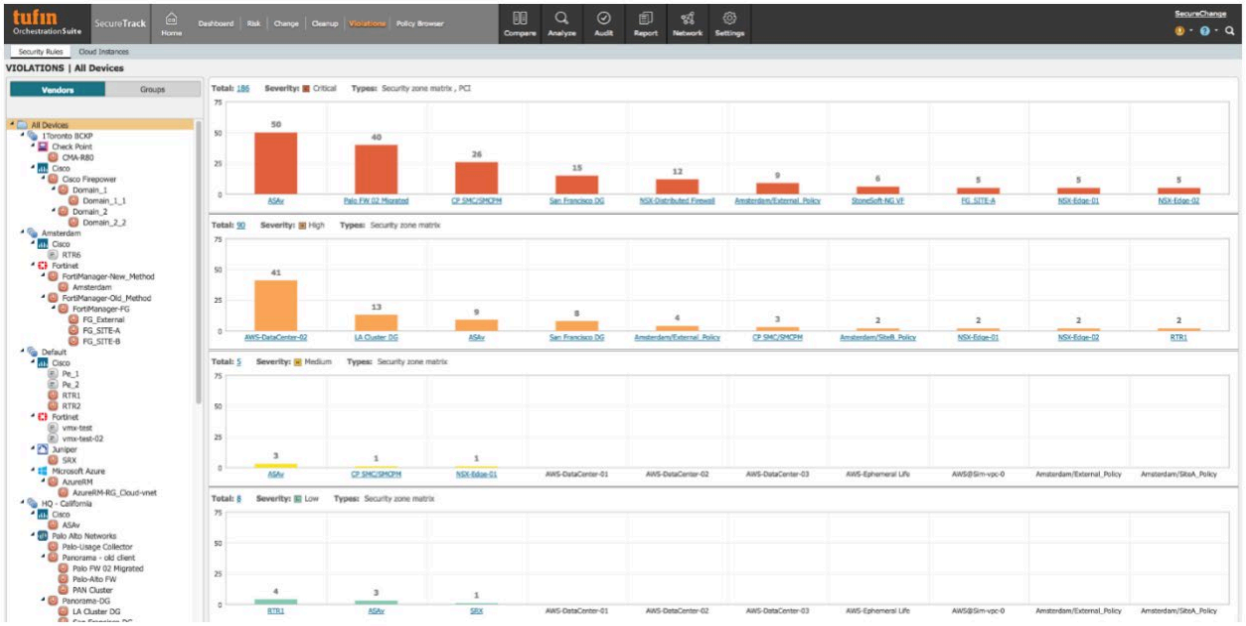
Organizations that handle personal data of EU residents must carry out an assessment of the safeguards, security measures, and the mechanisms that ensure the protection of personal data that are used to demonstrate compliance with GDPR.

Compliance is an ongoing process that begins with defining the specific benchmarks of compliance for your unique environment. Proactive analysis and real-time assessment of policy changes are required to achieve continuous compliance, protect the organization from cyberattacks, and avoid penalties. The ability to ensure continuous compliance will save valuable time and personnel resources associated with audit preparation.

Capability	**Compliance Enablement**
Noncompliance Alerts	Monitor changes in real time across all vendors and platforms to identify and address compliance violations.
Automated Access Request Risk Analysis	Enforce continuous compliance by identifying and resolving policy violations before the change is implemented.
Multi-Vendor, Multi-Platform Management	Consolidate and coordinate access change requests across every network device to ensure an accurate and readily retrievable data set.
Compliance Reports	Produce compliance reports to easily satisfy requirements for internal and external audits.

Check Compliance in Real-Time

Designating zones and the services allowed between them enables live monitoring of the current state of compliance compared to the desired state of policy. Live alerts should be generated for review of newly provisioned, non-compliant access to reject or approve with the option to track for regular recertification. The application of security policy provides a unique vantage point to understand enterprise-wide internal and external compliance. Deploying zone-based unified security policy provides a compliance benchmark for risk identification and mitigation.



Safeguarding Data with the Tufin Orchestration Suite

The violations dashboard summarizes security policy violations by risk level across the next generation network.

About Tufin

Tufin (NYSE: TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Tufin Orchestration Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility. Find out more at www.tufin.com.