WHITE PAPER

TUFIN ORCHESTRATION SUITE APPLICABILITY GUIDE FOR FISMA HIGH-IMPACT SYSTEMS

TO ASSIST CUSTOMERS WITH APPLICABILITY OF ORCHESTRATION SUITE TO FISMA HIGH-IMPACT SYSTEMS

MITCH ROSS | SENIOR CONSULTANT, CISSP
FRED KING | SENIOR CONSULTANT
JASON MACALLISTER | SENIOR CONSULTANT

VERSION 1.0

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Enterprise networks are becoming increasingly complex and fragmented, spanning many on-premises, private, and public cloud environments and incorporating physical, virtual, software-defined, and cloud networking components. At the same time, digital transformation imperatives increase the workload of information technology (IT) teams struggling to keep pace with business needs, security challenges, and compliance requirements. Often the amount of time between the initiation and implementation of network changes constrains an organization's desire to adapt quickly to market changes and customer demand. The struggle of IT to keep pace often has the undesirable effect of promoting shadow IT as unique lines of business look for alternative ways to respond to their needs. While the immediate need may be met, the consequences can be policy violation, broken or absent authorization security boundaries, compliance failures, or worse.

The challenge is finding the proper balance between necessary security enforcement and business agility. The proper balance takes into consideration speed, cost, compliance, and risk. The best balance is, optimally, where security is maintained at a high level while also being able to allow the organization to move quickly. In order to facilitate an increasingly optimized balance, it may be necessary to increasingly automate and orchestrate security and policy management.

The Tufin Orchestration Suite (TOS) provides network security policy orchestration and balances business agility and security across heterogeneous physical networks and hybrid cloud platforms. TOS combines Tufin SecureTrack (SecureTrack), Tufin SecureChange (SecureChange), and Tufin SecureApp (SecureApp) to:

- Enable end-to-end security change automation
- Define and enforce a unified security policy
- Support continuity of compliance and audit readiness
- Support management of security policy from a single pane of glass

Tufin engaged Coalfire, a respected cybersecurity engineering, advisory, and assessment company, to conduct an independent technical assessment of TOS. The objective of the assessment was to identify the inherent capabilities of TOS to address or support security outcomes in alignment with the Federal Information Security Management Act (FISMA) of 2014 security controls, based on a High-impact level categorization. Consideration for alignment is based on analysis of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 High-impact security baseline.

This product applicability guide may be useful for government agencies or other entities desiring to utilize TOS within the framework of a FISMA High impact security program of compliance. The guide discusses the relevant capabilities of TOS to support or address FISMA High requirements. The focus of this paper is on technical controls that are pertinent to and in alignment with TOS and its components' capabilities.

COALFIRE SUMMARY OPINION

TOS, comprised of SecureTrack, SecureChange, and SecureApp, can be a useful tool to support or address relevant technical FISMA High requirements. TOS helps provide visibility for networks to define and confirm security authorization boundaries and their associated network policies for control enforcement. SecureTrack can help unify and enforce policy across broad, heterogenous networks to maintain consistent and continuous compliance with organization network policy and flow enforcement. SecureChange can be useful for orchestrating change management through pre-defined workflows that address network changes from the initial request to verifying policy compliance, implementation, and continued monitoring. SecureApp helps define and refine network security policy from the application perspective and maintain the network's security and compliance throughout the application lifecycle. Overall, TOS can be useful for addressing the lifecycle of network security policy as part of a defense-in-depth approach to security that aligns with the lifecycle of the NIST risk management framework. Finally, through a rich set of application programming interfaces (APIs), TOS can be integrated with a variety of other products or tools to enabled increased value and insight. TOS can provide broad or partial support for FISMA High requirements from the Access Control (AC) and Configuration Management (CM) families of requirements. TOS provides narrower or partial support for the Audit and Accountability (AU), Incident Response (IR), System and Communication Protection (SC), and System and Information Integrity (SI) control families.

INTRODUCING FISMA

FISMA is a United States federal legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats. FISMA was signed into law as part of the Electronic Government Act of 2002. When most agencies (and their vendors) discuss being "FISMA compliant," they are usually referring to meeting the controls identified in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This is because the law is enforced through various processes (as described by the Office of Management and Budget [OMB] Circular A-130), which establish definitions, processes, and requirements for federal agencies to follow. FISMA (through A-130) recommends guidance issued by NIST, such as Federal Information Processing Standard (FIPS) 199, FIPS 200 for impact-level categorization (Low, Moderate, or High-impact systems), and NIST SP 800-53A Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations*, (NIST SP 800-53 Rev. 4) for the selection and implementation of security controls based on the system impact level.

FISMA AUTHORIZATION PROCESS

Under FISMA, individual government agencies' senior officials may authorize an information system and accept the risks to the agency based on the security control implementation. Agencies may require commercial organizations to meet requirements unique to the agency. As a result, commercial service providers tend to obtain multiple Authorizations to Operate (ATOs) based on each individual agency's standards and requirements. As it is up to each agency's senior official to accept the risk associated with the information system, it is understood that there is little official reciprocity among agencies for recognizing the authorization and assessment of a commercial vendor. What is required for one agency may not meet another agency's needs. To maintain each ATO, a commercial service provider must be reassessed regularly. Having many ATOs from multiple agencies indicates that an organization will need to have the budget and resources for the many assessments required to maintain them.

UNDERSTANDING FISMA SCOPE

Beyond a selection of security controls, FISMA requires each agency to develop, document, and implement an agency-wide program to provide information security for the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. The selection of security controls is part of a more comprehensive risk management framework based on NIST SP 800-37. Figure 1 illustrates the major components of the risk management framework (RMF) and the documents that guide each component.

The selection of controls is based on the categorization and assignment of impact relative to the category or categories of data being protected.

The goal of an agency's security program is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Within NIST SP 800-53 Rev. 4, baselines (Low, Moderate, High) have been established that determine the minimum set of requirements necessary for an organization or agency to be authorized to manage data at these relative impact levels.

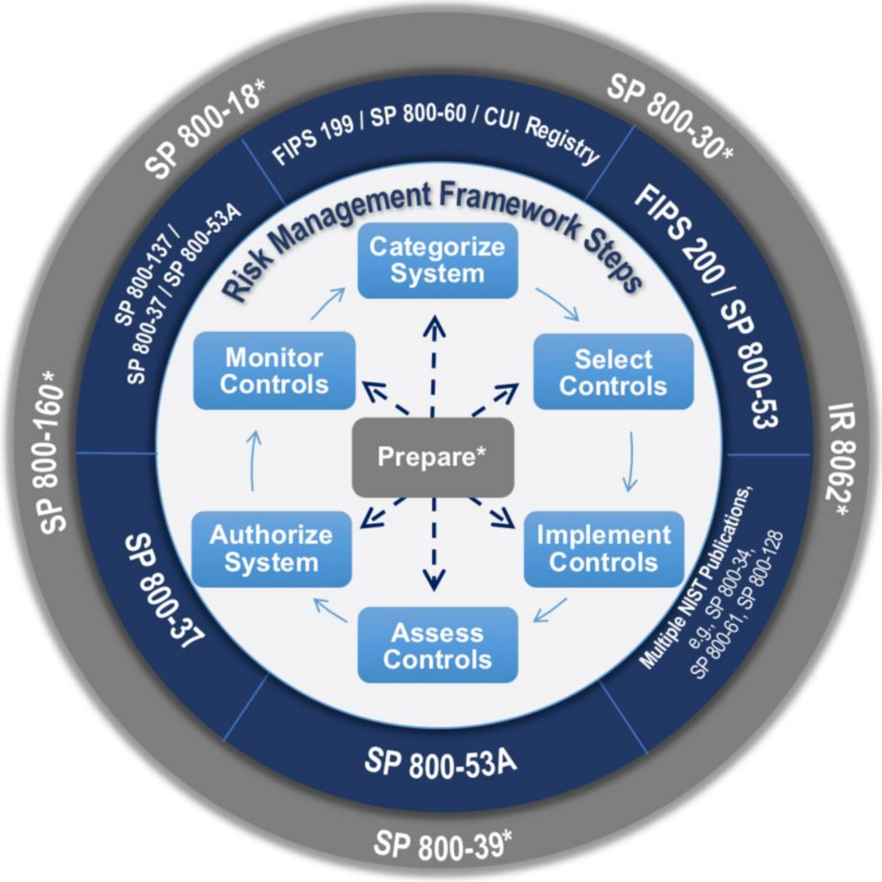


Figure 1 - NIST Risk Management Framework

For network security policy, TOS' lifecycle management capabilities can be instrumental in supporting an organization's adherence to the lifecycle of the RMF through the implementation of selected controls, assessment of control effectiveness, and continuous monitoring and reporting of network policy compliance. Tufin provides insight into the interconnectivity of the network, enables the enforcement of organizationally defined boundaries, manages changes through orchestrated and automated workflows, monitors network policy compliance, and supports application-centric network security.

INTRODUCING TOS

TOS takes a policy-based approach to automate change requests to boost security and increase agility for large organizations with complex networks. TOS is a policy-centric solution that automatically analyzes risk and orchestrates network security policy to manage risk. From application to firewall, TOS unifies security policy and provides advanced automation capabilities that can increase business agility, eliminate errors from manual processes, and support continuous compliance.

Figure 2 conceptually illustrates the elements and high-level architecture of TOS.

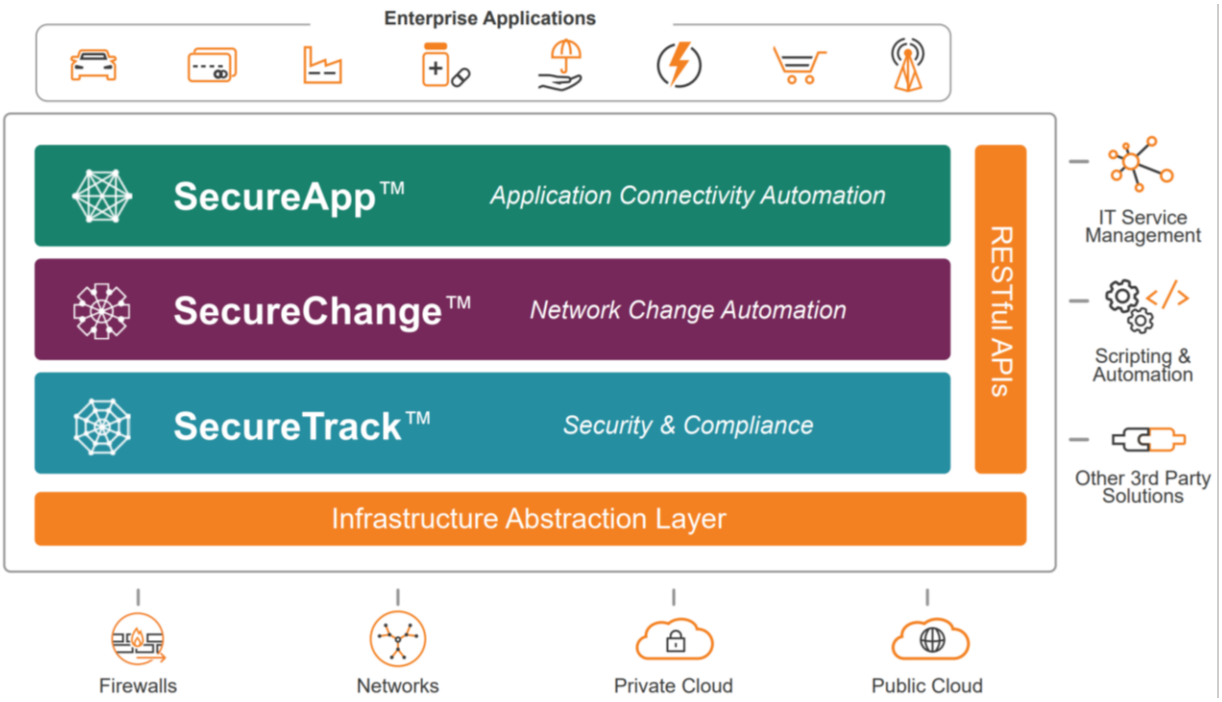
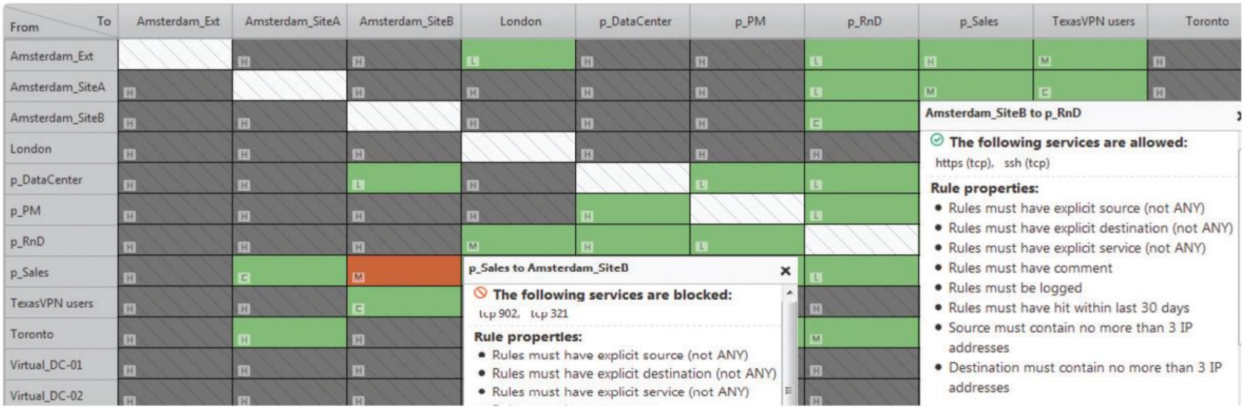


Figure 2 - Tufin Orchestration Suite

By using TOS, the entire security policy change lifecycle can be managed across an organization's security, network, and application ecosystem. Groups that have been performing change control using just a ticketing system or email and spreadsheets to manage changes will significantly improve their ability to create, approve, and execute changes, which will also enhance their ability to meet or exceed any applicable service level agreements (SLAs). The customizable workflow's ability to model changes prior to implementation can significantly reduce implementation times and negative impacts to the business due to misconfigured changes. Post-implementation confirmation that changes have been implemented as requested reduces rework. Organizations that use other tools to make changes can seamlessly implement the changes needed for network and core security components using TOS and its components. This gives organizations real-time compliance validation that adds value to not only the operations teams, but audit, compliance, and reporting functions as well.

TOS utilizes a Unified Security Policy (USP) that defines and enforces a central, zone-based segmentation matrix to strengthen the security posture and meet regulatory requirements. The USP matrix can be configured as a blacklist or whitelist policy and can accommodate zones based on IP address or defined security groups. TOS provides a central console for identifying and addressing high-risk access across vendors and platforms and allows for the execution of proactive risk analyses for access changes. Figure 3 depicts the central console with the USP and identification of risk resulting from TOS analysis.



From \ To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	London	p_DataCenter	p_PM	p_RnD	p_Sales	TexasVPN users	Toronto
Amsterdam_Ext		H	H	L	H	H	L	H	M	H
Amsterdam_SiteA	H		H	H	H	H	L	M	C	H
Amsterdam_SiteB	H	H		H	H	H	C			
London	H	H	H		H	H	H			
p_DataCenter	H	H	L	H		L	L			
p_PM	H	H	H	H	H		L			
p_RnD	H	H	H	M	H	L				
p_Sales	H	C	M				L			
TexasVPN users	H	H	C				H			
Toronto	H	H	H				M			
Virtual_DC-01	H	H	H				H			
Virtual_DC-02	H	H	H				H			

p_Sales to Amsterdam_SiteB ×

🚫 **The following services are blocked:**

tcp 902, tcp 321

Rule properties:

- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have explicit service (not ANY)

Amsterdam_SiteB to p_RnD

✓ **The following services are allowed:**

https (tcp), ssh (tcp)

Rule properties:

- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have explicit service (not ANY)
- Rules must have comment
- Rules must be logged
- Rules must have hit within last 30 days
- Source must contain no more than 3 IP addresses
- Destination must contain no more than 3 IP addresses

Figure 3 – Unified Security Policy – Zone-to-Zone Based Connectivity Matrix

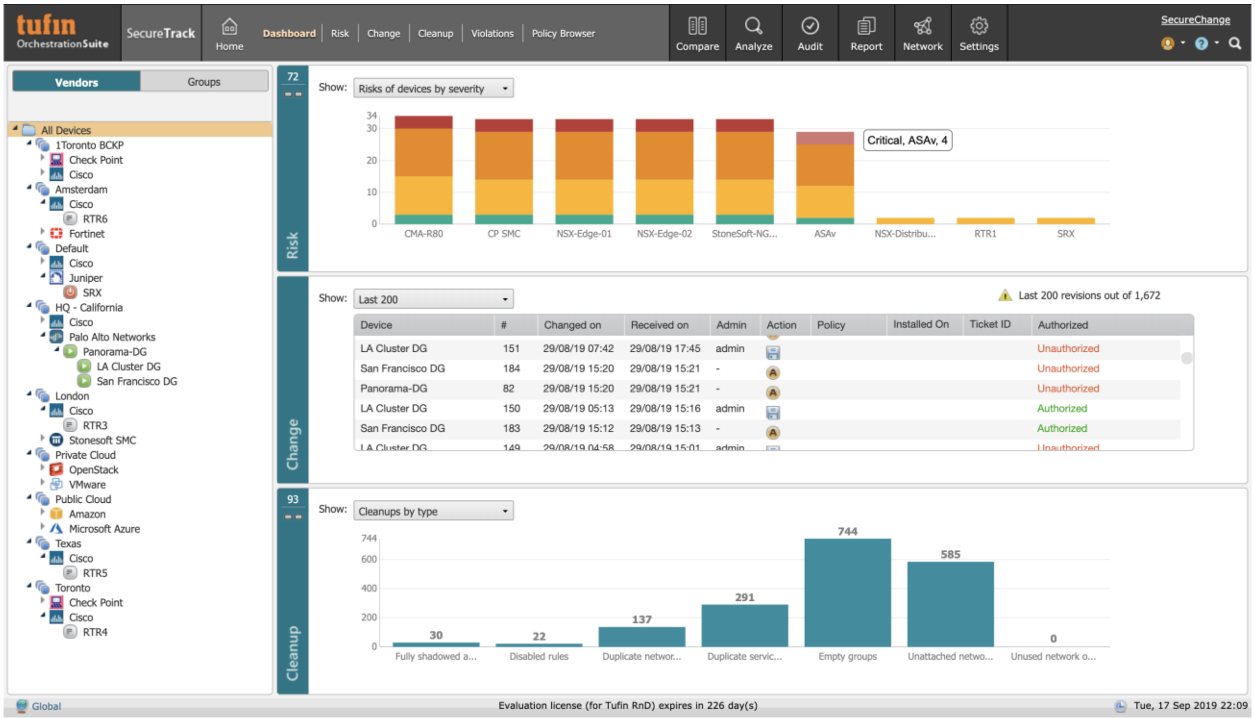
TOS offers the ability to extend its capabilities using a comprehensive set of REST APIs. Utilizing these APIs, the TOS user can create connections to other applications, devices, and cloud services that also utilize the popular REST API interface. A number of these application providers offer this integration out of the box. These applications include IT service management (ITSM), IP management (IPAM), vulnerability scanning and management tools, security information and event management (SIEM) tools, security orchestration automation and response (SOAR) tools, endpoint detection and response (EDR) tools, and others. The TOS user may also elect to build custom capabilities and integration into TOS using the REST API interfaces.

TUFIN SECURETRACK

The SecureTrack component of TOS is a comprehensive firewall and security policy management solution for multi-vendor firewalls, next-generation firewalls, and multi-cloud platforms including public, private, and hybrid clouds. It greatly accelerates and simplifies firewall operations, provides end-to-end network visibility across the entire enterprise, provides management and control of security policy from a single console, promotes the continuous compliance and auditability of the firewall environment, and supports multiple vendors.

SecureTrack can manage and monitor a wide variety of physical devices such as Cisco devices, F5 devices, Juniper devices, and many more. SecureTrack is also able to monitor and manage virtual and cloud devices and configurations, including VMware NSX Cloud, Cisco ACI, Amazon Web Services (AWS), and Microsoft Azure.

SecureTrack offers a dashboard view that provides an overview of all security risks, configuration changes, and optimization opportunities for an organization’s network security devices as depicted in Figure 4.



Show: Last 200

Last 200 revisions out of 1,672

Device	#	Changed on	Received on	Admin	Action	Policy	Installed On	Ticket ID	Authorized
LA Cluster DG	151	29/08/19 07:42	29/08/19 17:45	admin	💾				Unauthorized
San Francisco DG	184	29/08/19 15:20	29/08/19 15:21	-	Ⓐ				Unauthorized
Panorama-DG	82	29/08/19 15:20	29/08/19 15:21	-	Ⓐ				Unauthorized
LA Cluster DG	150	29/08/19 05:13	29/08/19 15:16	admin	💾				Authorized
San Francisco DG	183	29/08/19 15:12	29/08/19 15:13	-	Ⓐ				Authorized
LA Cluster DG	149	29/08/19 04:58	29/08/19 15:01	admin	💾				Unauthorized

Figure 4 - Tufin SecureTrack Dashboard

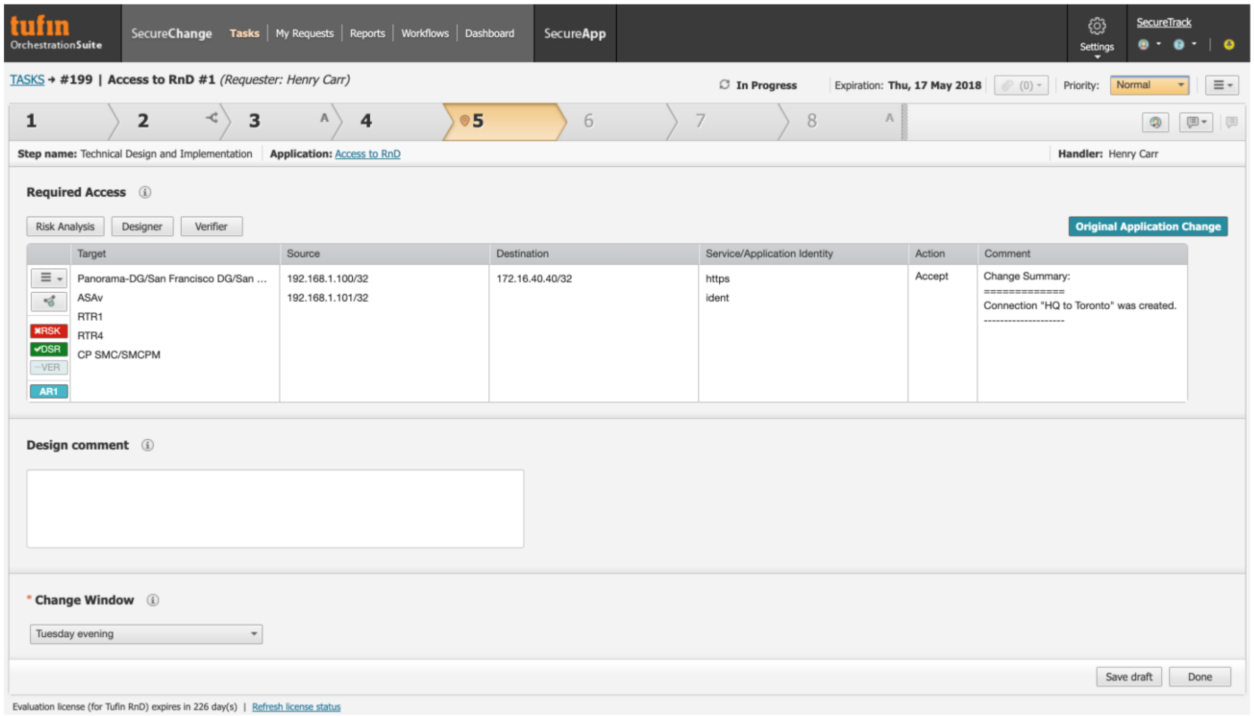
SecureTrack utilizes a central repository for all firewall rules enterprise wide. This enables simplified management across multi-vendor, multi-platform technologies as well as effective firewall rule optimization such as shadowed rules, overly permissive rules, and more. SecureTrack also provides comprehensive management tools, including a centralized dashboard, reporting capabilities, advanced searchable correlations between policy and firewall rules for violations and exceptions, and easy identification of network security gaps.

SecureTrack also enables continuous compliance with real-time monitoring and alerts for security policy and regulatory compliance risks.

TUFIN SECURECHANGE

The SecureChange component of TOS provides automation and orchestration of the network security policy change process. This allows organizations to accurately implement security policy changes across the enterprise in minutes instead of days, all while maintaining security and compliance. SecureChange provides increased agility through automation, auditable processes, and network security policy lifecycle management.

SecureChange provides standardized workflow templates and allows for the creation of customized workflows to manage network access requests. For example, a workflow may be created to decommission security rules or servers, modify group objects, request or remove access for internal users or contractors, create new security rules, and so forth. Each workflow contains customized steps with actions, owner assignments, and approval settings to assure that the ticket follows the required process to evaluate, approve, and implement the request as shown in Figure 5.



TASKS → #199 | Access to RnD #1 *(Requester: Henry Carr)*

In Progress   Expiration: Thu, 17 May 2018   (0)   Priority: Normal

Step name: Technical Design and Implementation | Application: Access to RnD | Handler: Henry Carr

Required Access

Target	Source	Destination	Service/Application Identity	Action	Comment
Panorama-DG/San Francisco DG/San ... ASAv RTR1 RTR4 CP SMC/SMCPM	192.168.1.100/32 192.168.1.101/32	172.16.40.40/32	https ident	Accept	Change Summary: ============= Connection "HQ to Toronto" was created. --------------------

Design comment

* Change Window: Tuesday evening

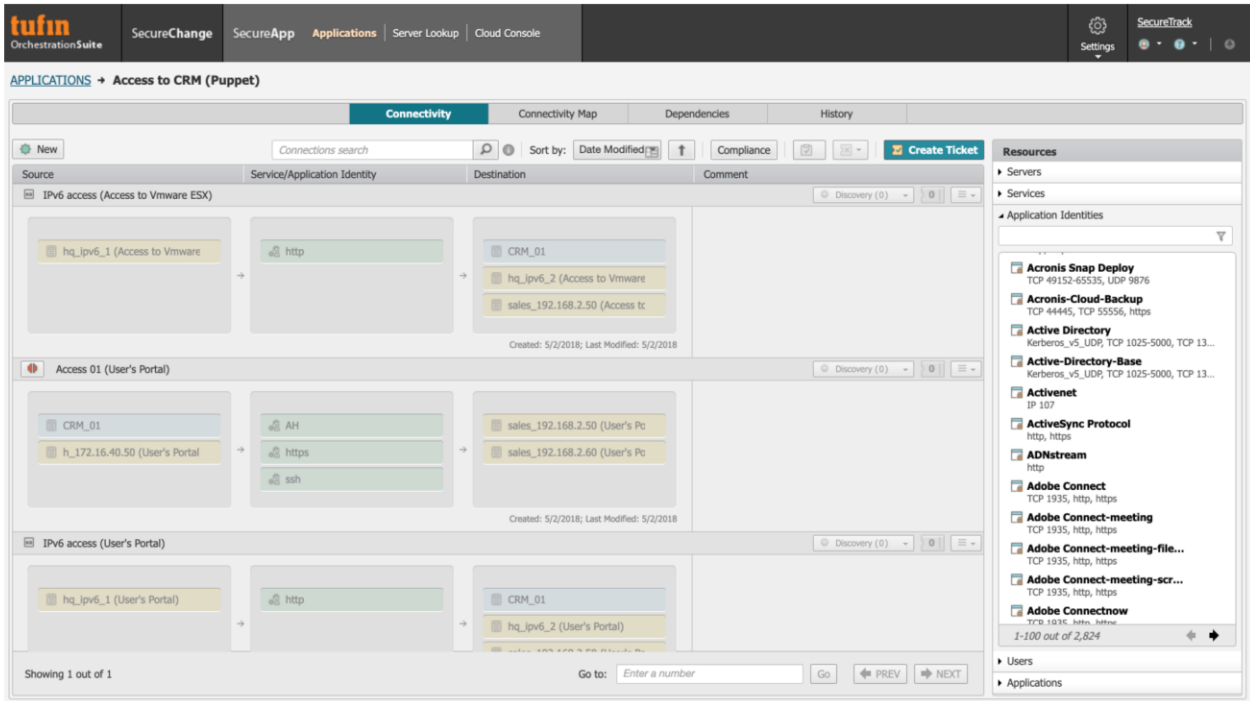
Evaluation license (for Tufin RnD) expires in 226 day(s) | Refresh license status

Figure 5 - Tufin SecureChange Workflow

A full, automatic log of changes is created and maintained to provide full accountability and deliver comprehensive reports.

TUFIN SECUREAPP

The SecureApp component of TOS is an automated solution that enables organizations to easily define, update, monitor, and remove applications and services from the network. SecureApp enables application developers to define application components such as web servers and databases and the relationships between them. These definitions can then be translated into automated changes to the network that are executed via workflows that guide the design, approval, and implementation of the network security policy change. Figure 6 depicts the SecureApp dashboard and the relationship between application components with how users are provided access to the application per defined policy.



APPLICATIONS → Access to CRM (Puppet)

Source	Service/Application Identity	Destination	Comment
IPv6 access (Access to Vmware ESX)			
hq_ipv6_1 (Access to Vmware	http	CRM_01 hq_ipv6_2 (Access to Vmware sales_192.168.2.50 (Access tc	
		Created: 5/2/2018; Last Modified: 5/2/2018	
Access 01 (User's Portal)			
CRM_01 h_172.16.40.50 (User's Portal	AH https ssh	sales_192.168.2.50 (User's Po sales_192.168.2.60 (User's Po	
		Created: 5/2/2018; Last Modified: 5/2/2018	
IPv6 access (User's Portal)			
hq_ipv6_1 (User's Portal)	http	CRM_01 hq_ipv6_2 (User's Portal)	

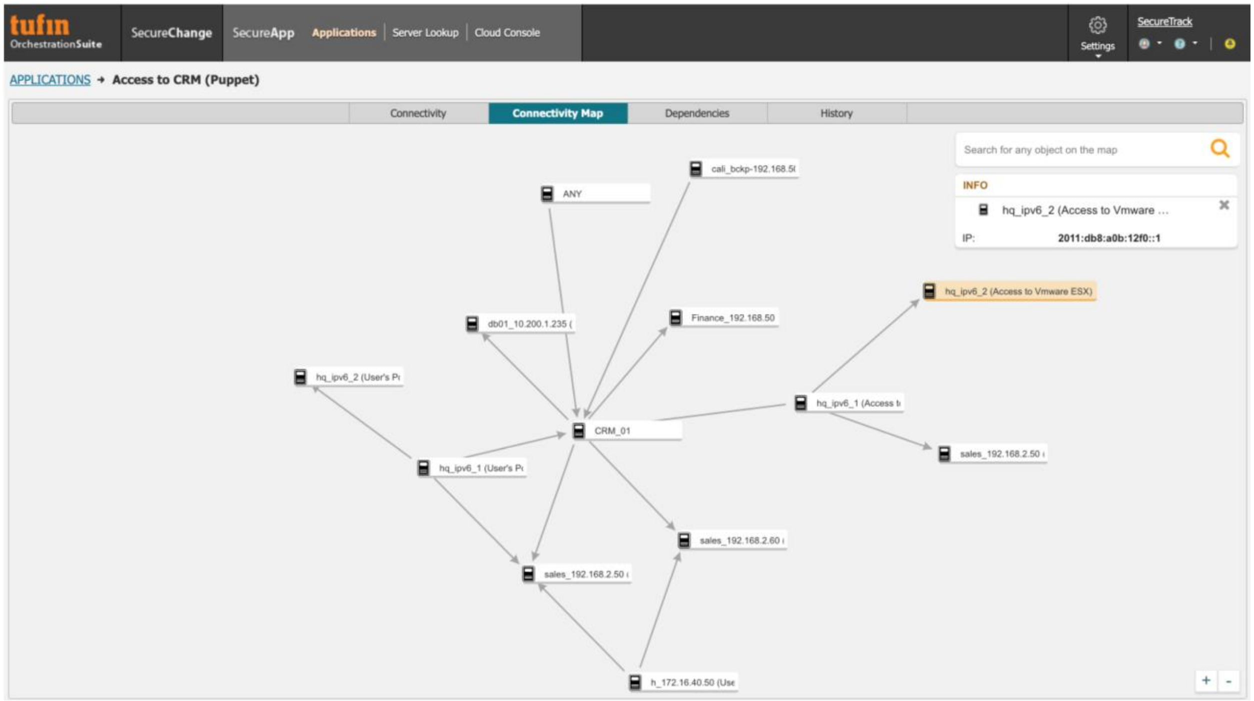
Showing 1 out of 1

Application Identities	
Acronis Snap Deploy	TCP 49152-65535, UDP 9876
Acronis-Cloud-Backup	TCP 44445, TCP 55556, https
Active Directory	Kerberos_v5_UDP, TCP 1025-5000, TCP 13...
Active-Directory-Base	Kerberos_v5_UDP, TCP 1025-5000, TCP 13...
Activenet	IP 107
ActiveSync Protocol	http, https
ADNstream	http
Adobe Connect	TCP 1935, http, https
Adobe Connect-meeting	TCP 1935, http, https
Adobe Connect-meeting-file...	TCP 1935, http, https
Adobe Connect-meeting-scr...	TCP 1935, http, https
Adobe Connectnow	TCP 1935, http, https

1-100 out of 2,824

Figure 6 - TOS SecureApp Dashboard

SecureApp uses topology intelligence to simulate network access paths and continuously displays the connectivity status across firewalls, routers, and load balancers. SecureApp also provides the ability to monitor application connectivity status and aids in the troubleshooting of connectivity issues utilizing graphical diagnostic tools. Figure 7 depicts an example of the SecureApp connectivity map, which identifies the connections between networks and endpoints in use for the application.



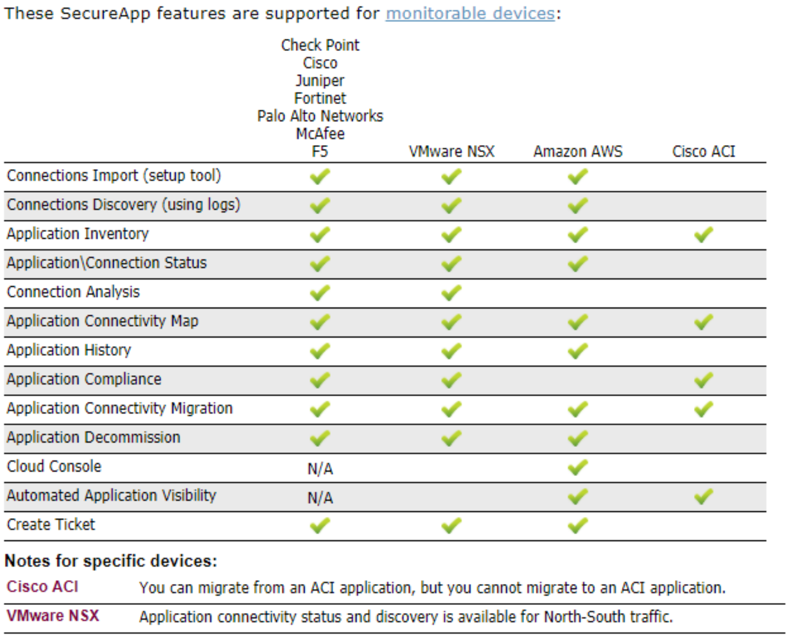
APPLICATIONS → Access to CRM (Puppet)

hq_ipv6_2 (Access to Vmware ...

IP: 2011:db8:a0b:12f0::1

Figure 7 - SecureApp Application Connectivity Map Example

SecureApp offers a portfolio of features to aid application developers in the management of the interaction of their applications with enterprise networks. The available features vary by vendor, as shown in the figure below.



These SecureApp features are supported for monitorable devices:

	Check Point Cisco Juniper Fortinet Palo Alto Networks McAfee F5	VMware NSX	Amazon AWS	Cisco ACI
Connections Import (setup tool)	✓	✓	✓	
Connections Discovery (using logs)	✓	✓	✓	
Application Inventory	✓	✓	✓	✓
Application\Connection Status	✓	✓	✓	
Connection Analysis	✓	✓		
Application Connectivity Map	✓	✓	✓	✓
Application History	✓	✓	✓	
Application Compliance	✓	✓		✓
Application Connectivity Migration	✓	✓	✓	✓
Application Decommission	✓	✓	✓	
Cloud Console	N/A		✓	
Automated Application Visibility	N/A		✓	✓
Create Ticket	✓	✓	✓	

Notes for specific devices:

Cisco ACI	You can migrate from an ACI application, but you cannot migrate to an ACI application.
VMware NSX	Application connectivity status and discovery is available for North-South traffic.

Figure 8 - SecureApp Features by Platform

SCOPE AND APPROACH FOR REVIEW

The understanding of TOS capabilities was gained through product specification, installation, configuration, administration, and integration documentation provided by Tufin and generally made available from Tufin's public-facing web site. Furthermore, Coalfire conducted interviews and engaged in live product demonstrations with Tufin personnel.

Coalfire's review of TOS began with a high-level alignment of the capability of the technology against the FISMA High-impact baseline control objectives with additional guidance for requirements provided by relevant NIST special publications and FIPS publications. This high-level alignment of TOS capabilities was further narrowed down to specific requirements that TOS may be capable of addressing or supporting. An additional analysis of the capability of the reviewed technology to address the applicable requirements was then conducted. Coalfire considered the inherent capability of TOS to enable or support security controls for the protection of FISMA High-impact systems and data.

SCOPE OF TECHNOLOGY AND SECURITY STANDARD TO REVIEW

Coalfire was tasked by Tufin to review TOS. The primary focus of the review included the components, features, and functionality of the three primary products of TOS: SecureTrack, SecureChange, and SecureApp.

For this review, Coalfire included requirements from NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf). For a broader understanding of the requirements and their applicability to technical solution implementation, Coalfire also reviewed supporting documentation provided by NIST, including assessment guidance. Applied understanding of

NIST 800-53 Rev. 4 requirements and guidance was supplemented by documentation and guidance on relevant subjects, many of which are referenced in the NIST SP 800-53 Rev. 4 requirements.

COALFIRE EVALUATION METHODOLOGY

Coalfire initially examined the FISMA High-impact baseline requirements and identified them as either procedural (organizational) or technical (the information system). Qualification of a requirement as procedural or technical was based on a review of the requirement narrative, assessment procedures, supplemental guidance, and references.

Non-technical procedural requirements that include, for example, the definition and documentation of policies, procedures, and standards were not considered directly applicable to the technical solutions' capability. In other words, TOS is not able to produce the organizations required documented compliance policy, procedures and standards. These types of things are addressed by people within the organization. Likewise, non-technical requirements, including operational procedures that describe manual processes, were not assessed against the technology's capability. Examples of this type of non-technical requirement include the maintenance of facility visitor logs, verification of an individual's identity prior to the assignment of credentials for logical access, or the performance of periodic physical asset inventories.

Technical requirements were then assessed to determine whether the proposed solution was able to address or support the requirement or requirement outcomes. Where achievement of the requirement objectives was more likely to be met using an external and non-adjacent mechanism, the requirement was determined to be not applicable to the assessed technology's capabilities. Requirements that Coalfire determined to be not applicable to TOS included encryption key management and Public Key Infrastructures (PKI), wireless network security, physical access control mechanisms, and antivirus or anti-malware solutions. That is not to say that these are not important factors to consider as it pertains to a FISMA High-impact system requirements, but rather that TOS does not natively provide the capabilities to address or support these requirements to the extent necessary to achieve compliance.

Where a requirement was qualified as applicable, Coalfire further assessed the capability of the solution to address the requirement. For applicable requirements, Coalfire designated a qualitative category of capability, including whether the solution was determined to fully support the requirement, partially support the requirement, or was unable to support the requirement. In cases where the requirement was determined to be applicable but unsupported, additional thought for the use of third-party solutions could be considered.

TOS APPLICABILITY TO FISMA HIGH IMPACT LEVEL

The following table details the applicability of TOS to provide control enablement for requirements through either default or configurable implementations. FISMA High-impact baseline requirements that are not listed in the following table were determined to not be applicable to be addressed or provided for by the specific capabilities of the reviewed technology. Rather, those omitted requirements from the following table would necessarily need to be addressed by other people, processes, or technology. At a minimum, every requirement of the FISMA High-impact baseline must be addressed by the organization seeking FISMA High-impact authorization for their systems. All requirements are the responsibility of that organization, including how controls are enabled or configured to meet those requirements. The enablement of technical controls is highly dependent on the knowledge and application of people and processes to ensure the proper operation of controls in alignment with the supported requirements.

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
AC-2	The organization: (a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment 1: organization-defined information system account types]; (b) Assigns account managers for information system accounts; (c) Establishes conditions for group and role membership; (d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; (e) Requires approvals by [Assignment 2: organization-defined personnel or roles] for requests to create information system accounts; (f) Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment 3: organization-defined procedures or conditions]; (g) Monitors the use of, information system accounts; (h) Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; (i) Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; (j) Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and (k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	TOS can partially support this control requirement — specifically, AC-2 (g): "monitors the use of information system accounts." The capability of TOS to monitor the use of information system accounts is limited to the supported systems for which TOS provides orchestration — primarily, the network devices and the network which the network devices control. Through orchestration of the network devices, TOS monitors access and actions taken by system accounts on the network devices. Where network devices managed by TOS are capable of enforcing identity-based network policies, TOS can also be used to monitor the activity of system accounts through the network. For broader monitoring of information system accounts beyond network device access or identity-based network policy monitoring, the organization would need to use other solutions, tools, or procedures. Monitoring account usage will require active participation by the organization's designated personnel to review data generated by tools relative to account usage.
AC-2 (1)	The organization employs automated mechanisms to support the management of information system accounts.	TOS can partially address the control requirement — specifically, the supplemental guidance suggestion of "using the information system to monitor account usage". This coverage is specific to the network and network devices for which TOS provides orchestration. SecureTrack monitors network devices that are

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		integrated with TOS to identify when network devices are being accessed, by whom, what actions have been taken on the network device, and whether the account was authorized to access or perform the identified action. This includes actions that are performed within TOS to effect change on the device, as well as outside of TOS and directly on the device through the device's own interfaces. Where identity-based network policies are employed, TOS can also monitor network activity by system account. For broader monitoring of information system accounts beyond network device access or identity-based network policy monitoring, the organization would need to use other solutions, tools, or procedures. Monitoring account usage will require active participation by the organization's designated personnel to review data generated by tools relative to account usage.
AC-2 (11)	The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].	TOS enables controls in alignment with this requirement — specifically, pertaining to the networks and supported network devices for which TOS provides orchestration. TOS' provisioning capabilities for supported and managed network security devices are aligned to change windows that can be predetermined and configured by the organization or pushed as emergency changes (e.g. incident response). TOS can be configured to designate when firewall configuration managers (or individual devices) can be accessed, utilized, modified, or reconfigured for this purpose. As it pertains to the use of TOS itself, Coalfire recommends that TOS integrates with a third-party Lightweight Directory Access Protocol (LDAP) or Security Assertion Markup Language (SAML) provider for the management of system accounts used to access TOS.
AC-2 (12)	The organization: (a) Monitors information system accounts for [Assignment: organization-defined atypical use]; and (b) Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles].	The organization is responsible for monitoring information system accounts for organizationally defined atypical use and reporting of atypical usage of information system accounts to organization-defined personnel or roles. TOS can support the organization with this requirement, specific to behaviors applicable and pertaining to TOS orchestrated network device configurations and network policy modifications. SecureTrack can identify unauthorized changes made directly to targets outside of the authorized change management and configuration orchestration processes as controlled by TOS and alert via email when policy violations occur. SecureTrack can also identify when unauthorized personnel attempt

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		unpermitted actions or actions that take place outside of the organizationally defined SecureChange workflow process. The authorized and unauthorized change tracking and reporting from the SecureTrack dashboard identifies where network security devices were modified outside of the approved workflow and operations windows. Similarly, SecureTrack can be tuned to monitor unusual network activities according to policy based on hit count, zone changes, or anomalous port-specific network behavior. Other solutions or processes would be required to be used for broader system applicability to include those parts of the information system that are outside the capability of TOS to support.
AC-2 (13)	The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the risk.	The organization will be responsible for disabling accounts of users posing a significant risk within an organizationally defined time period of discovery of the risk. To help facilitate the organizations disabling of user account and lessen impact of the risk associated with the account, TOS can partially support this requirement specific to the networks and network devices for which TOS provides orchestration. A role of a user, whether defined locally to TOS or integrated with TOS through LDAP or SAML, can be modified by the TOS administrators as part of the organization’s risk response process. Through the removal of a user from a role, the TOS administrator is essentially removing the user’s rights to perform the functions that are aligned with the specified role. However, for the TOS customer requiring FISMA High authorizations, it is recommended that user identity, authentication, and security group membership be managed externally from TOS by a third-party identity access management (IAM) or directory service provider rather than by TOS directly. This allows the organization to centrally disable system accounts and simultaneously remove access for all services that were previously permitted. As an additional response mechanism to disabling a user's account credentials, with TOS, the organization can use the SecureChange workflow to automate network security responses through pre-bundled workflows to modify network policies by which user groups, security groups and IP addresses are granted

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		access, or which object groups are typically granted access to temporarily or permanently blacklist access. This can be an effective response to quickly preventing network access for users or systems that pose a risk.
AC-3	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	With applicability limited specifically to network security using supported network devices orchestrated by TOS, approved access authorizations for logical access to information and system resources can be orchestrated through TOS. In the USP, the organization can define the requirements that are desired to govern the resources and traffic on the network. The requirements defined in the USP provide continuous compliance. Any violation of those requirements is shown in the SecureTrack violations dashboard. The USP dictates what access is and is not permissible in the environment as pre-defined by the organization. In the USP, the organization can create security zone matrices. A security zone matrix is a set of requirements, rule definitions, or traffic that must be blocked or allowed between the security zones that are defined in network zones. The matrix can be defined with requirements from industry standards or by custom-defined internal corporate network requirements. A rule base can also be created using automated policy generation (APG) based on the analysis of risk and what is required to support business practices. Zones can consist of IP addresses, security groups, or user groups. Network zones are groups of IPv4 or IPv6 network addresses, such as an organization's internal network or DMZ. Zones can include IPv4 and IPv6 subnets with explicit network addresses or security groups. Zones can also include other zones to build a hierarchy. Success factors for enforcement are dependent on well-defined access parameters and network policy requirements as specified by the organization in AC-1 and AC-2. Beyond network restrictions, a defense-in-depth approach to security considers logical access restrictions to systems, applications, and data as well.
AC-4	The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].	TOS centrally controls firewall rules and security groups, which affects the flow of information between systems. Changes to rule sets are evaluated for security impacts by SecureTrack. Changes are managed by SecureChange and implemented in an automated fashion via organizationally pre-defined workflows set up in ChangeTrack. Authorization and approval for changes to firewall rules are created and enforced through SecureChange workflows that manage the entire

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		lifecycle of a network policy change request, including design, security assessment, approvals, and implementation. TOS-orchestrated firewalls are capable of being monitored for unauthorized changes that might occur outside of the defined workflow process, and TOS can be configured to issue email alerts, send alerts by syslog, and display the alerts on the SecureTrack dashboard under USP Alerts. At the network level (through supported network devices), approved access authorizations for controlling the flow of information within the system and between interconnected systems can be enforced through security policy as orchestrated by TOS. In the USP, the organization can define the compliance requirements that are desired to govern the resources and traffic on the network. The requirements defined in the USP provide continuous compliance and any compliance violation of those requirements are shown in the violations browser. The USP dictates what access is and is not permissible within the environment. In the USP, the organization can create security zone matrices. A security zone matrix is a set of requirements, rule definitions, or traffic that must be blocked or allowed between the security zones that are defined in Network Zones. The matrix can be defined with requirements from industry standards or by custom-defined internal corporate network requirements. Zones can consist of IP addresses, security groups, or user groups. Network zones are groups of IPv4 or IPv6 network addresses, such as an organization's internal network or DMZ. Zones can include IPv4 and IPv6 subnets with explicit network addresses or security groups. Zones can also include other zones to build a hierarchy. Success factors for enforcement are dependent on well-defined access parameters and network policy requirements as specified by the organization in AC-1 and AC-2.
AC-5	The organization: (a) Separates [Assignment: organization-defined duties of individuals]; (b) Documents separation of duties of individuals; and (c) Defines information system access authorizations to support separation of duties.	TOS can support this requirement, pertaining specifically to the enforcement of separation of duties for administration and the orchestration of networks and network devices managed by TOS. This capability scales to large networks, distributed networks, and heterogeneous environments that include physical, virtual, software-defined, and cloud network security devices and networks.

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		Regarding supporting separation of duties and defining roles within TOS, TOS (by way of SecureTrack) recognizes two types of users: administrators and users. Only administrators can configure system-level settings in SecureTrack, such as users and network zones. Only an administrator can add or configure monitored devices. Administrators can assign users specific devices in the organization's deployment. Users can manage policy revisions and configure and run queries, audits, and reports for their defined devices. Administrators have administrative supervision over other users' queries, audits, and reports. All user types are configured in the user page. There are multiple schemes: a default scheme and a multi-domain scheme where users are defined, and a scheme that applies determines the available user types. Multi-domain schemes add super administrator, multi-domain administrator, multi-domain user, and domain user types. SecureChange and SecureApp permissions are based on users, groups, and roles. Tufin recommends that roles be assigned to groups so that the role applies to any user who is a member of the group. Predefined roles include auditor, business owner, requester, security administrator, and system administrator. Custom groups can also be added to SecureChange that can be configured for specific roles and permissions according to the organization's defined parameters for separation of duties. It is still the responsibility of the organization to ensure that the assignment of permissions and roles to individual users does not compromise the intent of this requirement, thereby allowing for the potential abuse of privileges or malicious collusion.
AC-6	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Using TOS user and administrative access and the orchestrated change management of support network devices, TOS can support the organization's design and employment of the principle of least privilege as it pertains to the enforcement of network security through workflows and task assignments. Furthermore, to help the organization better understand user and systems access, SecureTrack includes the Automatic Policy Generator (APG) which automatically creates a secure, effective, and optimized firewall rule base, limiting the allowance of traffic not actually used within the organization. It can be used for creating a new rule base, as when deploying a new firewall or adding an interface to a firewall, tightening overly permissive rules, and for performing network forensics, such as identifying specific traffic patterns on the network. APG analyzes firewall logs to determine actual business practices and

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		creates an optimized rule base that limits traffic allowance to traffic used in the organization. APG can be useful to facilitate an understanding of network connections between endpoints.
AC-6 (5)	The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].	An organization can use TOS alongside its access control processes and procedures to define privileged roles and permissions and subsequently restrict those privileged roles and permissions to organization-defined list of personnel or roles. Granular, role-based access control capabilities exist for various TOS and TOS-managed security functions that provide the ability to restrict privileged access. For SecureChange and SecureApp, user roles and associated permissions may be created, or the following pre-defined roles may be selected: auditor, business owner, requester, security administrator (super administrator), and system administrator. Each new role may be assigned one or more of the thirteen available permissions, each specifying a function. The design of new accounts or the usage of default accounts within the Orchestration Suite may be aligned directly with organizational requirements for the separation of privileged versus non-privileged access.
AC-6 (9)	The information system audits the execution of privileged functions.	Within TOS, every action that a SecureTrack privileged user takes in SecureTrack is recorded to provide complete accountability and is easily viewed in a dashboard. The details recorded include Date/Time, Username, User IP, Category of Action, Object Type affected, Object Name affected, and Details about the action. This audit trail can be exported for additional analysis or other actions. TOS also provides the ability to export audit events to an external SIEM solution to allow for an expanded view and a broader correlation of events across the organization. TOS enables organizations to optimize their policy health and demonstrate continuous compliance with regulatory standards. TOS allows an organization to define security zones and cyber assets, and to instantly generate compliance reports that map specific requirements to the actual firewall rules that are in place on the network, including supporting evidence of secure configurations and business justification for the configuration. An automated audit trail and customizable workflows enable compliance with change management frameworks. The organization will be required to determine if TOS is capable of auditing events that they deem necessary for the management of their risk and compliance program.

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
AC-6 (10)	The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	TOS uses role-based access controls and pre-defined workflows for controlling changes to network security policy configuration. These built-in controls help prevent non-privileged users from executing privileged functions. Moreover, SecureTrack identifies changes that violate organizationally defined security policy or are made outside of the organizationally approved change process.
AC-17 (1)	The information system monitors and controls remote access methods.	TOS can partially address this control in a limited fashion through the monitoring remote access methods. TOS SecureTrack can monitor hit counts and can identify and notify where violations occur. For example, the organization can configure an alert or notification action in TOS if a rule permitting remote access through a virtual private network (VPN) connection was used more than a certain number of times in a specific period. Other options and parameters for policies that are set can be identified to further monitor remote access methods.
AC-17 (2)	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.	Connection to TOS interfaces for remote, non-console access can be set up to exclusively use HTTPS and Secure Shell (SSH), with session encryption using Transport Layer Security (TLS) 1.2. TOS uses strong encryption libraries. Moreover, if the device that is supporting remote access through the VPN is managed by TOS, TOS can confirm that the VPN solution is configured to use proper cryptographic mechanisms to protect the confidentiality and integrity of remote sessions into the authorization boundary. SecureTrack can identify when there are policy violations for VPN settings and usage.
AC-17 (3)	The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.	SecureTrack retrieves network topology and firewall policy information from devices monitored by SecureTrack and builds a topology model of the network based on the policy information retrieved. The network topology model is used by many TOS features, including SecureChange automation tools like Design and SecureTrack features like the Interactive Map. The topology and firewall policy information provide visibility into the remote access points that exist into the authorization boundary, as well as into specific network security zones. This information can be useful for adjusting policy and configuration to limit the access control points according to the organization's specifications and identifying when and where violations of policy occur.
AC-18 (1)	The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.	TOS can protect wireless access through segmentation of wireless networks to a unique security zone and isolating this zone from the wired network with a policy in place for controlling communication between the wireless network zones and the wired network zones. Likewise,

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		TOS can ensure that there is a perimeter firewall in use between the wireless network and wired network.
AU-2	The organization: (a) Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; (b) Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; (c) Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and (d) Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].	Within TOS, every action that a SecureTrack privileged user takes is recorded to provide complete accountability and can be easily viewed in a dashboard. The details recorded include the date and time, username, user IP address, category of action, object type affected, object name affected, and details about the action. This audit trail can be exported for additional analysis or other actions. TOS also provides the ability to export audit events to an external SIEM solution to allow for an expanded view and a broader correlation of events across the organization. The organization will be required to determine if TOS is capable of auditing events that they deem necessary for the management of their risk and compliance program.
AU-3	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	Every action of a SecureTrack user is recorded in an audit recorded to provide complete accountability. Each audit record contains the following details: • The date and time of the action • The username of the user that performed the action • The IP address of the host from which the action was performed (automatic actions, such as scheduled reports, are listed without a user IP address) • The category or feature area that the action belongs to • The type of action (e.g., add, remove, modify, or generate report) • The type of object and object name on which the action was performed • A description of the action The audit trail view can be filtered on any field and the resulting report may be exported to a PDF file. SecureTrack may also be configured to send audit events to a SIEM system.
AU-3 (1)	The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information].	TOS can support the inclusion of full-text recording of privileged commands, such as commands resulting in the modification of security policy. TOS can also record the individual identities where group user accounts are used.

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
AU-6 (1)	The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	TOS can be integrated with a SIEM solution. In addition, TOS has integrations with leading SOAR solutions that are free for TOS customers to use. SOAR solutions can take corresponding information from an event from the SIEM tool and, as part of the orchestration, gather information about the network topology and policy set related to the event from TOS. This allows for a greater depth of insight and clarity as to the state of the systems at the time of the event, which can lead to informed or automated responses to security events.
AU-9	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Logical access over the network to the audit systems can be restricted through network policy to prevent unauthorized access. TOS can help to identify and orchestrate network policy to limit accessibility to the audit-related systems. This would be an additional layer of protection relative to a defense-in-depth posture. This requirement is more likely be handled by a third-party solution external to TOS, such as a SIEM solution or the media that is being utilized by the SIEM solution. The intent of this requirement is likely primarily around the application controls and user access controls of the applications that handle audit records, audit settings, and audit reports.
CM-2	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	The capability of TOS, as it pertains to developing, documenting, and maintaining a baseline configuration of the information systems, is limited to providing configuration control specific to baseline network configurations, including firewall configuration and rule bases across multi-vendor, multi-platform technologies. A compliant organization will need to establish baseline configurations for their network and network devices. This includes baseline network topologies, network access, routing, and network security policy, and baseline configurations for network devices. A compliant organization will also be responsible for reviewing baseline configuration standards regularly to identify where standards may need to be modified or updated to better manage risk. These baseline standards, as defined by the organization, can be recorded in SecureTrack and used as a gauge to measure the organization’s compliance posture. These compliance checks can be performed in an automated manner to quickly identify standards violations and allow the organization to address any infractions in a timely manner. Most organizations have both formal and informal IT policies. These IT policies usually establish, through a set of requirements or outcomes, the necessary criteria

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		for defining network security policies. Essentially, the IT policies define what can be permitted and what must be denied in the organization's firewall configurations and policy rule bases. SecureTrack's Best Practices feature enables organizations to create best practice baseline policies and track violations. The administrator creates the best practice baseline policy by selecting audit checks from a list of industry best practice audit checks for firewalls. In order to maintain a certain minimum-security standard in different organizational areas, it is possible to create and maintain a best practices standard for each area. The organization can choose to run a single Best Practices audit that will apply to all monitored devices or create multiple audits, where each audit will apply to different organizational areas according to the organization area's unique security needs. Additionally, firewall policy can be audited against a standard before it is implemented. This pre-audit capability allows organizations to be proactive to ensure compliance with security standards. In addition to the SecureTrack database maintaining the best practice baseline policy, it includes information about network devices such as vendor, version numbers, and patch level. If a baseline policy changes and a new version is needed, the previous versions of that policy are also retained by SecureTrack.
CM-2 (2)	The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	SecureTrack is an automated configuration management tool and can manage the baseline configurations of network devices using policies. Policies are SecureTrack objects that define the baseline configurations of connected devices. SecureTrack maintains the device policies and keeps them up to date by tracking policy revisions. Each authorized change to a device policy creates an updated revision to the policy.
CM-2 (3)	The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.	For policy configuration changes, TOS maintains a history of configuration changes that can be used to roll back changes to a previous baseline if necessary. The retention history is determinable by the organization’s configuration of the network devices which TOS manages. SecureTrack retains the firewall policy configuration that are retrieved from the firewall or firewall manager. Furthermore, TOS backups are configurable to the organization’s needs or requirements.
CM-3	The organization:	SecureChange manages security policy change requests using customizable workflows. From request, design, security assessment, and approval to implementation,

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
	(a) Determines the types of changes to the information system that are configuration-controlled; (b) Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; (c) Documents configuration change decisions associated with the information system; (d) Implements approved configuration-controlled changes to the information system; (e) Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; (f) Audits and reviews activities associated with configuration-controlled changes to the information system; and (g) Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].	SecureChange administers compliance through the correlation of change requests with SecureTrack policies, thereby facilitating reviews of proposed changes with explicit consideration for security impacts. Features in SecureChange support the implementation of approved changes by retaining information about changes to configurations and facilitating the audit and review processes often required in change management policy and process. In addition, SecureChange supports change control oversight activities so that audit and internal oversight requirements are met using on-demand Ticket Query Reports.
CM-3 (1)	The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval; (c) Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period]; (d) Prohibit changes to the information system until designated approvals are received; (e) Document all changes to the information system; and (f) Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed.	SecureChange automates and documents proposed changes to network devices. Each proposed change request generates a change ticket, which is then introduced to a workflow. Custom workflows are created in SecureChange and reflect an organization's internal change control processes; steps in the workflow can mimic a wide array of change process scenarios used in an organization. With SecureChange's ticket handling functionality, Task Handlers (users with authorized roles) have access to proposed change tickets through the SecureChange workflow interface. If the Task Handler is authorized with the role of Approver, unapproved proposed change tickets are explicitly presented for review in the form of Tasks to the Approver. Tasks in a workflow are assigned to a handler; therefore, if approval is the next step in the workflow, the Approver reviews the proposed changes and either approves or rejects the request. If a request is rejected, the workflow does not permit the change to occur. SecureChange workflows within SecureChange can be provisioned to prevent any policy changes from moving through the workflow until approval of the change has been granted. Once a workflow for a change has been approved and implemented, the resulting change ticket that documents

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		the changes is retained in the SecureChange system. A notification is provided to the requester once the change has been made.
CM-3 (2)	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	This is an organizational control to test, validate, and document the changes to the information system before implementing the changes within the operational system. TOS supports this requirement by providing the ability to orchestrate change to network policy through pre-defined workflows, from change request to implementation. In addition, TOS can validate the impact to the change prior to implementation to determine what systems are impacted and what type of impact will occur as a result of the change. The awareness of impact includes everything from how the change affects the availability or reachability of a system to whether the requested change violates policy.
CM-4	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	SecureTrack can support organizational processes designed to determine the potential security impacts of network device changes. Once best practice baseline policies are created, SecureTrack's Best Practices Audit features can then be used to determine if proposed changes to SecureTrack policies could result in security impacts if they were to be implemented.
CM-4 (1)	The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	For changes to network policies, TOS offers impact and risk analysis to identify the impact of the change prior to the change being implemented. TOS provides visibility into change impact through topology diagrams and a report of impacted systems and the expected impact to the system. The flow of change management for network policy changes can include the verification of changes being implemented and tested in a test environment prior to releasing the change implementation to the production environment.
CM-5	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	This is primarily an organizational control. The organization will be responsible for defining, documenting, approving, and enforcing physical and logical access restrictions associated with changes to the information system. TOS can be used to enable logical access restrictions for changes made to the information system. TOS automates the workflow of changes to network policy using customer pre-defined workflows. TOS then applies role-based access controls for the assignment of responsibilities pertaining to the workflow. Workflows can be customized to limit when a change can occur. TOS can identify changes that are made outside of the authorized processes as well as changes that violate

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		security policy. Using TOS SecureChange and SecureApp can allow the organization to abstract the mechanism for executing the change from the network device.
CM-5 (1)	The information system enforces access restrictions and supports auditing of the enforcement actions.	SecureTrack enforces access restrictions using local and external server authentication. External server connection types include LDAP, RADIUS, and TACACS+. SSO via SAML is also a method that SecureTrack uses to enforce access restrictions. Local users can be provisioned in SecureTrack and assigned various permissions, including device permissions which provide appropriate access to connected devices for each user. When using LDAP, permissions in SecureTrack are defined through LDAP group membership. When using RADIUS or TACACS+, user permissions are defined using the same roles and permissions available to local users of SecureTrack. SecureTrack can be configured to use the SecureTrack Audit Trail, which sends syslog messages to an external syslog server. In addition, SecureTrack can retain the same audit trail locally. SecureTrack audits its own system configuration, device monitoring, and analysis and reporting functionalities. SecureChange enforces access restrictions using local and external server authentication. External server connection types include LDAP and RADIUS. SSO is also a method that SecureChange can use to enforce access restrictions. Authorization in SecureChange is implemented through a set of assigned roles defined in SecureChange. SecureApp enforces access restrictions through either user accounts that are configured in SecureChange or user accounts imported from an LDAP server. Roles in SecureApp are assigned to security groups; therefore, users are assigned roles based on the SecureApp group that they are members of.
CM-5 (2)	The organization reviews information system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.	SecureTrack records changes to connected network device configurations and records the changes in policy revisions. SecureTrack's Revision History feature tracks revisions to network device configurations made within the last 72 hours. In addition, audit logs that coincide with each policy revision are generated and retained. SecureTrack's audit logs include the information necessary to determine if unauthorized changes have been made and support organizational review processes conducted for this purpose. SecureChange is connected to and works in conjunction with SecureTrack. Change tickets are created by

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		SecureChange for each proposed change to network devices connected to SecureTrack. Change tickets include the information necessary to determine whether unauthorized changes have been made and support organizational review processes conducted for this purpose. SecureApp is connected to and works in conjunction with both SecureTrack and SecureChange. A SecureChange ticket is initiated when SecureApp changes are requested, and a preconfigured SecureChange workflow is used. Changes to network devices proposed using SecureApp are recorded using the same mechanisms as both SecureTrack and SecureChange. SecureApp also includes the Application History function, used to track changes to applications. Application History, SecureChange tickets, and SecureTrack policy revisions and audit trails support organizational review processes conducted to determine if unauthorized changes have been made.
CM-6	The organization: (a) Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; (b) Implements the configuration settings; (c) Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and (d) Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	SecureTrack can support organizational processes designed to establish and document the configuration settings of connected network devices and implement these configuration settings. Additionally, SecureTrack and SecureChange's change management features support organizational processes to document and approve any deviations from baseline configuration settings as well as support the monitoring and control of changes to configurations.
CM-6 (1)	The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components].	SecureTrack includes automated mechanisms to centrally manage, apply, and verify configuration settings. Each approved policy configuration is monitored and verified by SecureTrack. Verification of policies is accomplished through organizational baseline configurations in SecureTrack being established through organizational authority, then constantly comparing device configuration against the baseline policies.
CM-6 (2)	The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to	SecureTrack supports organizational incident response to unauthorized changes. SecureTrack can respond to unauthorized changes made to network devices whose configurations are monitored by SecureTrack. For

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
	[Assignment: organization-defined configuration settings].	unauthorized and out-of-band changes, such as those that occur through network devices' intrinsic user interfaces or shells, SecureTrack can detect and send notifications and reports to organization personnel. SecureTrack polls each connected network device for device configurations every five minutes by default and compares them with the most recent approved baseline policies retained in SecureTrack. Policy change notifications in SecureTrack can be configured to provide real-time information on changes to monitored policies. Policy change notifications can be sent via SNMP traps or syslog; therefore, an organization's response depends on communication from a SIEM rule or SNMP monitoring system rule to communicate the alert to organizational personnel. SecureTrack's New Revision Report feature can also be configured to directly email reports based on any changes made to monitored device policies. In this scenario, and since SecureTrack polls monitored devices for changes every 5 minutes by default, unauthorized and out-of-band changes such as those that would be done through network devices' intrinsic user interfaces or shells, SecureTrack will detect the new revision of policy and email reports directly to organizational personnel.
CM-7	The organization: (a) Configures the information system to provide only essential capabilities; and (b) Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].	SecureTrack supports an organization's requirements to configure their information systems to provide only essential capabilities and can be configured to restrict the use of protocols, services, and ports to only those which are necessary. SecureTrack provides organizations the tools and functionality necessary to define and adhere to very specific configuration parameters for SecureTrack-monitored and managed network devices.
CM-7 (1)	The organization: (a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and (b) Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].	SecureTrack supports an organization's requirements to review network device configuration parameters to identify unnecessary or insecure network protocols, ports, and services. Additionally, SecureTrack supports an organization's requirements to disable network protocols, ports, and services deemed unnecessary or insecure. SecureTrack's ability to manage network device configurations and retain and control network security policies and baselines aids organizations in making determinations about the relative security of any network protocol, service, or port.
CM-8	The organization: (a) Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system;	SecureTrack can be utilized to support the management of information system component inventories as it pertains to an inventory of networks devices. SecureTrack's Managing Devices interface includes all components connected to and managed by SecureTrack. Once connected to SecureTrack for monitoring, the Name for Display field identifies any

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
	2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and (b) Reviews and updates the information system component inventory [Assignment: organization-defined frequency].	devices added. The Verifying Communication interface in SecureTrack provides an up-to-date status on the presence and communications with connected or disconnected devices, making this interface key to organizations in the determination of component installation, removal, and system updates.
CM-8 (1)	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	Limited to network devices that TOS manages, SecureTrack can be utilized to support the management of information system component inventories. SecureTrack's Managing Devices interface includes all components connected to and managed by SecureTrack. Once connected to SecureTrack for monitoring, the Name for Display field identifies any devices added. The Verifying Communication interface in SecureTrack provides an up-to-date status on the presence and communications with connected or disconnected devices, making this interface key to organizations in the determination of component installation, removal, and system updates.
CM-8 (2)	The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	Limited to network devices which TOS manages, SecureTrack supports automation of the management of a complete and accurate information system component inventory. SecureTrack's Managing Devices interface includes all components connected to and managed by SecureTrack, including information on current configurations. SecureTrack updates the connected device baselines every five minutes by default.
CM-8 (4)	The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.	SecureTrack supports component inventory accountability information and identifies the individuals accountable for administering the network devices connected to SecureTrack. SecureTrack's User Authentication interface provides the full name, username, and permission and role information for any individual assignments to a single domain or multiple domains of managed network devices. In addition to identifying individuals and their scope within the system, contact information in the form of email addresses is provided and can be used for incident response purposes.
IR-4	The organization: (a) Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;	TOS can be helpful for the detection, analysis, and containment of security incidents. SecureTrack can be useful for identifying policy violations and security incidents relative to the observed behavior of traffic on

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
	(b) Coordinates incident handling activities with contingency planning activities; and (c) Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	the network. Workflows can be automated for response to support more rapid containment of security incidents. In addition, TOS supports SOAR system integration. SOAR solutions can gather intelligence from TOS as part of the analysis of events and help inform automated incident response steps.
IR-4 (1)	The organization employs automated mechanisms to support the incident handling process.	TOS can be helpful for the detection, analysis, and containment of security incidents. SecureTrack can be useful for identifying policy violations and security incidents relative to the observed behavior of traffic on the network. Workflows can be automated for response to support more rapid containment of security incidents. The Modify Group field allows organizations to select a group of network objects from a device and select objects to add or remove from the group, and/or provides the ability to create new groups. The TOS admin can add multiple Modify Group fields in a ticket in order to change multiple groups in the same ticket. If the selected group is from a supported device, the changes can be implemented directly to the policy. In addition, TOS supports SOAR system integration. An integrated SOAR can gather actionable intelligence from TOS such as network topology and relevant policy sets at the time of a detected incident.
IR-4 (4)	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	TOS supports SOAR system integration. SOAR solutions can gather intelligence from TOS as part of the analysis of events and to help inform automated incident response steps.
IR-5	The organization tracks and documents information system security incidents.	TOS can be used to support an organization's capability to respond to network-related incidents. Information from TOS can be sued as inputs for an organization's system tracks and documents security incidents.
IR-6 (1)	The organization employs automated mechanisms to assist in the reporting of security incidents.	TOS is used by SOAR systems to assist the organization with the reporting of security incidents pertaining to the network.
SC-2	The information system separates user functionality (including user interface services) from information system management functionality.	The TOS USP can help to identify the separation of system management functions from user functions from a logical network perspective. Policies can be implemented to enforce separation of system management interfaces. TOS provides a web interface and API for the creation and management of firewall rules through the USP. Users of this suite require only authorization to use the suite, while the suite authenticates to individual firewall devices. The Orchestration Suite provides physical separation from the information system environment

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
		being managed via a fully separated hardware infrastructure that houses and runs the suite.
SC-7	The information system: (a) Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; (b) Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and (c) Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	TOS through the USP helps to ensure boundary protections for external system boundaries and key internal boundaries within the system. TOS provides visibility into the network ingress and egress points. TOS APG, through logs ingested from managed network devices, helps create an optimized rule base to limit traffic to what is used or needed by the organization.
SC-7 (3)	The organization limits the number of external network connections to the information system.	TOS can help the organization establish a secure perimeter and monitor the perimeter for changes or policy violations to ensure that the ingress and egress points at the perimeter are limited according to the organization's policy.
SC-7 (4)	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need.	TOS can partially support the organization’s implementation of traffic flow policy and their review of policy exceptions. The organization will be responsible for implementing a managed interface at each external telecommunication service. The organization will be required to establish a traffic flow policy for each managed interface. TOS can be used to monitor and manage traffic flow policy for the managed interface and identity where any policy violations occur. The organization will be responsible for the confidentiality and integrity information being processed, likely using other tools or techniques. The organization will be responsible for documenting exceptions to traffic flow policy with the supporting business need and duration of that need. SecureChange, through the workflow engine, can be used to record policy exceptions and associated mission/business rationale as well as set parameters for the duration of the change. Where duration parameters are set, TOS can be utilized to automate the configuration change to return to the previous state once the approved duration has been met. The organization will be responsible for reviewing the exceptions to traffic flow policy and removing exceptions that are no longer supported. TOS can provide a report of policy exceptions for the organization to review.
SC-7 (5)	The information system at managed interfaces denies network communications traffic by default and allows network communications	When using TOS to orchestrate and automate security policy for network security devices, the default zone in the USP denies all network communications traffic by

ID	CONTROL DESCRIPTION	PRODUCT APPLICABILITY
	traffic by exception (i.e., deny all, permit by exception).	default. Policy by exception is enabled through additional security zones defined per workflow, security zone, or exception.
SC-7 (8)	The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.	Through the USP, TOS can be used to enforce traffic for outbound communications to external networks through authenticated proxy servers at managed interfaces. TOS can also provide visibility, notification, and reporting on exceptions to the policy that route traffic without using the proxy.
SC-7 (21)	The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions].	Through integration with network security devices both at the edge and internally, TOS can be used to orchestrate and automate policy implementation, management, and monitoring for employing boundary mechanisms to separate security zones that are defined by the organization. A USP is a matrix listing all the security zones in the environment and identifies what traffic is allowed between the zones. This allows the organizations to control the actual versus the desired network segmentation, highlighting policy violations before a change is made on the network, so as not to break compliance or expose the network to unnecessary risk. In addition, the management of internal security zones can occur through security domains within TOS to assign roles and responsibilities as they pertain to the security of an administrator's relevant domain.
SI-4 (5)	The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].	TOS can alert and notify an organization in the event of a change to the network configuration that permits traffic flow that previously was not permitted.

Table 1 - Tufin Capability Matrix for FISMA High Requirements

It should be noted that no one technology or tool can fully address or achieve security or compliance. The use of technology and tools is best applied as part of a governance, risk, and compliance program that is comprised of a system of people, processes, and technology.

CONCLUSION

TOS can be an effective tool for an organization that seeks to continually maintain their security and compliance goals. As with any tool, the effectiveness of TOS is directly correlated to an organization's maturity with respect to well-crafted security policies, processes, and standards. Through careful orchestration and automation of network security policy, organizations can effectively maintain compliance while efficiently and more promptly meeting the demands of their users and their customers. TOS integrates into a broad range of physical, virtual, and cloud network device vendor products to enable centralized analysis, design, implementation, management, and monitoring of an organization's network.

With SecureTrack, TOS provides improved visibility of the state and condition of network policy across heterogenous and multi-platform environments and enables organizations to clean up outdated and unused policies; simplify, consolidate, and unify duplicated network policies; address network policies that violate organizational standards; and design comprehensive universal security policy sets that align with an organization's security and compliance goals. Insights into network policy across large and distributed networks can be useful to analyze and design network policy and establish appropriate trust zones for addressing risk and enabling boundaries around an organization's assets. Network and security administrators can review network policy sets, policy exceptions, policy violations, and analyze flow and topology diagrams to gain improved end-to-end insights into their networks. Network architects and designers can use the topology diagrams to validate planned changes for impacts to security and functionality of the network. SecureTrack can also provide visibility into changes that occur to network policy and alert or notify when changes occur outside an organization's approval process.

SecureChange allows an organization to orchestrate and automate change procedures applicable to the architecture, design, and implementation of network security policy. Default and custom processes or steps can be created to guide network changes step-by-step from initial request to board review, security and compliance checks, functional checks, approval, implementation, and testing. The orchestration engine of TOS can support zero-touch automation for the timely implementation of network policy changes while continually maintaining and supporting security and compliance goals and requirements.

SecureApp enables visibility into application connectivity to improve network security. SecureApp helps to provide context to the flow of network connectivity between endpoints by characterizing the traffic and checking the traffic against network security compliance objectives. An organization can identify and reduce connectivity to only that which is necessary for their applications to function properly. This helps to reduce the surface area of attack for applications and enables network security policy to align more appropriately to an organization's applications and software.

Finally, TOS has a rich set of APIs which allow for integration with other toolsets that may be in use by an organization, such as ticketing systems, asset management systems, SIEM solutions, and SOAR solutions, among others. The capabilities of TOS, along with tools from Tufin's alliance partnership, can support improved lifecycle management of an organization's network policies. Coalfire has reviewed TOS capabilities as they align to the support of FISMA High control requirements and determined that TOS can be a useful tool when incorporated into an organization's in-depth security program.

ADDITIONAL INFORMATION, RESOURCES, AND REFERENCES

https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

https://csrc.nist.gov/publications/detail/sp/800-137/final

https://csrc.nist.gov/publications/detail/sp/800-128/final

https://csrc.nist.gov/publications/detail/sp/800-39/final

https://csrc.nist.gov/publications/detail/fips/200/final

https://www.tufin.com/

https://forum.tufin.com/support/kc/latest/index.htm?toc.htm?home.htm?trk=pg-support

ABOUT THE AUTHORS

Fred King | Senior Consultant, Cyber Engineering, Coalfire
Mr. King contributes as an experienced consultant on IT architecture, security compliance, cyber security, and the implementation of effective security controls in diverse environments.

Jason Macallister | Senior Consultant, Cyber Engineering, Coalfire
Mr. Macallister consults on information security and regulatory compliance topics as they relate to advanced infrastructure, emerging technology, and cloud solutions.

Mitch Ross | Contributor | Director, Cyber Engineering, Coalfire
As Director, Mr. Ross contributes as an author and thought leader on information security and regulatory compliance topics for Coalfire's clientele with an emphasis in security in the cloud.

Published September 2019

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public-sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

Tufin Orchestration Suite Applicability Guide for FISMA High-Impact Systems | September 2019