WHITE PAPER

TUFIN ORCHESTRATION SUITE

THROUGH THE LENS OF FISMA

THOMAS BRACKIN | CISSP, CCSK

COALFIRE

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

TABLE OF CONTENTS

INTRODUCTION

The Tufin Orchestration Suite™ (TOS) analyzes the network, automates configuration changes, and proactively maintains security and compliance across an enterprise network. By improving network security processes, the TOS can have a positive impact on businesses by reducing the time and cost to implement configuration changes.

The TOS includes:

- SecureTrack™ – A central management solution for a variety of devices that includes network intelligence and security analysis technologies for network security change automation. SecureTrack helps manage network layer, next-generation, and IPv6 firewalls, as well as network security infrastructure, including routers, switches, and load balancers, from a central platform.
- SecureApp™ – An automated solution that enables organizations to easily define, update, monitor, and remove applications and services from their networks. By providing detailed insight into an application's connectivity needs and status, SecureApp helps to accelerate service deployment, assure business continuity, and simplify network operations.
- SecureChange™ – A comprehensive solution for automating network configuration changes to firewalls and routers. SecureChange enables organizations to dramatically improve their network change process with an automated solution for designing, provisioning, and verifying security configuration changes, so accurate changes can be made faster.

Additionally, for federal agencies, the TOS is designed to meet security control requirements for the Federal Information Security Management Act (FISMA) when deployed in an on-premises IT system. FISMA is federal law passed in 2002 that requires federal agencies to develop, document, and implement an information security program that prescribes to the National Institute of Standards and Technology (NIST) 800-53 security controls and the NIST Risk Management Framework (RMF). The NIST RMF is the product of the Department of Defense, the Office of the Director of National Intelligence, and the Committee on National Security Programs, and was developed to improve information security, enhance risk management processes, and unify agency security standards.

The intent of this white paper is to provide information to IT professionals implementing the TOS within a FISMA-authorized, on-premises IT system to determine that the TOS adheres to the control requirements of the organization and its overall security posture. This white paper assumes that IT professionals will integrate the TOS with an existing FISMA-compliant environment and that supporting controls such as centralized authentication (e.g., Active Directory [AD], centralized log management, analysis and reporting capabilities through a Security Information and Event Management [SIEM] tool, network partitioning and network access control through virtual local area networks [VLANs] and firewalls) are in place and may be integrated with the TOS where appropriate.

For FISMA, IT professionals must develop and maintain a System Security Plan (SSP) that addresses the implementation for each selected control. This white paper outlines the TOS' ability to support the implementation of applicable security controls, enabling IT professionals to update an IT system's SSP to address the secure deployment and use of the TOS. The TOS' features and core capabilities were compared with FISMA High selected controls from NIST Special Publication (SP) 800-53 Revision (Re.) 4 and analyzed for their ability to impact or support control requirements.

This white paper only addresses control requirements relevant to the deployment, configuration, and maintenance of the TOS with other control requirements omitted under the assumption that these will be addressed by underlying IT infrastructure. Control requirements were not independently tested by Coalfire. The opinions in this white paper represent Coalfire's judgement of documented TOS features and controls

from interviews with key Tufin personnel, product demonstrations, and published information sources supplied by Tufin.

TUFIN ORCHESTRATION SUITE

TOS is a policy-centric solution for automatically analyzing risk and designing, provisioning, and auditing network security changes. TOS reduces the attack surface and minimizes disruptions to critical applications. Its network security automation enables enterprises to implement security changes in minutes instead of days with continuous compliance and increased agility.

TOS provides multi-vendor device support for enterprise networks, including finance, telecommunications, energy and utilities, healthcare, retail, education, government, manufacturing, transportation, and auditing. Tufin's Technology Alliance involves a close partnership with industry leaders to provide integration of the award-winning TOS with their solutions.

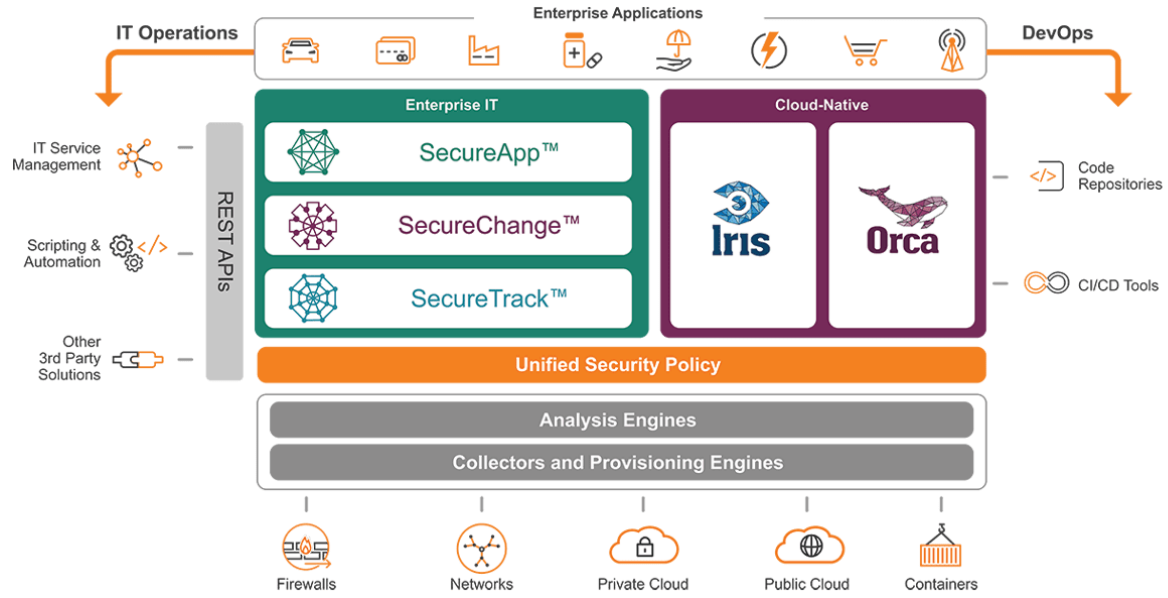

Figure 1: Overview of the Tufin Orchestration Suite

SUMMARY OF CORE FUNCTIONALITY – SECURETRACK

SecureTrack is a comprehensive management solution for firewalls and additional network devices. Today's enterprise networks are complex and diverse, including thousands of firewalls, routers, switches and load balancers from multiple vendors. As a result of frequent changes required by networked enterprise applications, device configurations need to be constantly modified, and have grown increasingly large and complex.

SecureTrack provides security and network engineers the visibility and insight to help ensure that security policies are optimized to enable business functionality while meeting stringent security and compliance requirements. It enables engineers to track and analyze network device configurations, optimize and recertify firewall rules, design changes, and enforce continuous compliance across a network.

SUMMARY OF CORE FUNCTIONALITY – SECURECHANGE

SecureChange is an essential part of TOS that provides a comprehensive solution for automating network configuration changes to firewalls and routers. Many IT organizations receive numerous network

configuration change requests per week. The accelerated pace of business can make it unfeasible for network security administrators to handle configuration changes manually. IT automation can help achieve agility while enforcing security policy across the network.

SecureChange enables organizations to dramatically improve their network change process with an automated solution for designing, provisioning, and verifying security configuration changes. From the initial request to the final configuration audit, SecureChange streamlines processes and improves accuracy, so organizations can make changes faster.

SUMMARY OF CORE FUNCTIONALITY – SECUREAPP

The servers that an application uses are often spread across the network and rely on rules in multiple firewalls to make sure that communication can pass through the network. SecureApp can enable business owners without network management experience to define servers and services for the application and track implementation progress. Based on the topology of the network and the policy revisions retrieved from the network devices, SecureApp can translate requirements into specific changes that network and security teams should make in all of the relevant firewall policies.

SecureApp includes an interface that helps organizations define application-critical connections. Organizations can see a list of applications, the connectivity that those applications rely on, and the status of the connectivity. SecureApp can also allow customers to see if connections for an application are blocked and send a request to repair the connectivity.

ARCHITECTURE

Scalable Deployment Capabilities

TOS is designed for scalability and can be used in businesses ranging from small offices to large enterprises, as well as Managed Security Service Providers (MSSPs).

For large environments, TOS can be deployed with the following:

- **High Availability (HA)** – Uses multiple TOS servers to provide redundancy and disaster recovery.
- **Distributed Architecture** – Uses additional SecureTrack servers to collect revisions and send them to a central SecureTrack server for comparison, analysis, and reporting. Distributed architecture can be achieved with distribution servers or remote collectors.
- **Multi-Domain Management** – Helps organizations divide devices into domains and manage access to network information in SecureTrack and SecureChange with user and group permissions.

High Availability

HA provides minimal downtime and data loss in the event of a server failure, site failure, or scheduled maintenance. TOS data is automatically synchronized from an active TOS server to a standby TOS server to maintain maximum data integrity and continuity during the failover process. The standby TOS server can be located on-site or at a remote disaster recovery location.

In TOS HA, the active TOS server runs TOS and sends database updates to the standby server in real-time. The database updates include all configuration and policy changes. TOS is installed on the standby server but is not enabled. The active server sends write-ahead logs to reduce the possibility of lost database transactions. During a failover, TOS is enabled on the standby server and can receive connections from clients and devices.

Distributed Architecture with Distribution Servers

In a distributed architecture using distribution servers, organizations can also implement HA for a central server. All TOS applications run on the active central server, and a second central server can be set up as the standby central server.

The two central servers use a heartbeat interface to determine the liveness of the other server. When communication fails on the heartbeat connection, the standby central server becomes the new active central server.

The central servers must be configured to use a virtual Internet Protocol (VIP) address to allow traffic to be redirected to the active HA server. All communication from the distribution servers to the central server uses the VIP address to ensure that traffic is directed to the active HA central server.

Distributed Architecture with Remote Collectors

In a distributed architecture using remote collectors, organizations can also implement HA for a central server. All TOS applications can be run on an active central server. A second central server can be set up as the standby central server.

The two central servers use a heartbeat interface to determine the liveness of the other server. When communication fails on the heartbeat connection, the standby central server becomes the new active central server.

The central servers must be configured to use a VIP address, to allow traffic to be redirected to the currently active HA server. All communication from the remote collectors to the central server uses the VIP address, to help ensure that traffic is always directed to the active HA central server.

Multi-Domain Management

MSSPs and large enterprises often must control the provisioning process for many groups, such as customers or departments. Each group often has network devices that secure their network segments. These groups must be able to manage their devices and control access to their network information, including scenarios of IP overlapping, multi-tenancy and cloud networks.

In SecureTrack, organizations can create domains and then assign devices and users to domains. Devices can include physical network devices, virtual devices on multi-tenant platforms, or cloud platforms. Users can access devices according to the permissions they are given. Administrators are only able to view devices that are in their domains, and may only use reports, queries, audits, and alerts for those devices. Super administrators can see devices for multiple domains and run reports, queries, audits, and alerts for all those devices.

In SecureChange, organizations can assign SecureChange domains to users and groups. When selecting devices for tickets, such as in access requests, users and groups assigned to domains can only select devices in those domains. This segregation of data can help in scenarios in which multiple groups of administrators are responsible for separate areas of the network. Organizations can assign the groups to separate domains and each group can only see the devices for its domain.

In SecureApp, organizations can import a list of domains as customers and define applications according to the customers that use the applications to allow for the following:

- **Data segregation** Connections can only contain resources that belong to related customers.
- **IP address segmentation** If different customers use the same IP address scheme in their networks, causing IP overlapping, SecureApp can analyze traffic for each customer separately.

Required Ports and Services

Organization firewalls must allow communication between SecureTrack and monitored devices and between SecureChange and other network resources. Tufin user guides specify detailed ports and services settings for integrating the software suite into a specific environment.

Supported Application Integrations

Note: The listings below are applicable to the latest hotfix available for this release.

Organizations can configure SecureTrack to monitor and analyze various brands of devices. Please refer to official Tufin documentation for specific versions and models that are supported. Below is a general list of vendors which TOS supports:

- Amazon Web Services (AWS)
- Check Point
- Cisco
- F5
- Forcepoint Stonesoft
- Fortinet
- Juniper
- Linux Netfilter
- Microsoft Azure
- OpenStack
- Palo Alto Networks
- Symantec Blue Coat
- VMware

With an appropriate Tufin Open Platform (TOP) plugin, SecureTrack can monitor a device's configuration if it can be retrieved as a standard exported text file. To develop a TOP plugin, see the TOP Developer Alliance (http://www.tufin.com/partners/top-developer-alliance/). Additional TOP plugins are available from Tufin at the following link: https://portal.tufin.com/aspx/TechnicalDocument.

Minimum Hardware Requirements

The minimum hardware configuration is adequate for a very small environment and provides minimal capacity for viewing and evaluating TOS functionality.

TOS requires the following minimum hardware specifications:

- **CPU:** 24 cores
- **Memory:** 32 GB
- **Storage:** 2 x 1 TB SATA HDD in RAID 1 (total 1 TB)

Browser hosts require at least 4 GB of RAM to view the large policies necessary for SecureTrack access. If the browser host does not have at least 4 GB of RAM, policies with tens of thousands of rules may not be able to be displayed in the browser.

Recommended Hardware Requirements

Note: The minimum recommended hardware configuration is the minimum required for a production environment. Actual hardware requirements can vary, depending on device and traffic environment, the number of firewalls in use, whether rule and object usage analyses are enabled, expected syslog traffic volume, and more. Sales engineers can be contacted for assistance in determining your specific hardware requirements.

Tufin recommends the following minimum hardware specifications for running TOS in a production environment:

- **CPU:** 32 cores
- **RAM:** 64 GB
- **Storage:** 4 x 1 TB SSD in RAID 10 (total 2 TB)

Tufin recommends that customers install TOS on a newly installed server class computer or VMware virtual machine that has not been previously used for any other purpose. Tufin recommends that organizations use a designated server for TOS.

Operating System Requirements

TOS can be supported on these 64-bit operating systems:

- For TufinOS 2.x, version 2.10 or higher.

  Note: TufinOS is only supported on preinstalled Tufin appliances, VMware ESX 4.0 or higher with 64-bit compliant cores, or Oracle VM VirtualBox (TufinOS 2.5 or higher).

  Note: TufinOS 1.x reached its end of life (EOL) on March 31, 2017, at the same time as Centos 5 (https://wiki.centos.org/FAQ/General#head-fe8a0be91ee3e7dea812e8694491e1dde5b75e6d). After this date, no updates or security patches will be created for TufinOS 1.x. Tufin strongly recommends that organizations migrate to TufinOS 2.x.
- Red Hat Enterprise Linux (RHEL) 6 (English version only; for other versions, organizations should contact Tufin support)
- CentOS 6 (English version only; for other versions, organizations should contact support)

FISMA COMPLIANCE WITH TUFIN ORCHESTRATION SUITE

OVERVIEW

Coalfire has evaluated applicable security controls in scope for integrating TOS into an existing FISMA High environment. The following tables provides Tufin's integration descriptions of select FISMA High security control implementations from NIST SP 800-53 Rev. 4. Customers can leverage this information to make an informed decision before implementing TOS within their existing FISMA-authorized solution in accordance with FISMA requirements and security best practices. Each table below includes columns for Control ID, Control Name, and Implementation Description:

ACCESS CONTROL

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
AC-2 (1)	Account Management | Automated System Account Management	TOS, when integrated with an existing identity management store leveraging single sign-on, Remote Authentication Dial-In User Service (RADIUS), or Terminal Access Controller Access-Control System (TACACS+), can enable customers to support the management of TOS accounts.
AC-4	Information Flow	TOS supports the use of single sign-on, RADIUS, and TACACS+ to enable customers to integrate TOS into an organization's existing information control flow policies.
AC-6 (10)	Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions	TOS functionality requires authentication, and as a result, when integrated with an existing identity management store leveraging single sign-on, RADIUS, or TACACS+, can enable customers to prevent non-privileged users from executing privileged functions through integration with an organization's existing privileged access policies.
AC-8	System Use Notification	Customers can configure TOS to present users with a notification banner in accordance with NIST 800-53 requirements, federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
AC-17	Remote Access	All TOS functionality requires authentication. TOS supports the use of single sign-on, RADIUS, and TACAS+ to help enable customers to integrate to manage remote access policies. Customers can leverage TOS to manage policies to restrict and enable remote access to privileged and non-privileged users.
AC-17 (2)	Remote Access | Automated Monitoring / Control	The TOS web access portal supports the use of Transport Layer Security (TLS) for encryption in transit.

AUDIT AND ACCOUNTABILITY

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
AU-2	Audit Events	TOS generates audit records for all events that occur within TOS through ticket history and log files written to the operating system.

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
AU-2 (3)	Audit Events | Reviews and Updates	When Tufin develops a new feature within the software, Tufin developers and code reviewers ensure that actions taken in the new feature are logged accordingly.
AU-3	Content of Audit Records	TOS-generated audit records contain the following information: • What type of event occurred • When the event occurred • Where the event occurred • Source of the event • Outcome of the event • Identity of any individuals or subjects associated with the event
AU-3 (1)	Content of Audit Records | Additional Audit Information	TOS generates audit records for all events that occur within the system with as much detail about the event as available.
AU-7	Audit Reduction and Report Generation	TOS logs all events into log files on the local machine to enable customer-configured SIEM solutions in the implementation of AU-9. SecureChange and SecureApp also maintain events in ticket history in a manner protected from unauthorized access, modification, and deletion. These audit events can be downloaded from the system to support after-the-fact investigations.
AU-8	Time Stamps	TOS has been designed to leverage Network Time Protocol (NTP) servers and utilize OS system clocks to generate and record time stamps for audit records that can be mapped back to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).
AU-8 (1)	Time Stamps | Synchronization with Authoritative Time Source	TOS can be configured by customers to compare internal system clocks to authoritative time sources (e.g., NTP servers) on an organization-defined frequency.
AU-9	Protection of Audit Information	TOS logs all events into log files on the local machine to enable the use of customer-configured SIEM solutions in the implementation of AU-9. SecureChange and Secure App also maintain events in a ticket history that is protected from unauthorized access, modification, and deletion.

CONFIGURATION MANAGEMENT

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
CM-1	Configuration Management Policy and Procedures	Tufin has developed software development life cycle (SDLC) documentation that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This documentation is given to all developers upon hire and is re-distributed when changes are made to the documentation, which occurs at least annually and as required. The documentation lays out all the procedures that facilitate the implementation of the configuration management policy and specifies what tools are used, as well as how they are used, to meet the SDLC requirements.
CM-2	Baseline Configuration	Tufin develops, documents, and maintains a baseline configuration through software development tools such as Git and other commercial software development tools used throughout the SDLC.

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
CM-2 (3)	Baseline Configuration | Retention of Previous Configurations	Tufin development teams utilize Git for management of source code. Git allows for rollback of code changes natively.
CM-6	Configuration Settings	As part of Tufin's SDLC practices, developers trained to harden default configurations for software products to the strictest possible security levels in accordance with deny-by-default policy and the principle of least privilege. When an end customer installs TOS, they must configure TOS to allow for any functionality by opening ports as applicable to their system. All TOS configuration defaults are available under configuration control with the rest of the software codebase.

CONTINGENCY PLANNING

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
CP-9	Information System Backup	TOS supports customers in fulfilling CP-9 requirements by allowing for full backups to be run on demand.
CP-10	Information System Recovery and Reconstitution	TOS administrator documentation, found on the Tufin support website, describes how customers can support the implementation of CP-10 through database and software recovery in the event of disruption, compromise, or failure.
CP-10 (2)	Information System Recovery and Reconstitution | Transaction Recovery	TOS utilizes database technologies that include transaction recovery by default. Tufin provides user-facing documentation on HA configurations to allow for database replication. Tufin also provides customers with detailed instructions within their user portal, which describes how to automate database backups to allow for quicker recovery.

IDENTIFICATION AND AUTHENTICATION

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
IA-2	Identification and Authentication (Organizational Users)	TOS supports the capability of an organization's information system to uniquely identify and authenticate organizational users and process actions on the behalf of organizational users. Actions performed by the TOS server can be uniquely authenticated and identified to support after-the-fact reviews. TOS logs the username or ID of users that initiate an action in all historical logs. Additionally, TOS supports integration with an organization's existing single sign-on, RADIUS, or TACACS+ solution. TOS does not currently support Personal Identity Verification (PIV) or multi-factor authentication for local accounts but plans to provide this functionality in a future release. Customers should implement these requirements utilizing their single sign-on solution to meet the control requirements.
IA-6	Authenticator Feedback	TOS is configured so that credentials are obscured as they are entered into the Tufin web portal for login.

INCIDENT RESPONSE

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
IR-4	Incident Handling	Tufin has defined internal incident handling procedures in their SDLC to address preparation, detection, analysis, containment, eradication, and recovery. In the event of an incident, the Tufin security team triages and classifies software vulnerabilities that are coordinated with software development teams for remediation planning. The Tufin security team notifies customers using announcements and by posting the threat in a security advisory, which includes a resolution timeline and mitigation strategy for the vulnerability. Once the vulnerability is remediated, the Tufin security team incorporates lessons learned into their SDLC process.
IR-5	Incident Monitoring	TOS vulnerability incidents are tracked and documented in an internal tracking system and used to inform software development for incident remediation.
IR-7	Incident Response Assistance	Tufin Support offers advice and assistance to customers regarding incidents and vulnerabilities involving TOS as well as third-party software bundled with TOS.
IR-8	Incident Response Plan	Tufin SDLC documentation includes the basics of incident handling which the Tufin security team has determined to meet the requirements of the company. This documentation is reviewed and approved by the appropriate parties to ensure that Tufin is sufficiently covered in incident handling and can provide customers with expedient vulnerability remediation.

RISK ASSESSMENT

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
RA-5	Vulnerability Scanning	As part of its SDLC practices, Tufin implements code scanning tools to detect vulnerabilities in code. Tufin also monitors third-party dependencies for vulnerabilities and patches as necessary before software packages are released. Tufin also incorporates lessons learned into the SDLC, which are used to help prevent previously detected vulnerabilities from appearing in future scans by alerting developers to insecure coding practices.
RA-5 (1)	Vulnerability Scanning | Breadth / Update Tool Capability	Tufin utilizes modern code scanning tools that allow for updates to the database of known vulnerabilities that the scanner is scanning against.

SYSTEM AND SERVICES ACQUISITION

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
SA-2	Allocation of Resources	Tufin allocates discrete resources to meet security requirements during the software development process. Security and development practices are documented in internal documentation in order to ensure that security practices are integrated into the software planning process.

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
SA-3	System Development Life Cycle	Tufin manages the development of software through the implementation of their SDLC documentation which, along with the SDLC documentation, incorporates security considerations in the development process. Tufin has a designated security team responsible for responding to security incidents and classifying any vulnerabilities in the software. Tufin then integrates all security processes into the development lifecycle by working with the development team to remediate vulnerabilities.
SA-4 (2)	Acquisition Process | Design / Implementation Information for Security Controls	TOS has been evaluated by Coalfire to develop a Product Applicability Guide. This guide provides details on how organizations can meet security control requirements by utilizing TOS. This information can be found on the Tufin support webpage. Additionally, TOS has thorough administrator guides that detail how to implement various security features in the product.
SA-4 (9)	Acquisition Process | Functions / Ports / Protocols / Services in Use	By default, TOS installs in the most restrictive state possible, with only functional components able to communicate with each other. End customers must configure the software to allow ports and protocols outside of the installed system to be used.
SA-5	Information System Documentation	TOS has been evaluated by Coalfire to develop a Product Applicability Guide. This guide provides details on how organizations can meet security control requirements by utilizing TOS, and can be found by contacting Tufin support. Additionally, TOS has thorough administrator guides that detail how to implement various security features in the product. Tufin reports all vulnerabilities and their mitigations through their customer portal.
SA-8	Security Engineering Principles	Tufin incorporates security engineering principles into all stages of the development of the TOS. In Tufin SDLC documentation, security engineering principles are considered and applied to TOS during the following activities: • Specification • Design • Development • Implementation • Modification
SA-9 (2)	External Information System Services | Identification of Functions/Ports/Protocols /Services	By default, TOS installs in the most restrictive state possible with only functional components able to communicate with each other. End customers must configure the software to allow ports and protocols outside of the installed system to be used.
SA-10	Developer Configuration	As a part of the SDLC, Tufin developers follow defined configuration management processes, which include the following: • Integrity verification • Requirement of secondary approvals for changes • Security testing

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
		All change approvals and security testing issues are tracked in the internal tracking system, which is used by the security and development team for constant cross-team communication.
SA-15	Development Process, Standards, and Tools	Tufin has developed SDLC documentation that addresses security requirements and identifies standards and tools for development. All parts of the SDLC process are documented in the internal tracking system to ensure that integrity is maintained throughout the process. The Tufin Security and Development teams constantly review the development process to ensure that tools, standards, and configurations meet the requirements of the organization.
SA-16	Developer-Provided Training	Tufin documentation is provided for customers to assist with the implementation of the security features built into TOS.
SA-17	Developer Security Architecture and Design	Tufin provides support for customers to integrate software securely into their environment and meet any security architecture or design specifications required by the customer.

SYSTEM AND COMMUNICATIONS PROTECTION

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
SC-8	Transmission Confidentiality and Integrity	TOS utilizes strong encryption algorithms by default, including TLS for data in transit.
SC-12	Cryptographic Key Establishment and Management	TOS encrypts databases used by the software by default using AES 256-bit encryption. The keys for encryption are managed by the software and are not able to be accessed by anything other than the software.
SC-13	Cryptographic Protection	TOS encrypts databases used by the software by default using AES 256-bit encryption. The keys for encryption are managed by the software and are not able to be accessed by anything other than the software.
SC-18	Mobile Code	TOS utilizes mobile code in user-facing web portals. Tufin development practices require mobile code to be created using the same SDLC process as other code and is required to go through code checks for security issues.
SC-28	Protection of Information at Rest	TOS encrypts databases used by the software by default using AES 256-bit encryption. The keys for encryption are managed by the software and are not accessible by anything other than the software.

SYSTEM AND INFORMATION INTEGRITY

CONTROL ID	CONTROL NAME	IMPLEMENTATION DESCRIPTION
SI-2	Flaw Remediation	As a part of the SDLC, Tufin identifies, reports, and corrects flaws in software. All software security testing is done with automated tools and issues are tracked in the internal tracking system for remediation by developers. Additionally, all software packages are tested prior to release for security issues. Tufin also monitors third party software packages for the latest releases to incorporated updates in their software packages.
SI-2 (1)	Flaw Remediation | Central Management	Tufin Security and Development teams track flaw remediation in a central location using the internal tracking system.
SI-2 (2)	Flaw Remediation | Automated Flaw Remediation Status	The Tufin SDLC process utilizes scanning tools, which automatically test software for security flaws during the development process.
SI-5	Security Alerts, Advisories, and Directives	Tufin provides alerts to customers on any security vulnerabilities in TOS, as well as steps to mitigate the vulnerabilities and timelines for remediation.
SI-7	Software, Firmware, and Information Integrity	Tufin performs integrity verification on software packages before public release and provides hashes to customers for them to perform their own integrity checks.
SI-7 (1)	Software, Firmware, and Information Integrity | Integrity Checks	Tufin performs integrity verification on software packages before public release and provides hashes to customers for them to perform their own integrity checks.
SI-11	Error Handling	When an error occurs in TOS, the message displayed to end users is generic and reveals no sensitive information. Only customer administrators can view detailed error information.

CONCLUSION

TOS can be implemented in an existing FISMA-authorized environment in a manner that can maintain existing security posture and can support compliance assurance. Federal agency IT professionals can deploy the solution into their environment knowing that the security controls detailed in this white paper support and meet FISMA compliance requirements. The built-in capabilities and mechanisms of TOS can help ensure that security and compliance requirements are maintained while offering cost savings and efficiencies.

ABOUT THE AUTHOR

Thomas Brackin | Senior Manager, FedRAMP and Assurance Services, Coalfire

Mr. Brackin leads engagements with clients looking for FedRAMP or FISMA accreditations as an experienced subject matter expert on cloud technologies, security best practices, secure software development practices, and the implementation of NIST 800-53 compliant security controls in cloud environments.

Published September 2019

ABOUT COALFIRE

Coalfire is the trusted 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 nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.