tufin The Security Policy Company.

Tufin Vulnerability Mitigation App

Leverage Tufin's Network Insights and Business Context with Vulnerability Data to Prioritize Remediation Efforts and Automate Mitigation

Tufin Vulnerability Mitigation Application integrates with leading vulnerability management solutions to enrich vulnerability intelligence with real-time network insights, ensuring effective remediation and automated mitigation via a risk-based approach.

The Tufin Vulnerability Mitigation app enables organizations to prioritize remediation and mitigation efforts by enhancing vulnerability scanner output with network insights. By combining vulnerability measures (CVSS and severity) with insights into how these vulnerabilities may be accessed and exploited via the network, admins have the context to identify and address the vulnerabilities that pose the greatest threat to critical business assets.

The app enables the integration between Tufin's SecureTrack, SecureChange, and leading vulnerability management solutions, including Tenable.io, Tenable.sc, Qualys VMDR, Rapid7 Nexpose, and Rapid7 insightVM.

This solution can be downloaded directly from the Tufin Marketplace.

Prioritize Remediation and Mitigation Efforts

The biggest challenge with vulnerability scans has always been too many critical vulnerabilities are discovered, and not enough resources are available to patch them. Organizations need a way to prioritize the vulnerabilities that should be patched first based on the risk they introduce to their business, and find a way to mitigate the risk until all patches can be fully addressed.

Assess Risk to Critical Assets

The Tufin Vulnerability Mitigation app retrieves vulnerability scan results and displays them in Tufin's vulnerability dashboard. To save you time and effort, and identify the riskiest vulnerabilities to your business, you can choose to start with high-value network segments first, the same segments/zones that you defined in Tufin SecureTrack.

For MSSPs or large organizations using more than one vulnerability management solution, you can consolidate multi-vendor scan results – all from a single dashboard.

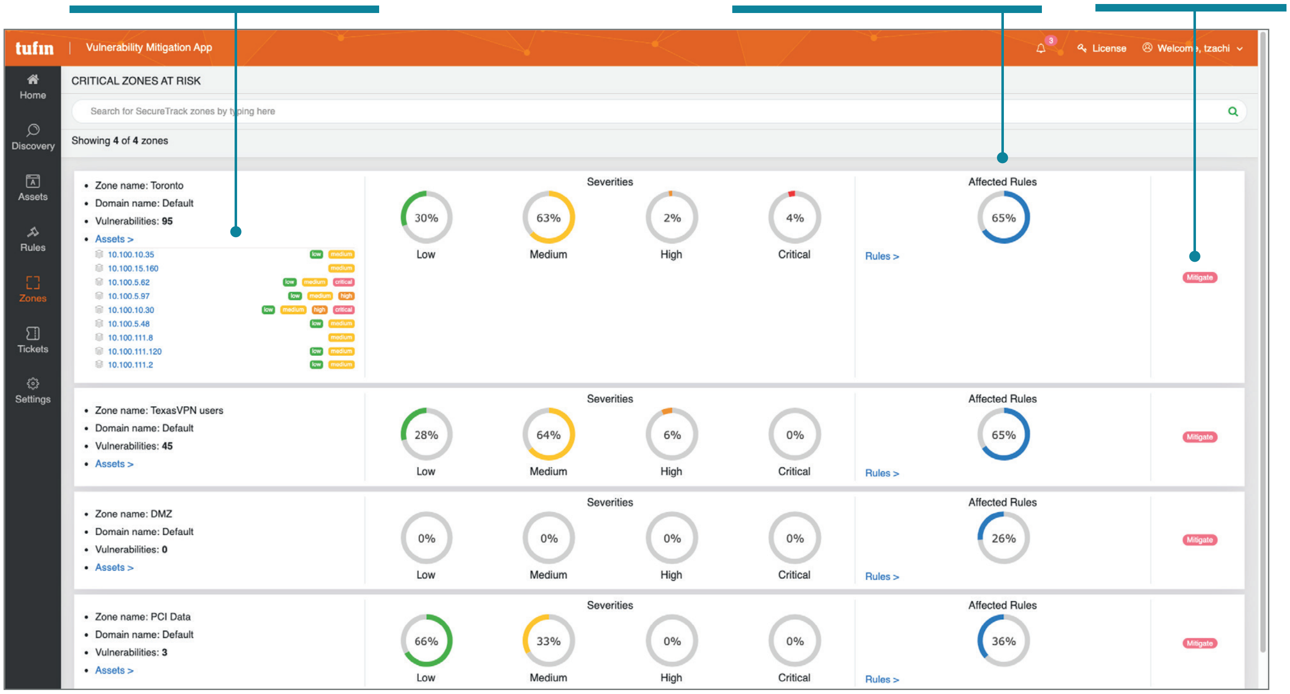
Highlights

- Prioritize vulnerability remediation efforts based on exposure of critical assets as well as severity of vulnerabilities
- Easily assess overall risk to critical assets resulting from vulnerabilities that are both accessible and exploitable
- Automate risk mitigation by blocking access to the critical asset until remediation efforts can be fully implemented
- Monitor and measure risk exposure over time via a comprehensive dashboard that highlights overall vulnerability exposure networkwide and the impact of mitigation and remediation efforts

Network segments' assets by vulnerability severity

Percent of total rules exposing this network segment

Generate mitigation workflow



CRITICAL ZONES AT RISK

Search for SecureTrack zones by typing here

Showing **4** of **4** zones

- Zone name: Toronto
- Domain name: Default
- Vulnerabilities: **95**
- Assets >

10.100.10.35	low medium
10.100.15.160	medium
10.100.5.62	low medium critical
10.100.5.97	low medium high
10.100.10.30	low medium high critical
10.100.5.48	low medium
10.100.111.8	medium
10.100.111.120	low medium
10.100.111.2	low medium

- Zone name: TexasVPN users
- Domain name: Default
- Vulnerabilities: **45**
- Assets >

- Zone name: DMZ
- Domain name: Default
- Vulnerabilities: **0**
- Assets >

- Zone name: PCI Data
- Domain name: Default
- Vulnerabilities: **3**
- Assets >

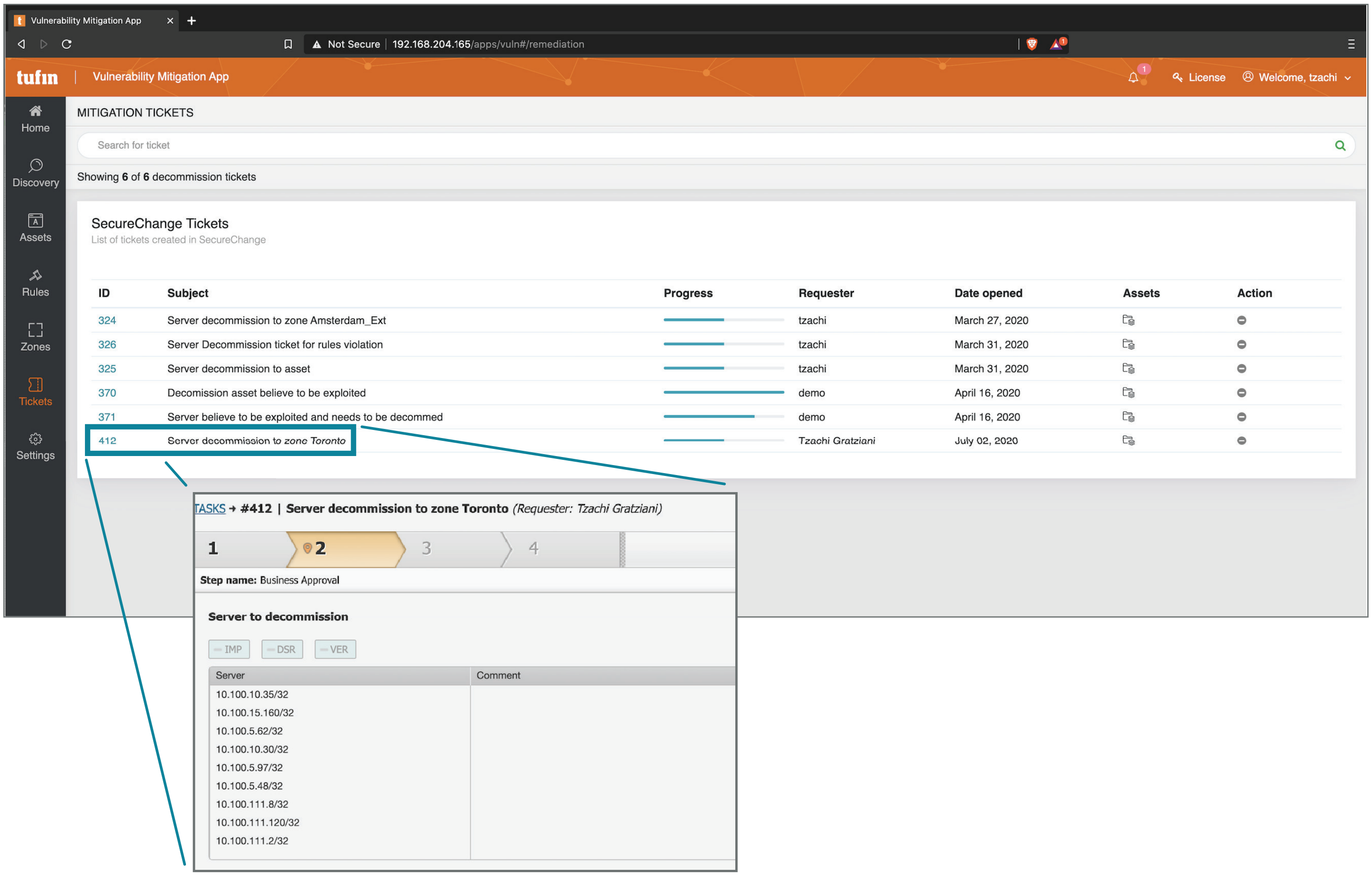
Zone	Severities: Low	Medium	High	Critical		Affected Rules	
Toronto	30%	63%	2%	4%	Rules >	65%	Mitigate
TexasVPN users	28%	64%	6%	0%	Rules >	65%	Mitigate
DMZ	0%	0%	0%	0%	Rules >	26%	Mitigate
PCI Data	66%	33%	0%	0%	Rules >	36%	Mitigate

Prioritize security efforts based on your most vulnerable and critical network segments

The Tufin Vulnerability Mitigation app lets you view list of exposed vulnerable assets within the specified network segments and their vulnerability severity levels. You can also view the rules that enable access to and from a vulnerable asset, the underlying services exposing the vulnerabilities, and relevant firewalls that provide access. Through the vulnerability dashboard, you can track remediation and mitigation trends over time to help determine how your efforts are reducing your attack surface.

Mitigate by Removing Access

There are scenarios where patching is not always an option. For example, a patch may not be available or, if available, performing a patch may require costly downtime. And yet, your security standards and regulations may prevent use of the affected applications until known high-risk vulnerabilities are resolved. Tufin offers a process that can help address these situations.



MITIGATION TICKETS

Showing **6** of **6** decommission tickets

SecureChange Tickets

List of tickets created in SecureChange

ID	Subject	Progress	Requester	Date opened	Assets	Action
324	Server decommission to zone Amsterdam_Ext		tzachi	March 27, 2020	🗂	⊖
326	Server Decommission ticket for rules violation		tzachi	March 31, 2020	🗂	⊖
325	Server decommission to asset		tzachi	March 31, 2020	🗂	⊖
370	Decomission asset believe to be exploited		demo	April 16, 2020	🗂	⊖
371	Server believe to be exploited and needs to be decommed		demo	April 16, 2020	🗂	⊖
412	Server decommission to zone Toronto		Tzachi Gratziani	July 02, 2020	🗂	⊖

TASKS → **#412 | Server decommission to zone Toronto** *(Requester: Tzachi Gratziani)*

1 | 2 | 3 | 4

Step name: Business Approval

Server to decommission

Server	Comment
10.100.10.35/32	
10.100.15.160/32	
10.100.5.62/32	
10.100.10.30/32	
10.100.5.97/32	
10.100.5.48/32	
10.100.111.8/32	
10.100.111.120/32	
10.100.111.2/32	

Remove network access associated with vulnerable asset through Tufin's pre-configured server decommissioning workflow

Using **Tufin's Vulnerability Mitigation app,** you can remove all network access associated with the vulnerable asset through Tufin's pre-configured server decommissioning workflow, an automated process initiated directly from the app.

Tufin SecureChange then streamlines the network change implementation process to locate and update all rules enabling access to this vulnerable asset in all relevant network security devices and infrastructure components, such as firewalls, SDNs, routers, and security groups across the hybrid environment. The necessary rule changes are designed and implemented, automatically removing access to the vulnerable asset. Tufin then validates that the change was implemented as intended. It's a fully automated and tracked process that can be managed directly from the app.

Through this process, the Tufin Vulnerability app allows you to mitigate the risk of unpatched vulnerabilities that put your high-value assets at risk.

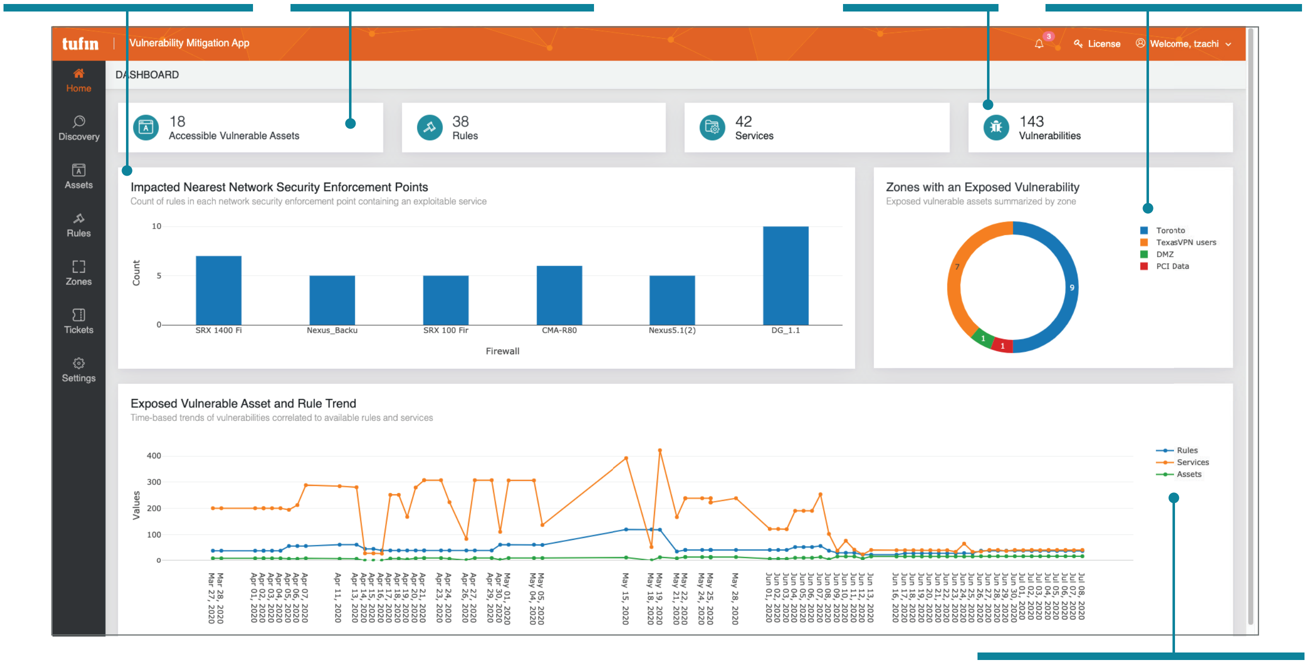
Track Results of Mitigation and Remediation Efforts

Identify which infrastructure provides the most exposure

Identify which assets are exposed through the rules and services by which they are exploitable

Total number of vulnerabilities in accessible assets

Understand which network segments are most impacted



Understand influence of remediation and mitigation efforts

To help prioritize your next steps, the app displays the creation, modification and actual usage of the rules that enable access to high-value assets. It allows you to identify if the rule was used, and therefore, how often the vulnerable asset has been accessed. If a rule, for example, has not been hit in the last 6 months, there will be limited or no business impact if you block access to the asset. However, if the rule is being used, before you make any changes, you will want to consider the following:

- What comments are associated with the rule?
- Is this rule being used?
- Is this rule included in recertification/removal processes?

Once you have all of this information, you'll be able to assess the business impact of limiting (or blocking) access to a vulnerable asset.