tufin The Security Policy Company.

技术合作伙伴解决方案简介

漏洞缓解应用程序

根据漏洞数据，利用Tufin的网络洞察力和业务背景，确定修复任务的优先次序，并自动进行缓解

Tufin漏洞缓解应用与领先的漏洞管理解决方案相集成，通过实时网络洞察力丰富漏洞情报，利用基于风险的方法进行有效的修复和自动缓解。

Tufin Vulnerability Mitigation应用程序通过增强漏洞扫描器输出与网络洞察力，使企业能够对修复和缓解任务进行优先排序。通过结合漏洞措施（CVSS和严重性）与洞见这些漏洞会如何通过网络被访问和利用，管理员将能够识别并解决对关键业务资产构成最大威胁的漏洞。

该应用可实现Tufin的SecureTrack、SecureChange和领先的漏洞管理解决方案之间的集成，包括Tenable.io、Tenable.sc、Qualys VMDR、Rapid7 Nexpose和Rapid7 insightVM。

该解决方案可直接从Tufin Marketplace下载。

对修复和缓解任务进行优先排序

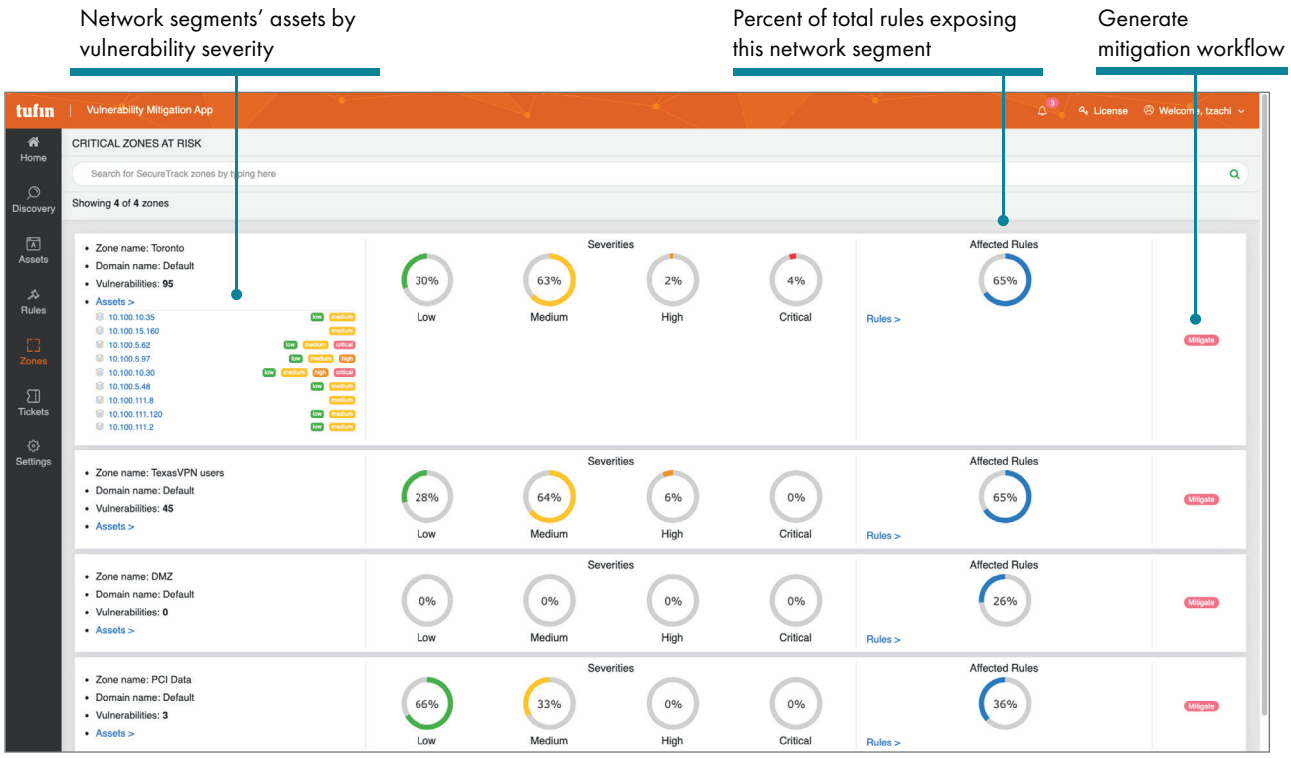
漏洞扫描的最大挑战一直是发现了太多的关键漏洞，却没有足够的资源来修补这些漏洞。组织需要一种方法，根据漏洞对业务造成的威胁，确定应该优先修补的漏洞，并找到一种方法来减轻风险，直到安装所有补丁。

评估对关键资产的威胁

Tufin漏洞缓解应用程序检索漏洞扫描结果，并将其显示在Tufin的漏洞控制面板中。为了节省您的时间和精力，并识别对您的业务威胁最大的漏洞，您可以选择先从高价值的网络段开始，也就是您在Tufin SecureTrack中定义的段/区。
对于使用一个以上漏洞管理解决方案的MSSP或大型组织，您可以从一个单一的控制面板整合多个供应商的扫描结果。

亮点

- 根据关键资产的暴露程度和漏洞的严重程度，确定漏洞补救任务的优先次序
- 轻松评估可访问和可利用的漏洞对关键资产的整体威胁
- 在全面实施补救措施之前，通过阻止对关键资产的访问来自动降低风险
- 通过一个综合控制面板监测和衡量长期的漏洞风险，突出显示网络的整体漏洞暴露情况以及缓解和补救措施的影响。

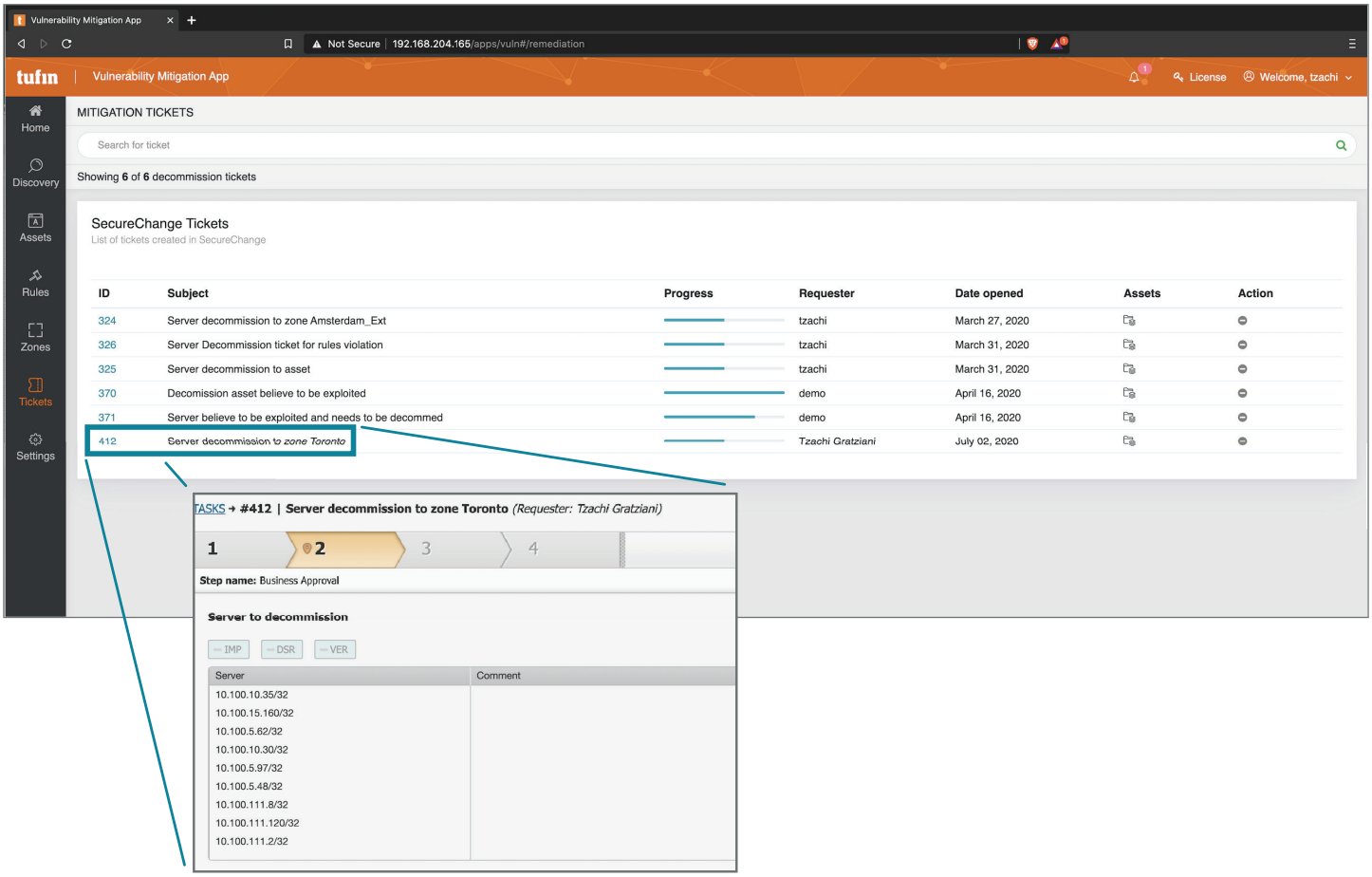


根据您最脆弱和最关键的网络段来确定安全工作的优先级

有了Tufin 漏洞缓解应用程序，您可以查看指定网络段内易受攻击的资产列表及漏洞的严重程度。您还可以查看允许访问和来自易受攻击资产的规则、受漏洞影响的基础服务以及提供访问的相关防火墙。通过漏洞控制面板，您可以跟踪随时间推移的修复和缓解趋势，以确定要如何减少攻击面。

通过删除访问权限来缓解

不是所有情况都可以使用补丁。例如，可能没有补丁，或者有补丁但执行补丁需要停机，造成昂贵代价。而且，您的安全标准和法规可能会阻止使用受影响的应用程序，直到已知的高风险漏洞得到解决。Tufin提供的流程可以帮助解决这些问题。



通过Tufin预先配置的服务器退役工作流程, 删除与脆弱资产相关的网络访问权限

使用Tufin Vulnerability Mitigation应用程序, 您可以通过Tufin预配置的服务器退役工作流程, 删除所有与脆弱资产相关的网络访问权限, 这是一个直接从应用程序启动的自动化流程。

Tufin SecureChange简化网络变更实施流程, 以定位和更新所有相关网络安全设备和基础设施组件(如防火墙、SDN、路由器和整个混合环境中的安全组)中允许访问该脆弱资产的所有规则, 接着设计并实施必要的规则变更, 自动删除对易受攻击资产的访问权限。然后, Tufin会验证变更是否按预期实施。这是一个完全自动化和可跟踪的过程, 可以直接从应用程序中进行管理。
通过这个过程, Tufin漏洞应用程序帮您减轻未修补漏洞的风险, 保护您的高价值资产。

确定哪些基础设施暴露程度最高

识别哪些资产是通过规则和服务暴露的

可访问资产中的漏洞总数

了解哪些网络段受影响最大

了解缓解和补救工作的影响

为了帮助确定下一步的优先级，该应用程序显示了允许访问高价值资产的规则的创建、修改和实际使用，让您知道是否使用了该规则，从而确定访问脆弱资产的频率。例如，如果一个规则在过去6个月内没有受到影响，那么阻止对该资产的访问所产生的业务影响会十分有限甚至没有影响。如果使用了该规则，在进行任何更改之前，您需要考虑以下几点：

- 哪些注释与规则相关联？
- 此规则是否正在使用？
- 此规则是否包含在重新认证/删除流程中？

一旦您掌握了所有这些信息，您就可以评估限制（或阻止）对脆弱资产的访问对业务的影响。