tufin The Security Policy Company.

e-book

7 Ways Policy-Driven Automation Helps With The Security Skills Shortage



The perfect storm of security skills supply and demand shows no signs of stopping.

If you're waiting for the cybersecurity skills shortage to ease up, you could be in for a long wait. The latest data from the U.S. Commerce Department shows 465,000 open security positions still remain unfilled.[1] At the same time, cybersecurity salaries are rising, particularly for in-demand skills such as cloud and app development security. And the trend for the next 10 years suggests more of the same, as the U.S. Bureau of Labor predicts that the cybersecurity job market will grow 7x faster than the national average through 2029.[2]

In other words, buckle in for a long, bumpy ride of overworked, understaffed security teams.

Yes, we can thank a rising tide of cybercriminal activity for the increased demand. Ransomware attacks in the U.S. rose 158% in 2020.[3] And the shift toward work-from-home arrangements coupled with the move of business applications to the cloud has created a much wider attack vector for cybersecurity teams to protect.

So, how do organizations protect a broader attack surface against more threats with fewer cybersecurity resources than they already need? By automating their security policies and shifting their existing cybersecurity resources to where they're needed most.



There are currently
465,000
unfilled cybersecurity jobs in the U.S. alone.

The cybersecurity job market is growing
7x faster
than the national average

1. Brooks, Khristopher J., "U.S. has almost 500,000 job openings in cybersecurity," CBS News, May 21, 2021, https://www.cbsnews.com/news/cybersecurity-job-openings-united-states/
2. Columbus, Louis, "What are the Fastest Growing Cybersecurity Skills in 2021?," Forbes.com, November 1, 2020, https://www.forbes.com/sites/louiscolumbus/2020/11/01/what-are-the-fastest-growing-cybersecurity-skills-in-2021/?sh=4b52a6e35d73
3. Jeffery, Lynsey and Vignesh Ramachandran, "Why ransomware attacks are on the rise – and what can be done to stop them," pbs.org, July 8, 2021, https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them

57% of businesses say they're negatively impacted by the cybersecurity skills shortage

According to a 2021 report released by Enterprise Strategy Group (ESG) and Information Systems Security Association (ISSA), more than half of all cybersecurity professionals surveyed said that the global shortage of cybersecurity skills has impacted their organization. In the same report, more than three-quarters of respondents described hiring security talent as "somewhat to extremely difficult." [4]

Beyond the challenge of finding new talent is the difficulty of keeping up with new cybersecurity practices and technologies. The ESG/ISSA report revealed that, while 91 percent of cybersecurity professionals believe it's critical to keep up with new cybersecurity skills, 59 percent complain that their existing job responsibilities often prevent them from getting this training. [5]

Despite the fact that there has been a cybersecurity skills shortage for years, 95 percent of cybersecurity professionals say the problem isn't getting any better and 44 percent believe it's actually getting worse. [6]

95%
of cybersecurity professionals believe the skills shortage problem isn't getting better...

... and 44% of cybersecurity professionals think it's getting worse



4. Oltsik, Jon and Bill Lundell, "The Life and Times of Cybersecurity Professionals 2021 – Volume V," Enterprise Strategy Group, July 2021.
5. ibid.
6. ibid.

DevOps and the cloud place additional pressures on security teams.

As businesses continue to digitally transform their internal and external operations, they are increasingly turning to DevOps processes and cloud-based delivery models. Built on the principles of faster development, collaboration, and innovation, the goal of DevOps teams is to move fast, take risks, and use whatever resources they can to get the job done. Security is often seen as a hindrance to this process.

DevOps has two important implications for security.

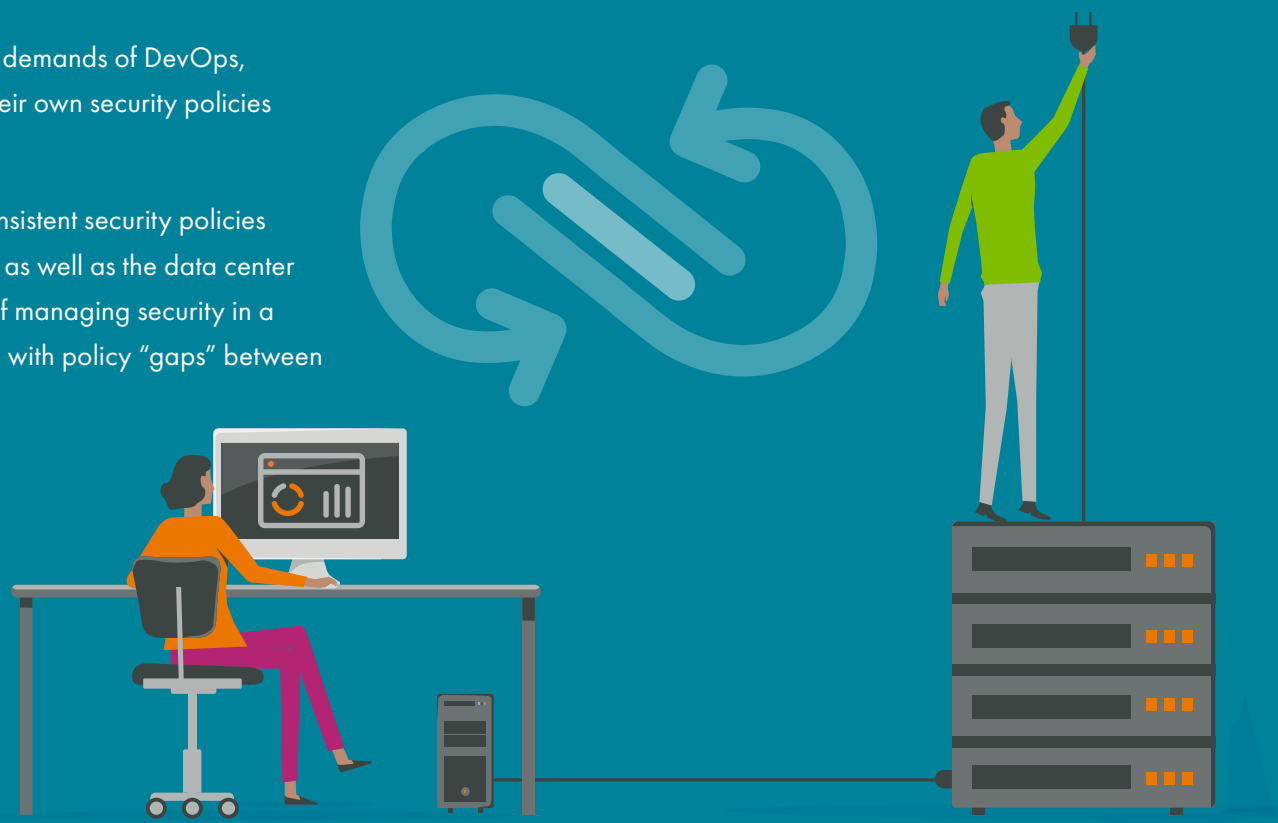
First, it increases the load on security teams as they now have to process double or triple the number of change requests in rapid fashion.

Second, as security teams struggle to keep up with the increased demands of DevOps, developers frequently circumvent security teams and configure their own security policies in the cloud.

The cloud also presents its own security challenges. Enforcing consistent security policies across business applications that are deployed in multiple clouds as well as the data center requires a unique set of security tools and skills. The complexity of managing security in a hybrid cloud environment means that many organizations end up with policy "gaps" between applications that leave them vulnerable to cyberattacks.

66%

of organizations leave back doors open to attackers through misconfigured cloud services. [7]



7. Sophos, "The State of Cloud Security 2020," https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx



Solving the cybersecurity shortage through automation

Security teams are challenged to meet rising security challenges with fewer resources. By automating their security policies, security teams can:

- Implement policy changes in minutes instead of days
- Tighten security controls consistently across their organization
- Quickly adapt to changing regulatory compliance requirements
- Reduce the complexity associated with managing security and connectivity across hybrid environments

Unlike other automation solutions, policy-driven automation means that security and policy compliance are inherent in the automated process. Changes are implemented with consideration of policy, follow a documented process, and are proactively examined for violations before they are approved. Policy-driven automation improves the efficiency of network security operations in an era of cybersecurity skills shortage.

65%

of organizations have deployed some level of security AI and automation in their business.[8]

8. Zorabedian, John, "What's New in the 2021 Cost of a Data Breach Report," Security Intelligence, July 28, 2021, https://securityintelligence.com/posts/whats-new-2021-cost-of-a-data-breach-report/

7 ways policy-driven automation helps with the security skills shortage



1 Implement changes in minutes.

Using manual processes to change firewall policies in a complex network can take days or even weeks to complete as security teams must analyze and plan changes, then fix problems because of misconfigurations or human error. Automating the change process end to end accelerates implementation and significantly reduces errors. Through policy-driven automation, changes can be implemented in minutes across multivendor solutions, physical firewalls, and even multi-cloud environments.



2 Improve audit preparation.

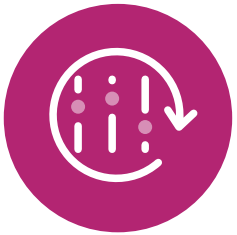
Policy-driven automation provides organizations with continuous compliance, proactive risk analysis, and comprehensive process documentation to ensure internal policies meet industry regulations (e.g., PCI DSS, HIPAA, etc.). Continuous compliance cuts audit preparation time by more than 90 percent while providing ongoing validation of the security and accuracy of each change through audit-ready reports.

© Copyright 2021 Tufin. All rights reserved.



3 Unify security policies.

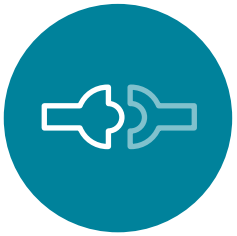
As network complexity increases and security resources remain scarce, it becomes more challenging to apply the right security policies at the right time. Policy-driven automation ensures that your current security team can meet demand by automating the process of decommissioning access to applications and servers that are no longer in use—effectively mitigate potential security threats. Defining and implementing a unified security policy assures that policy violations are identified automatically, saving your security team from the process of manually analyzing each change against a series of policy restrictions.



4 Centrally manage multivendor firewall policies.

Over the years, firewalls have accumulated thousands of rules with constantly changing access control lists. These rules can be conflicting, redundant, or obsolete, severely affecting network performance and availability. Policy-driven automation with centralized management eases the task of streamlining and monitoring a multitude of firewall rules. Specifically, automation capabilities such as server decommissioning and rule decommissioning optimize firewall security while boosting business agility.

© Copyright 2021 Tufin. All rights reserved.



5 Ensure connectivity.

As network complexity increases and security resources remain scarce, it becomes more challenging to apply the right security policies at the right time. Policy-driven automation ensures that your current security team can meet demand by automating the process of decommissioning access to applications and servers that are no longer in use and effectively mitigating potential security threats. Defining and implementing a unified security policy assures that policy violations are identified automatically, saving your security team from the process of manually analyzing each change against a series of policy restrictions.



6 Bridge communication gaps between IT and business teams.

Organizations struggle to translate and carry out business rules in their IT infrastructure. Policy-driven automation can bridge that gap by automatically mapping business rules between applications and infrastructure and abstracting security policies into application connectivity models. Automating the translation of application connections to network and firewall terms allows organizations to avoid costly errors and improve communication.

© Copyright 2021 Tufin. All rights reserved.



7 Accelerate secure application migration.

The cybersecurity skills shortage faced by network security operations teams magnifies the problem of constrained resources when dealing with massive projects such as application migration. Policy-driven automation allows for secure application migration. Policies can be automatically optimized based on access and security requirements to help minimize risk while accelerating application migration.

Conclusion

The demands of DevOps processes, the complexity of securing cloud assets, and the rise of sophisticated cyberattacks have placed a premium on security talent. As a result, organizations are often forced to place increasing demands on security teams or settle for best-effort security in the name of cost and efficiency. With policy-driven automation, organizations can meet the business need for agility and productivity while addressing the reality of a cybersecurity skills shortage. Automation solutions, for example, can be used to perform time-consuming calculations and analyses or handle mundane tasks that divert security resources from focusing on higher-level tasks and additional training.

With security policy automation, organizations can achieve higher levels of security with the resources they already have today. Give your security team the tools and training they need to succeed with Tufin's cloud security and policy automation solutions. To learn more, visit us at **tufin.com**.

About Tufin

Tufin (NYSE: TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2,000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility.

www.tufin.com

tufin
The Security Policy Company.

Copyright © All rights reserved. Tufin, Unified Security Policy, Tufin Orchestration Suite and Tufin logo are trademarks of Tufin. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. You may not copy, reproduce, photograph, translate, transmit ,make available to the public, make derivative works, perform in public, rent , broadcast or make any commercial use of the publication in full and / or in part without prior written approval.

DP20211012