Secure Access Market Evolution

Brought to you by Informa Tech

Contents

Overview

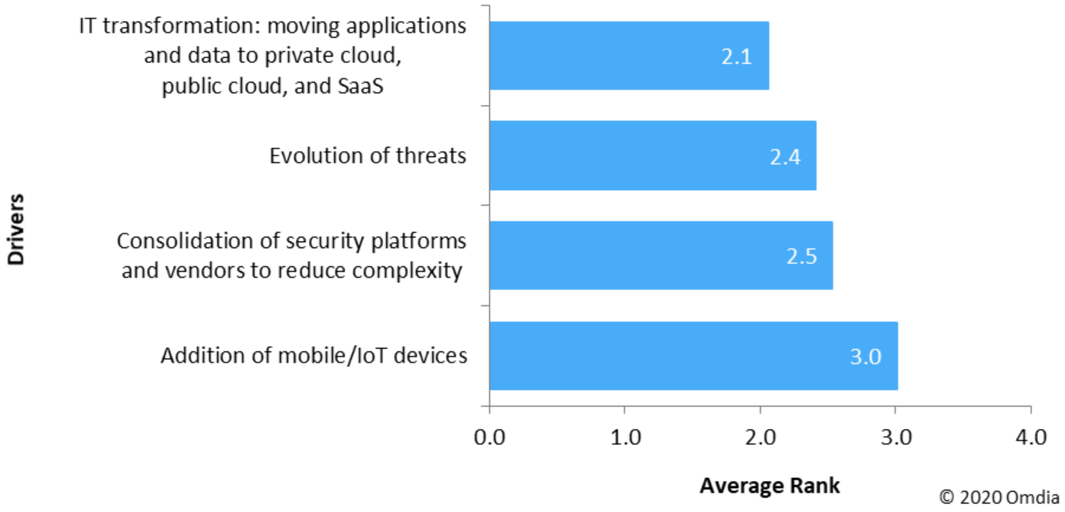
Many secure access buyers are at a crossroads; most use SSL VPN solutions that are integrated into their firewalls, but with the increased erosion of the perimeter, work-at-home acceleration during COVID-19, and the rise of the cloud and IoT, we believe there will be a requirement to look at holistic secure access solutions that go beyond what the firewall can do, incorporating VPN, zero-trust, network access control, cloud app security, and mobile/IoT security.

We present a summary of some key drivers and changes that are impacting how buyers purchase and deploy secure access solutions.

Key investment drivers for secure access solutions

4 key drivers have been shifting the conversation about how to provide secure access to networks, applications, and data for the last 10 years: reacting to new threats, simplifying infrastructure, moving to the cloud, and preparing for IoT. When we talked to secure access buyers in a recent survey, we asked them to rank how these drivers impact their decision to invest in new secure access solutions, and IT transformation (the move to the cloud) took the top spot—the architectural issues and new security challenges associated with moving to the cloud absolutely dominate all areas of cybersecurity technology discourse.

New security solutions selection criteria (mean rank)



Source: Next-Gen Threat Prevention Strategies and Vendor Leadership North American Enterprise Survey, 2020

As buyers move more infrastructure, applications, and data into the cloud, a trend that only accelerated in 2020 due to the coronavirus pandemic, traditional VPN solutions (tied to firewalls) cover fewer and fewer use cases and can be unnecessarily expensive to scale. The pain of scaling these solutions was particularly acute at the beginning of the pandemic, when many companies were forced to massively scale up their firewall infrastructure not to protect their networks, but to increase secure access capacity.

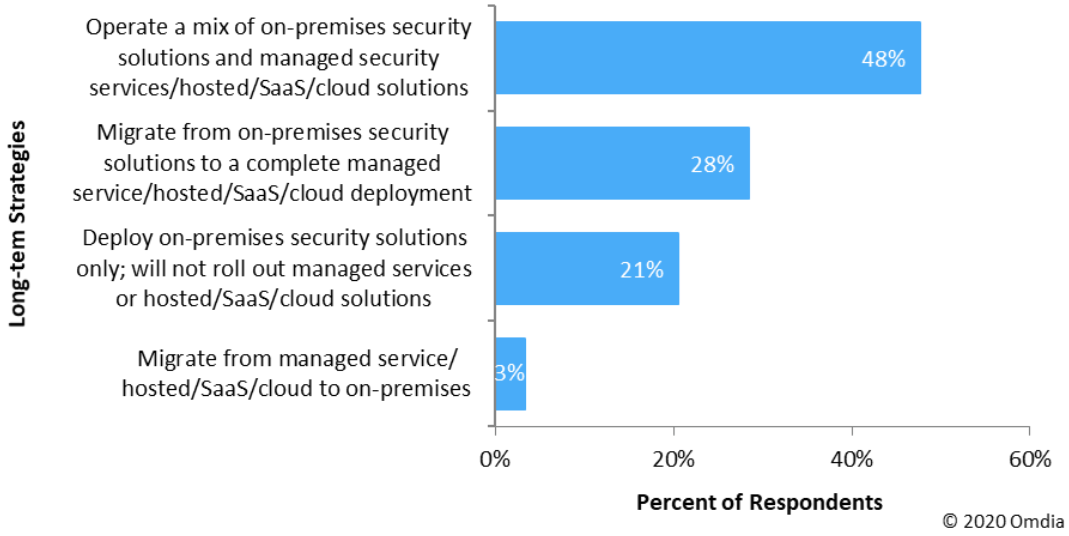
But is the move to the cloud and hybrid networks a passing fad, or a permanent trend?

Long-term secure access architecture strategy

We asked respondents to tell us what their strategies for deploying secure access solutions will be over the next 2 years. A very pragmatic (and probably correct) 48% of respondents believe that in the long term they will be operating hybrid environments that mix deployment of secure access products on their premises and hosted solutions/SaaS.

These hybrid deployments impact the secure access market significantly because it can be difficult to find unified solutions that can handle the broad range of secure access use cases that hybrid IT environment and the cloud enable; secure mobile users, securing access to business SaaS applications, securing access to infrastructure and applications in the cloud, etc. Even if there is a way to bolt on new solutions to cover new use cases, they typically add their own management consoles and policy infrastructure, and as we saw in the last chart, buyers are looking to reduce complexity and consolidate to platforms, not add more point security solutions.

Secure access deployment strategies



Source: Next-Gen Threat Prevention Strategies and Vendor Leadership North American Enterprise Survey, 2020

Conclusion

The world was already moving rapidly towards the cloud, creating countless new security perimeters around users, data, and infrastructure leveraging the Internet and the cloud to work flexibly, and COVID-19 is rapidly accelerating the problem of providing secure access in a hybrid/cloud world with significant increases in remote user populations. Now it appears that many of those temporary work from home situations will become permanent after a string of announcements from large companies in many industries. We believe the time is right for a move to a secure access platform because:

- SSL VPN alone doesn't cover enough secure access use cases
- SSL VPNs tied to firewalls cause significant cost and scaling issues
- IT organizations want a single platform to write policy and provision access for all secure access use cases (remote users, third party users, IoT devices, SaaS application access, cloud access, zero trust access, etc.)
- The shift to hybrid IT and cloud is permanent, and providing secure access in hybrid/cloud environments requires a platform-level approach

To learn more

Watch this free webinar

"Secure Access and NGFW: Is it time for a divorce?"

presented by Omdia and our partner

Pulse Secure

The webinar can be accessed at: https://bit.ly/3fQNYEG

For additional Omdia events, visit:
https://omdia.tech.informa.com/what-we-do/events-and-webinars

Follow the conversation @OmdiaHQ

Author

Jeff Wilson
Chief Analyst, Cybersecurity Technology
Jeff.Wilson@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.