Point of View

How to Get the Most Out of Your Security Infrastructure

Manage Risk, Reduce Complexity, Realize Better TCO

Why "Adding On" No Longer Adds Up

Since early 2020, the majority of organizations have been adopting transformative digital tools and capabilities at an accelerated rate. While these innovations have been needed to keep pace with changing conditions related to the COVID-19 pandemic, business operations have simultaneously been suffering as a result of increasingly complex network and security infrastructure.

On top of record numbers of cyberattacks, IT teams now face the challenges of managing overly complex environments created over time through piecemeal additions designed to expand networking capabilities or close security gaps. Staff need extended training to understand and administer all the disparate tools and solutions deployed throughout their organization's infrastructure. Increasing headcount isn't a practical option, since nearly half (46%) of companies already face staffing challenges as they look to hire security team members.[4]

In addition, complexity impedes visibility needed for security investigations, which increases exposure time to threats. It can complicate security policies and create new gaps in protection. To make matters worse, complexity also ties up security operations (SecOps) resources with manual analysis—for example, trying to track down where a threat may (or may not) be hiding across an ever-expanding attack surface.

At the end of the day, all of these complexity problems increase both operating expenditures (OpEx) and the total cost of ownership (TCO) for security. Network and security teams need to work smarter and more efficiently by eliminating unnecessary work across disparate, disjointed security enforcement points. In short, they need to simplify operations.

Fact

The pace of adopting new digital technologies for greater business agility has rapidly accelerated over the last two years.[1]

Fact

75% of executives report too much complexity in their organizations, leading to cyber and privacy risks.[2]

Fact

Without visibility into digital infrastructure, it becomes difficult to recognize when, where, or why there is a problem.[3]

[1] "Digital transformation is changing. Here's what comes next," ZDNet, October 1, 2021.
[2] "Is your organisation too complex to secure?," PwC, October 11, 2021.
[3] "The unsolved opportunities for cybersecurity providers," McKinsey & Company, January 5, 2022.
[4] "Navigating Change: The Operational Impact of Network and Security Transformation," Netskope, November 2021.

The Consolidation Situation

Organizations need to consolidate key security services for web, cloud, and private applications to a cloud-native security platform.

Risk is perhaps the biggest reason for businesses to consolidate their sprawling security infrastructure. It's difficult for SecOps teams to understand the level of risk posed by digital transformation projects and adoption of new cloud platforms and applications. With 50 or more different security and networking tools deployed at some organizations, security teams are unable to quickly detect, investigate, and respond to connectivity-related incidents—especially when relying on multiple solution interfaces.

The ideal solution is a single platform that monitors end-to-end connectivity—from any user, at any location, to any cloud or web application. Businesses need a single tool that enables users to adopt new cloud platforms and applications (both managed and unmanaged) without introducing unchecked risks. This platform should use a single endpoint agent/client, provide unified policy management, and simplify incident remediation across all channels. It should also help optimize network performance and ensure better user productivity (less downtime) while reducing OpEx costs.

Reduce network complexity.

A consolidated security platform includes steering capabilities that help organizations save on unnecessary site-to-site connectivity, while allowing direct-to-net access for branches and eliminating expensive private connections. This supports both cost savings and a better user experience.

Streamline day-to-day operations.

A true single-platform approach can simplify security policies by 10x. This streamlining frees up time for staff to focus on more proactive risk management tasks. An effective solution will use a single agent, deliver unified policy management, and support unified incident remediation. It should be able to provide near real-time policy refinement to reduce cycles and overall administration time. A solution that offers *real-time user coaching capabilities* can further increase knowledge and reduce overhead associated with manual user training initiatives.

Reduced TCO.

Security consolidation can also reduce TCO by 30%+ through elimination of appliances, reduction of software license spend, reduction in administration overhead, and fewer tasks that need to be performed by human security staff.

Critical Questions to Ask

- ☐ How can I better deploy the time and resources of my existing security team?
- ☐ What can be done to reduce my connectivity costs?
- ☐ Where can I improve efficiencies, eliminate waste, and reduce operating costs?

You Can't Control What You Can't See

Enterprise organizations need a single console, single client, and cloud platform with unified policy management.

To manage an expanded attack surface and multiplying network edges, businesses need full context and content awareness that provides visibility into both the type of content and the attempted action performed by the user.

Lack of unified visibility and control across web, email, cloud platforms, and associated applications leads to lengthy processes for understanding compliance risks. Organizations also need comprehensive visibility and policy enforcement across the business to eliminate redundant applications and IT services, for better operational efficiency and cost savings.

In terms of control, businesses specifically need integrated data protection across the critical vectors of web, cloud applications, and email. This should include both data at rest and data in motion in order to provide a complete picture in support of rapid correlation and investigation. This efficiency helps conserve security team resources for more meaningful activities.

Simplified management.

A unified platform reduces the number of tools needed to monitor and troubleshoot connectivity issues, can provide end-to-end visibility using a single management console, and helps quickly manage redundant or risky applications.

Protect users and data.

With policy-based controls, a single platform can improve prevention of cloud-based threats (like ransomware and phishing) and data loss, leading to a reduction in incidents that require investigation and/or remediation.

Compliance.

A unified platform can also help streamline reporting processes, reduce manual auditing workloads, and provide a framework for quickly integrating new technologies while satisfying compliance requirements.

Critical Questions to Ask

- ☐ Does my visibility extend across all the different network edges?
- ☐ Can I control data at rest and in motion across all vectors—clouds, web, email, etc.?
- ☐ How do I reduce manual auditing and reporting processes?

A Matter of Measurement

Organizations need a platform with built-in analytics capabilities to draw insights across all parts of the business.

Understanding where the risk lies in your organization requires analyzing data about the applications and security measures in use. With increasing complexity and today's application surface area extending to the cloud and web, it has become incredibly difficult for security teams to obtain clear analytics about the organization's efforts to protect users and data.

Analytics can help SecOps teams quickly assess the risk associated with digital transformation projects so that they can effectively communicate potential problems with business units and collaborate on a solution that enables both business and security needs with minimal churn. This kind of data also becomes invaluable for security leaders when reporting to executive leadership.

Improve application security.

Attacks on web applications represent 39% of all breaches.[5] Platform-based analytics tools designed to measure and analyze cloud and web activity can help businesses draw rich insights about their application usage, exposure to risk, and the overall effectiveness of their security program. Accurate and timely delivery of information reduces costs associated with manual security team analysis of potential threats.

Executive communications.

CISOs and CIOs often find it hard to track risk trends efficiently and communicate that information to business leaders at a level they understand. This limitation inhibits driving forward strategic security initiatives that require board-level financial backing. Security leaders need access to a complete picture of compliance risk in order to quickly and easily present a high-level view to executives and board members in a format that they can readily process.

Critical Questions to Ask

- ☐ Can I identify the sources of risk in my organization?
- ☐ Is there a way to deliver meaningful and actionable data insights to my stakeholders?
- ☐ What can I do to help manage my current security efforts and protect users and data?

[5] "Cybercrime thrives during pandemic: Verizon 2021 Data Breach Investigations Report," Verizon, May 13, 2021.

Networking Considerations

As any infrastructure expert will remind you, remember the network. More businesses are using more cloud applications, enabling more remote access to more critical data, and seeing heightened security risks as a result. But what's often missed in the rush to apply proper security measures to govern data access is a set of clear expectations for networking. This is crucial: If the network performance degrades because of security, the user experience degrades as a result, and business productivity slows to a crawl. Users need fast, direct access to their apps and data, and they need it from anywhere.

This can be reasonably achieved by:

- Preventing "hairpinning," or the practice of backhauling user traffic to corporate data centers
- Phasing out VPNs
- Determining the right role for SD-WAN in replacement of expensive, outdated networking technologies such as MPLS
- Ensuring the network has a modern peering setup with leading cloud infrastructure providers
- Creating more effective cross-functional teams among formerly siloed networking and security organizations

(A recent paper, "The Network is the Security," covers all of this in detail.)

Simplify Operations With a Single Platform

A complex IT infrastructure increases costs. It also drags down network performance and business agility. Complexity inhibits scalability—primarily due to limited staff resources available for analyzing and securing new technologies, which leads to lengthy project timelines. Most importantly, it exposes organizations to undue risks at a time when threats are growing in number and sophistication.

Simplifying operations starts with consolidation. Consolidation to a unified security platform establishes better visibility. Visibility gives organizations the ability to institute policy-based controls and perform accurate compliance auditing to eliminate risks and inefficiencies that drive up OpEx. Platform-based analytics can further enhance the value and performance of the organization's security program over time.