White Paper

Overprovisioning: The ticking time bomb for network security

ACCEDIAN

Executive Summary

According to Peter Drucker, one of the founding fathers of management consultancy, “Efficiency is doing things right, effectiveness is doing the right things.” At present, many enterprises are falling short of both when it comes to their network operations.

Information Technology (IT) teams overprovision to protect network performance from traffic variations caused by network failures and/or transient surges driven by unpredictable demand. The approach is understandable given what’s at stake. If an enterprise network fails, the costs will often be far more than anything associated with overprovisioning.

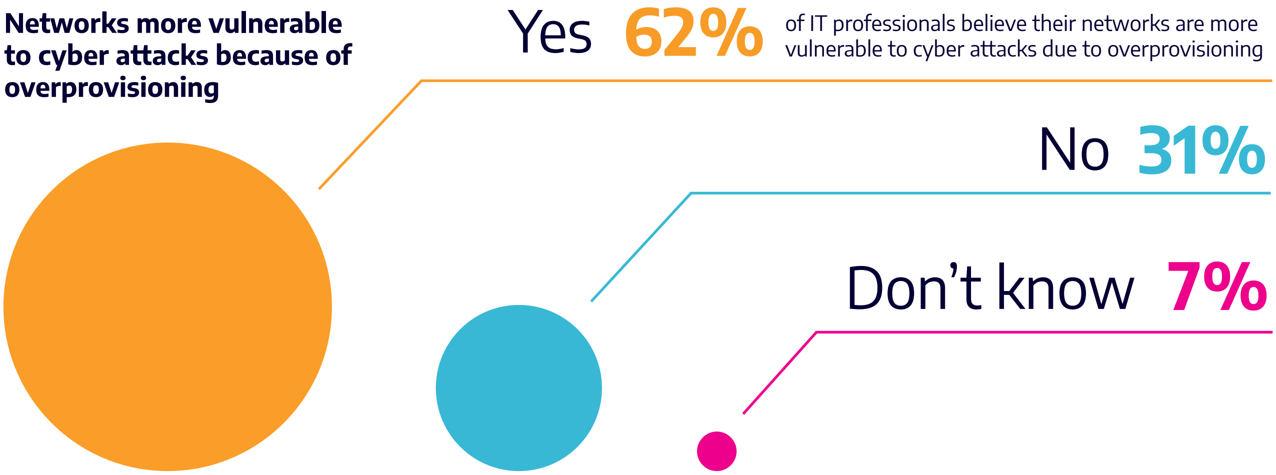
This is particularly true if the service your organization provides is critical. In such cases, the cost of unplanned network downtime can be measured in more than dollars. For instance, during the COVID-19 vaccination period, the websites of a number of healthcare providers crashed under the weight of demand for bookings, leading to untold stress and anxiety for citizens unable to secure a slot.[1]

Overprovisioning means there is more infrastructure to protect (a larger attack surface), more attack vectors, and an increased opportunity for the misconfiguration of tools, human error or Security Operations Center (SOC) fatigue. Put bluntly: If you overprovision you are putting your enterprise at risk. Overprovisioning is a ticking time bomb in so far as if you widen the attack surface too much it becomes a matter of “when” not “if” a cyber attack is successful.

And given security incidents doubled[2] from 2019 to 2020, this is a particularly relevant concern.

To gain a better understanding of the extent of overprovisioning in enterprises, Accedian sponsored a survey in June 2021 by interviewing 500 senior IT professionals at US enterprises. This paper reports on common practices and concerns around overprovisioning, and also points the way to a leaner, more effective alternative: leveraging metadata enabled by in-depth network traffic analysis and machine learning.

Networks more vulnerable to cyber attacks because of overprovisioning



[1] clickondetroit.com/health/2021/01/09/beaumont-website-crashes-due-to-demand-for-covid-19-vaccine/ and www.independent.co.uk/news/uk/home-news/nhs-website-down-vaccine-covid-b1830461.html

[2] pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report

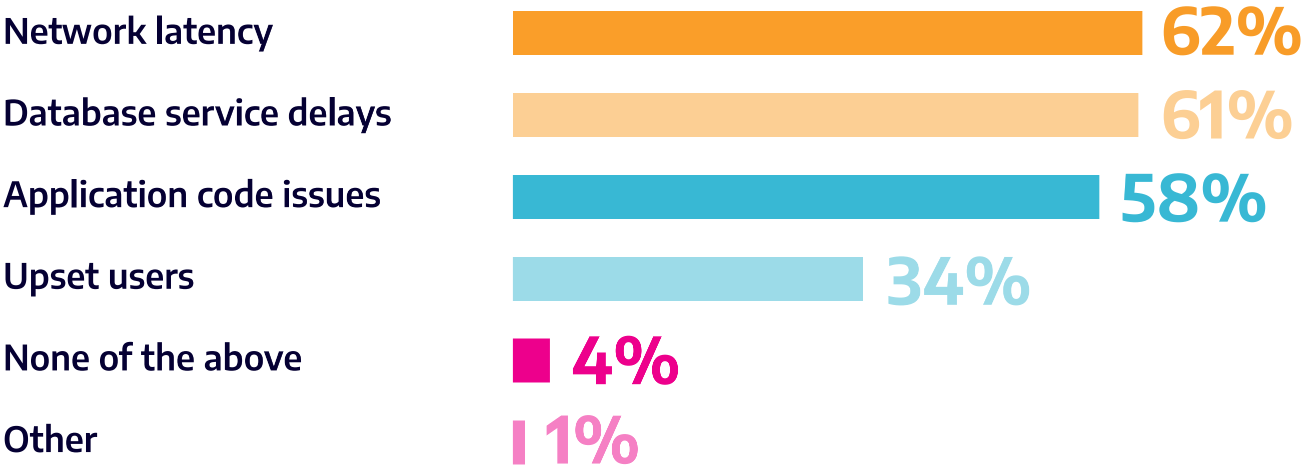
Overprovisioning is a treatment, not a cure

One clear takeaway from the research is that overprovisioning continues to be a common practice in enterprises in a broad range of sectors including financial services, public sector, healthcare, IT, manufacturing, and retail. What's also clear is that the practice is often used to defer solving a problem rather than addressing it head on.

Sixty-six percent of respondents admit to overprovisioning over the past 9-12 months (in this case by spinning up excessive cloud instances). What's more, these respondents explicitly said they did so in order to counteract network performance issues instead of identifying the root cause and fixing them.

There is clearly a level of fear here. The IT team is throwing resources at the issue to stave off any chance of failure. This fear is driven by a range of factors including not wishing to upset users (34%), worries over database service delays (61%), and network latency (62%), as well as concerns over application code issues (58%). Anecdotally, respondents also cite wishing to have a buffer for unaccounted for users and short-term factors such as the need to accommodate remote working during the pandemic.

Why IT professionals overprovision networks

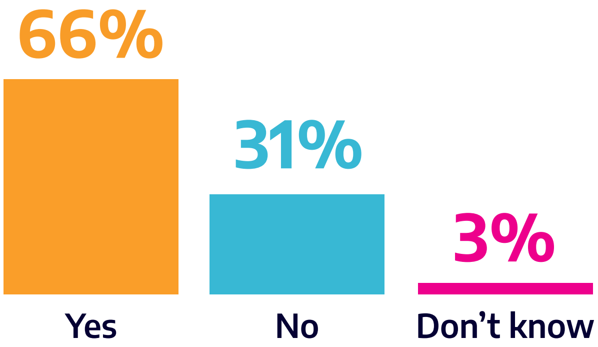


By overprovisioning, network teams are treating the symptoms of their network issues, instead of looking for a cure.

To find a cure, network teams need to understand the root cause of performance issues. Without a detailed view of how their network is performing, they will continue to spend money on resources with no end in sight. In fact, what usually happens is that overprovisioning in one area serves only to reveal challenges in other areas. The IT leaders we spoke to agree, 78% saying that overprovisioning in CPU, memory or network capacity, led them to discover further performance bottlenecks.

The net result is that even more of the network is overprovisioned. For 22% of the IT professionals we spoke to, between 40-50% of their average deployment is overprovisioned, including storage, compute, network resources, etc. For 21% of respondents, that figure rose to between 50-60%.

Overprovisioned cloud instances to counteract performance issues



Over the last 9-12 months, did you spin up excessive cloud instances (overprovision) in an attempt to immediately counteract performance issues instead of fixing the issue?

Open to attack, putting network security at risk

The continuing reliance on overprovisioning is surprising, simply because it's a band-aid for something that could be solved easily. But it is even more surprising given that the practice makes enterprises less secure from cyber attacks – and that the majority of IT leaders are well aware of this fact.

When asked to name their biggest concerns around overprovisioning, nearly three quarters (72%) of respondents cite security – well ahead of other key concerns such as management (55%) or budget (48%). Sixty-two percent say they believe their networks are more vulnerable to cyber attacks due to overprovisioning, and 68% report that they are moderately or majorly concerned that overprovisioning increases their attack surface.

What makes these findings even more bewildering is that the majority of network administrators we spoke to (62%) believe that network security is more important than cloud application performance (38%).

When it comes to security, our findings make for shocking reading. An informed audience fully understands the risks of overprovisioning and yet are ploughing ahead regardless. Why is this happening?

The biggest concerns around overprovisioning

Budget
48%

Security
72%

Management
54%

Perceived lack of time and tools hinder change

One of the reasons it is still a widespread practice is that enterprises are not monitoring overprovisioning effectively, and so have a poor understanding of the extent to which this practice occurs and is adding risk to the organization.

In fact, our survey shows that half of IT respondents admit that they do not use tools specifically aimed at monitoring overprovisioning. Of those who do use monitoring tools (39%), the most commonly deployed are Microsoft, SolarWinds, AT&T, IBM, and Oracle.

However, the main challenges facing network teams don't come from a lack of awareness of overprovisioning but instead from a lack of time and resources. A plurality (40%) of the IT professionals we interviewed say they overprovision simply because they lack the time needed to diagnose the root cause of performance issues. Others (36%) cite a lack of diagnostic tools as the main reason for overprovisioning.

Network teams within enterprises are therefore stuck between a rock and a hard place. They need to ensure that their network is able to deliver the service levels required to operate effectively at all times, but lack the time and resources to monitor for network issues and fix their root causes. As a result, they fall back on the blunt tool of overprovisioning, in full knowledge that doing so increases the security risk of the organization. There must be a better way.

The alternative: Network and application performance monitoring

When traffic jams become more frequent on freeways, the authorities can build more lanes. But this is an expensive and unsustainable approach. The more lanes you build, the more demand increases. Before long you're back to square one. The alternative is to get smart. "Smart Highways" use connected sensors and advanced algorithms to help reroute traffic around pinch points, allowing motorists to keep moving without the need to build additional lanes or roads.

The same is true of networks. Instead of overprovisioning, network teams can install smart, end-to-end network and application monitoring tools, such as Accedian's Skylight™ platform. Skylight delivers high-performance network and user experience monitoring across any application, any cloud, and any network.

In essence, the approach involves four steps:

- **Deploy**. Place Skylight sensors, which are available as both hardware and software, anywhere in the network according to the unique needs of your enterprise. Our range of sensors include:
  - L2-L7 passive traffic analysis
  - L2-L7 high-definition active testing
  - L2-L4 testing & demarcation
- **Orchestrate.** Leverage our zero-touch provisioning to deploy new sensors in just minutes for a high-velocity solution. Skylight also simplifies, secures, and accelerates service validation, fault management, and performance insight.
- **Analyze.** Our powerful machine learning analytics deliver a rapid time to insight, drilling down from end-user application issues deep into the network with root cause analytics and configurable alerts. We deliver a 'single pane of glass' view of network and application user performance, using machine learning to alert you to active and potential issues in the network.
- **Predict.** Skylight streams data in real time to monitor how well networks, applications, and services are performing, and whether it is time to make changes or adjust policies. With Skylight, you can get ahead of potential issues before they impact performance.

Companies can reduce risks by addressing the performance issues that lead to overprovisioning and save money while improving visibility with performance metrics across cloud, network, and applications. Skylight is a highly automated, light touch approach to performance monitoring that makes life easier for network professionals.

A more secure enterprise

By reducing or removing the need for overprovisioning, end-to-end network and application monitoring automatically makes enterprises more secure by reducing the threat surface.

Visibility to all network traffic from all users empowers SOC teams with metadata and machine learning that give them all the information they need to create a baseline of normal network behavior. They can then identify any exceptions to that baseline, like unusual activity that could be a sign of a security breach.

Network and application monitoring will allow them to turn what was once a vulnerability into a security asset.

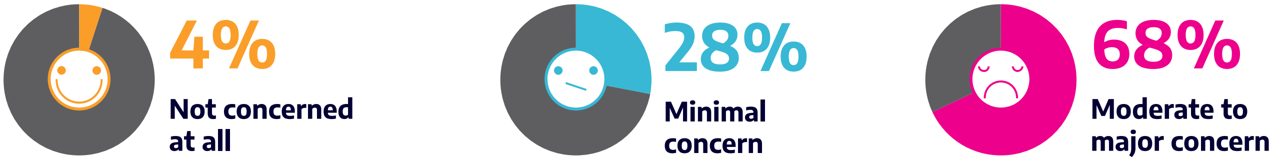
Summary

Overprovisioning is a costly solution for ensuring network performance. In today's software-defined age, virtualized network monitoring tools that leverage advanced analytics provide a more advanced response that delivers efficiency and effectiveness, while also meeting the security needs of our digital age. It's time for enterprises to make the change.

What you need to know about Overprovisioning:

- It's a common solution to ensure enterprise networks continue to deliver in the case of surges in demand or outages.
- IT professionals say they turn to overprovisioning because they lack the time and tools to manage network performance.
- 72% of IT professionals say that security is the biggest threat posed by overprovisioning.
- As a result, 62% believe their networks are more vulnerable to cyber-attacks.
- End-to-end application and network monitoring helps IT to rapidly identify and fix performance issues.
- The goal is to reduce the threat surface and provide IT and security teams with network traffic data to improve performance and detection of potential threats.

Concern that overprovisioning is increasing attack surface



About Accedian

Accedian is the leader in performance analytics, cybersecurity threat detection and end user experience solutions, dedicated to providing our customers with the ability to assure and protect their digital infrastructure, while helping them to unlock the full productivity of their users.

Learn more at accedian.com

Accedian | 2351 Blvd. Alfred Nobel, N-410 | Saint-Laurent, QC H4S 2A9 | 1 866-685-8181 | **accedian.com**