IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

How Can CIOs Overcome Visibility Challenges and Stop their Technology Initiatives from Being Derailed?

Nadeem Zahid

Nadeem Zahid
Senior Direct Strategy
and Cloud
Savvius

Biography

Nadeem Zahid is a Senior Director Strategy and Cloud and leads the strategy, technology alliances and business development at Savvius (www.savvius.com), a LiveAction Company.

He is instrumental in influencing company and product vision and direction, developing and maintaining technology/solution eco-system partnerships and developing new market routes and use cases for the growth.

Nadeem has over 21 years of leadership experience in the networking industry with leading technology companies including Cisco, Juniper, Brocade, and Extreme Networks. He also ran his own IT consulting/ISV company, tFinery, for strategy consulting to fortune 500 IT clients.

Keywords Visibility, Network monitoring, CIO, Savvius, LiveAction, Digital transformation
Paper type Opinion

Abstract

When dealing with digital transformation initiatives, having visibility into IT infrastructure shouldn't be a choice, it should be a requirement. Unfortunately, as the author of this article explains, many of today's CIOs find themselves outside their comfort zone, lacking the required visibility needed to make the day-to-day decisions that keep the business running and transforming smoothly. These network blind-spots can have a significant impact on the organization. But, how can CIOs overcome these visibility challenges and keep their technology initiatives from being derailed?

Introduction

Typically, a CIO focuses on ensuring mission-critical applications and services stay up (and are updated), allocating adequate team resources, and resolving a variety of issues on tight deadlines. It requires interfacing with the heads of application and infrastructure teams, living at the war-room doorstep, and fighting uphill battles with a board that traditionally views IT as a cost centre. As a result, many CIOs spend large portions of their time trying to figure out how to do more with less by make existing IT tools, practices, and processes more efficient and cost-effective.

Blind spots

The reality is that visibility should always be a key priority for a CIO across his/her application and infrastructure framework. Having blind spots inside the IT service delivery framework (such as compute, network, and data traffic) can severely impact performance and security, and result in under or over-provisioning; all of which can affect the user-experience, disrupt business continuity, drive down profitability, drive customers to the competition, and much more.

When organizations layer on a digital transformation initiative, this becomes another charter that is at least partially owned by the CIO. For example, think about the implications associated with the move toward more cloud technologies. It is a daunting responsibility in itself. As an organization moves to the cloud, not thinking about the visibility mechanisms inside the cloud can result in lost control on mission -critical workloads which are under peak demand, and severely impact business and reputation. Without adequate visibility, cloud migration is like throwing applications into a black box. Without adequate prior performance and cost modeling, it raises business risk and the organization’s cost of doing business.

Another example might focus on the strategic consolidation of applications at data centre sites. This results in a large amount of east-west traffic in the data center and can create a variety of IT blind spots. Lack of visibility into this sort of critical infrastructure drives increased business risk and eliminates the ability of IT to proactively investigate issues and solve problems quickly during downtimes or when performance is impacted (all of which costs the organization money). Provisioning the right mechanisms for network visibility into east-west traffic can reduce the level of risk associated with the most vibrant parts of the data center, and therefore reduce headaches for the CIO.

Hopefully it has sunk in: blind spots are bad, and visibility is good! So, how do you achieve “adequate visibility?” First, it’s critical that visibility be a CIO-level initiative. That doesn’t mean the CIO should be staring at a screen all day in his office. Rather the CIO should focus on three primary items:

1. adequate visibility across the IT service delivery framework;
2. awareness associated with the darkest and riskiest blind spots that could impact the business; and
3. a plan and a budget that can remove those risks.

The functional heads can then help the CIO figure out what appropriate measures need to be taken in terms of applications and infrastructure visibility and how much spend should be allocated for the appropriate tools, resources and training. These heads, such as a Vice President or Director of Network Operations, should do a complete domain assessment and extend the level of visibility throughout the dark corners of their network purview.

For example, are all of the remote-offices covered in terms of having remote visibility into the ingress/egress of wired/wireless/VPN traffic and the user experience? Is there visibility into the WAN traffic patterns for cost and performance optimization? Can you see all of the north-south and east-west traffic associated with your most critical asset, the data centre and, as you add cloud to the IT domain, do you have insight into those zones?

At the VP and Director level, there should be enough visibility mechanisms laid out that when the CIO calls them into the war-room to discuss issues associated with digital transformation, they can immediately point out if an issue is within their domain or not, without external dependency, and back it up with the data. This level of visibility reduces finger-pointing, saves precious time, and reduces the need for future war room meetings.

Conclusion

In summary, CIO's should be asking their department heads what their visibility strategy is for any technology initiative – and there is no reason why an IT team should not be armed with the proper tools for actionable and evidence-based visibility.

The reality is that nothing beats network data that has been captured, retained and examined. It allows teams to accurately advise, in real-time, on business-critical application performance and user experience. After all, what's not visible, cannot be controlled.