10 Reasons NOT to Deploy SONiC NOS in Your Network

SONiC (Software for Open Networking in the Cloud) has gained significant popularity as an open-source Network Operating System (NOS) in data centers. This trend extends to edge and campus environments, driven by hyperscalers' successful deployments of SONiC, demonstrating its growing adoption across various use cases. For those willing to invest the necessary effort, open networking can offer a level of flexibility, cost-effectiveness, and innovation that proprietary solutions struggle to match. But is SONiC truly an all-or-nothing proposition? Let's delve deeper.

When SONiC Isn't the Right Choice

Companies should carefully evaluate their readiness before adopting SONiC. The decision has to be based on technical capabilities, resource availability, and long-term networking strategy. Here are 10 reasons not to use SONiC NOS in your network infrastructure:

1. Lack of in-house expertise in OSS, particularly SONiC. Unlike proprietary NOS, SONiC is open-source, offering greater control and customization but demanding a skilled team for configuration, optimization, and troubleshooting. This team should be comfortable with Linux, networking protocols, and open-source development. Without them, companies may face challenges like prolonged deployment, suboptimal performance, and network instability.

2. No DevOps-friendly internal culture. Traditional network operations struggle with SONiC's rapid pace. Adopting it might require a cultural shift, involving DevOps practices like automated testing and version control to manage frequent changes and their impact on the network.

3. An absence of Quality Assurance (QA) infrastructure. Lacking a robust Quality Assurance (QA) infrastructure, organizations struggle to ensure network stability and security. While diverse networking hardware labs are essential for compatibility and performance testing, automated tools and skilled engineers are needed to analyze results, validate new features, and prevent network disruptions. Furthermore, a shortage of expertise in hardening SONiC exposes organizations to security vulnerabilities due to improper access controls, data encryption, and overall system misconfiguration.

4. Uncertain implementation strategy. Understanding network architecture and SONiC's capabilities is crucial for developing an implementation strategy. Without a well-defined plan, organizations risk disruptive network changes and prolonged outages.
5. No operations strategy. Maintaining a SONiC network requires an operations strategy. This can involve building an internal multi-skilled team capable of troubleshooting, patching, and keeping up with the latest developments (requiring ongoing training and resource dedication). Alternatively, commercial support is available but comes with its own costs. Without a solid operations strategy, organizations may face challenges maintaining network stability and resolving issues efficiently.

6. Shift in network ownership paradigm. Adopting SONiC represents a departure from traditional approaches. While traditional network operators often prefer working with vendors or system integrators who provide end-to-end solutions, SONiC requires a more active role in network management, from initial design to ongoing operations. If an organization is comfortable with a higher level of ownership and control, SONiC can be a rewarding option.
7. Unclear use case and implementation outcomes. Organizations deploying SONiC should thoroughly assess its capabilities against their specific networking requirements. This includes feature sets, performance benchmarks, and scalability considerations. Without a clear understanding of how SONiC will address specific needs, there's a high risk of wasted resources and an inadequate network solution.
8. Limited direct connections with switch and ASIC vendors. SONiC's reliance on SAI for hardware interaction necessitates collaboration with hardware/ASIC vendors for compatibility. This secures access to crucial drivers and firmware updates but requires dedicated expertise to navigate technical discussions and potentially influence development. Unlike traditional networking, organizations need to actively manage these relationships to ensure optimal performance, avoid support delays, and address low-level issues.
9. Unwillingness to collaborate with third parties and communities. Some companies resist cooperating with third parties and the broader SONiC community due to time constraints or an unwillingness to engage with external resources. However, going it alone can lead to missed opportunities for improved compatibility, continuous development, security updates, and adoption of best practices. If you're hesitant about collaborating, experienced partners like PLVision can assist with planning, deployment, ongoing maintenance, and provide SONiC-based solutions.
10. Incomplete Understanding of Total Cost of Ownership (TCO). While SONiC eliminates licensing fees, a thorough TCO analysis is crucial. Estimate potential expenses like personnel training, custom development, integration costs with existing

infrastructure, and potentially commercial support depending on your use case and chosen implementation strategy.
Overall, while implementing SONiC is a critical decision, it unlocks significant advantages for organizations ready to embrace open networking.