

7 Misconceptions About Cloud-Based Infrastructure Management

Cloud networking is evolving at a rapid pace. As a leader in this evolution, Extreme Networks has delivered one of the industry's only third-generation cloud networking platforms. This represents a significant leap forward in-terms of reliability, security, scale and intelligence over previous first and second-generation solutions. With much of the industry still lagging, we have found that there are many misconceptions about cloud infrastructure management that are based on the limitations of the more prevalent second-generation solutions.

This document outlines the seven most common misconceptions with cloud-based infrastructure management and how choosing a third-generation solution, such as ExtremeCloud™ IQ, can avoid these pitfalls.

1. A Loss of Connectivity to the Public Cloud Is Going to Have an Impact on My Network Services.

With Extreme, a loss of connectivity to the public cloud will not impact network traffic or the underlying infrastructure. This is because there is no dependency on the cloud management system for the infrastructure to function. The devices can even perform mission-critical functions like RADIUS and user authentication caching to ensure continued secure access to the network. This is because Extreme's switching, routing, and wireless solutions are all based on distributed control and data planes (with a centralized management plane). Alternative offers that are based on centralized control planes mean that there is a dependency between the infrastructure and the cloud, and the infrastructure control plane would be lost with the loss of the public cloud. With Extreme's distributed architecture, although you will lose connectivity to the management interface, the network itself is not impacted in any way.

2. If My Cloud-Subscription Service Expires, My Users Will Lose the Ability to Connect to the Network.

Unlike some competitive solutions, if your cloud-subscription service expires, your users will still be able to connect and utilize the network completely. This is again because with Extreme each infrastructure component has its own control plane and its own local configuration

file. Therefore, with Extreme, although access to the cloud-management tool itself will be disabled until the subscription is renewed, users will still have untethered access to the network.

To prevent this occurrence, ExtremeCloud IQ provides numerous, overt warnings well in advance of the subscription expiration date so that you can renew your service proactively.

3. Continuous Feature Updates to the Cloud Management Platform Means I Will Lose Control Over Software Updates and Patches on My Infrastructure.

When Extreme Networks talks about continuous innovation and continuous delivery as one of the benefits of a third-generation cloud management platform, this only relates to the management features. While it is true that you will receive new and improved management functions like a streamlined GUI, a new way to display information or even a new configuration wizard without having to go through a complex management upgrade. However, no changes are ever applied to the network devices or the operation of those devices. All infrastructure changes are left in strict control of your IT organization and network administrators. All software upgrades, firmware upgrades, and patches are completed in your own change control windows exactly how it is done today.

4. My Infrastructure Is More Secure With an On-Premises Management Platform.

While that might have been the case a few years ago, there have been huge advances in cloud-based security. The top cloud vendors—AWS, Google, and Microsoft Azure—have spent billions on security and have massive teams of cybersecurity experts and data scientists, far exceeding the capabilities of any individual enterprise. Additionally, Extreme has achieved ISO 27001 certification for our cloud offerings, further enhancing our cloud security offering.

Furthermore, many next-generation network security solutions are leveraging Artificial Intelligence/Machine Learning (AI/ML) technology to faster detect and remediate against threats. Since the use of AI and ML requires a huge data pool to learn from, as well as significant compute resources, it is best suited for public cloud implementations. In fact, much of the innovation that is occurring in networking and security is via the public cloud. However, if you are still not convinced, ExtremeCloud IQ comes in private and local deployment models in addition to its public cloud offer. Private and local deployment models never use the public cloud, with the local IT administrator maintaining full control.

5. Cloud-Management Is Well Suited for Distributed Environments; However, It Is Not Scalable Enough for Dense Campus Environments Like Hospitals and Stadiums.

While it is true that some companies start with their remote locations when looking at cloud management, it does not mean that the solution can't work for the main campus as well. ExtremeCloud IQ is based on a third generation, micro-services-based architecture where each individual

micro-service is deployed in a cluster of high-availability servers. This architecture not only offers the scalability to support millions of devices and/or clients, it also allows for elasticity to deal with the fluctuations in demand that can occur in both hospitals and stadiums.

6. Public Cloud Is the Only Option Available for Infrastructure Management.

Not with Extreme. One of the benefits of ExtremeCloud IQ is that we offer flexible deployment options with the choice of public, private, local and even hybrid cloud options. Additionally, Extreme offers the ability to seamlessly change deployment models as requirements evolve. When changing, the features and functionality remain largely the same between options. In fact, our machine learning driven troubleshooting and client network monitoring capabilities are available across all deployment models.

7. Cloud-Management Will Only Manage My Wi-Fi Environment.

While this may be true for some vendors, Extreme is executing its strategy of being the first end-to-end cloud-driven networking vendor. Within 5 months of the acquisition of Aerohive, we have already integrated parts of the Extreme XOS switching portfolio, the VSP switching portfolio, and the WiNG wireless portfolio for visibility and monitoring.

Our roadmap outlines an aggressive time-line for incorporating the broader Extreme Networks portfolio first for visibility and monitoring, then for configuration and provisioning. This includes not only our wireless and switching solutions, but also applications, such as Extreme Management Center.



<http://www.extremenetworks.com/contact>

©2020 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see <http://www.extremenetworks.com/company/legal/trademarks>. Specifications and product availability are subject to change without notice. 29157-0220-26