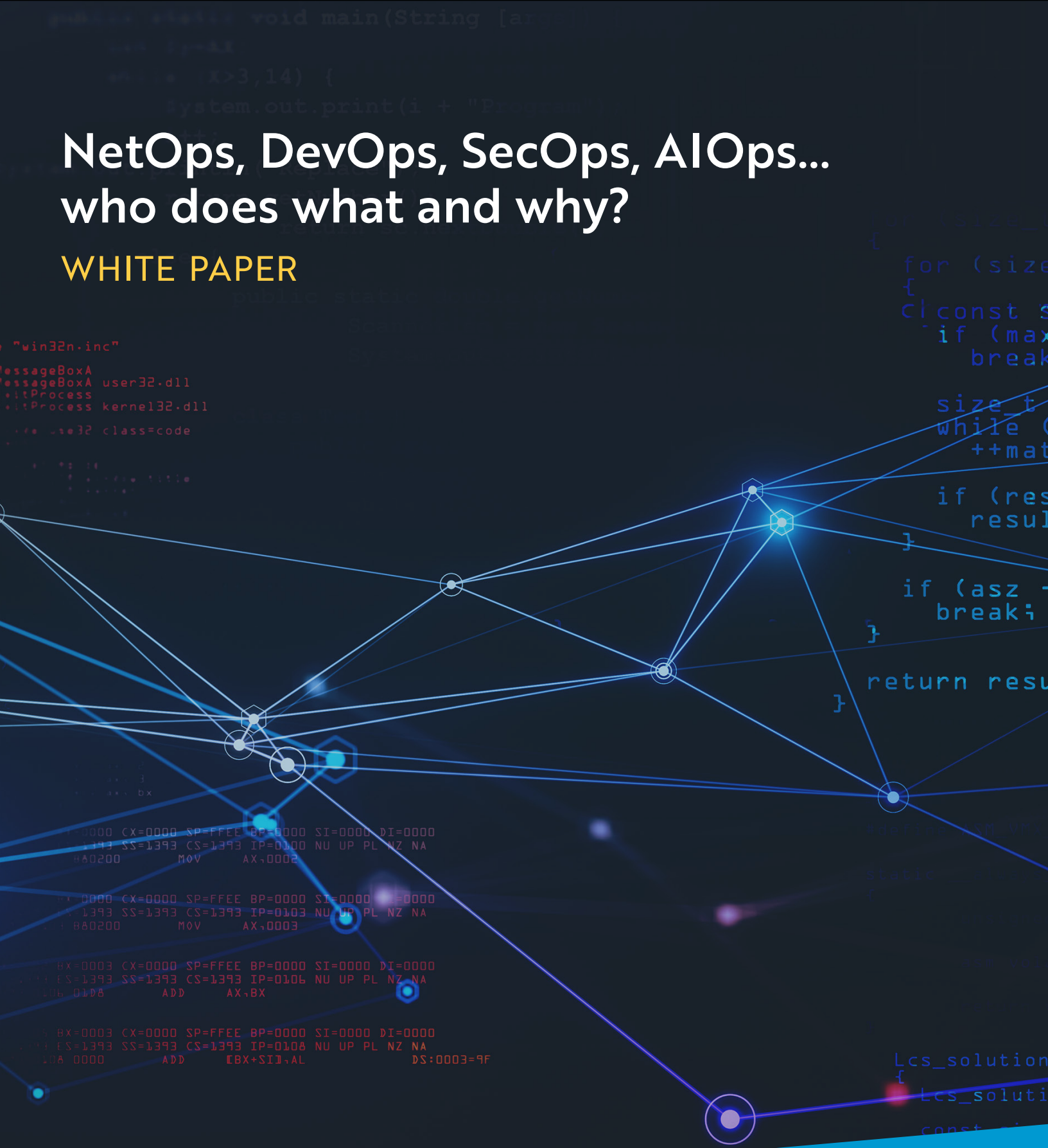
# NetOps, DevOps, SecOps, AIOps... who does what and why?

WHITE PAPER



LiveAction®

# Table of Contents

# Executive Summary

Explore the history of various Ops groups, what the different titles mean, their key functions and what they have in common to support an enterprise's stability.

# IT Operations & Developers – A short history

In the beginning, there was just IT Operations, or Ops for short and Developers, two separate entities with separate management, goals, and very little (if any) communication. The people writing the code and the people deploying and supporting it did not work together.

This resulted in a lot of dysfunction, antipathy, and botched releases. IT Ops used a methodology focused on operational stability and tended to be change resistance, or at least cautious. Devs focused on software and wanted obstruction-free change.

The dysfunction between these two groups was becoming untenable. Something had to give. In 2008 John Allspaw and Paul Hammond gave a lecture called "10 Deploys a Day: Dev and Ops Cooperation at Flickr," a concept that suggested Devs and Ops begin working together.

The idea resonated with Patrick Debois, an engineer from Belgium who coined the term #DevOps in a Twitter hashtag advertising a small agile system admin conference he was hosting. He named the conference "DevOpDays". The concept of DevOps was designed to standardize development and operations practices into one collaborative methodology.

**Going forward, Devs would integrate the operations of building, testing, maintaining, and releasing the products they built into their workflow, becoming DevOps.**

NetOps came around shortly after, applying the DevOps principles to the network infrastructure side of the house. One of these principles is **continuous integration (CI) and continuous delivery (CD)** to streamline efficiency.

SecOps became the next obvious step after the proven success of these changes with both DevOps and NetOps. SecOps had the goal of incorporating security into the development and infrastructure management processes.

Now that we understand the climate that brought on these changes, let's define each group by motivation, look at how these new methodologies overlap, any hybrid combinations, and other Ops categories that they inspired.


Image Source: cyberdb

# Categories of who does what and why?

## The Original "Ops" Categories

- **ITOps** – before DevOps existed it was ITOps and Development. When DevOps came onto the scene some ITOps teams were absorbed, and other continued on doing the same work they did before. Their responsibilities include software deployment, infrastructure provisioning and configuration, software monitoring, determining needs for improvement in software and applications and ticketing this to developers.

- **DevOps** – DevOps do everything ITOps does, but they also develop and write code. Devs write code, deploy, and patch software and applications. DevOps integrations development and operations, working in a continuous loop called the CI/CD methodology. This method allows for maximum efficiency in application and software building.

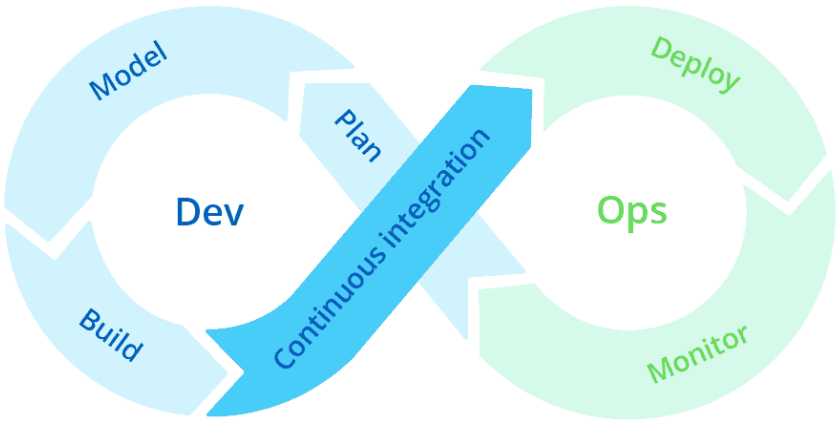



Image Source: Mendix.com

- **NetOps** – networking resource and organizational stability focused. Actions revolve around the understanding that the network is the backbone of all business operations, and that availability should be protected at all costs. This group focuses on network health, network automation, configuration, and provisioning and always has a plan B for failovers in case the network is impacted. NetOps teams make data-based decisions from network analytics and reports.

# Categories of who does what and why?

NetOps typically use Ansible or Python and use the same CI/CD methodology as DevOps but with network activities. NetOps practice "treating infrastructure as code" or IAC. They care most about: network availability, speed, capacity, and openness. They want to prevent performance degradation at all costs.

- **SecOps** – focus on minimizing risk to network infrastructure, operations, development and efficiently resolving existing security concerns. Often characterized by regulations, closed environments, locked down privileges, and compliance requirements, SecOps can be viewed as blockers by other groups. Without cooperation from other groups, SecOps often struggle to keep pace with known vulnerabilities and security risks.

To fill the gaps between these categories, and address emerging technologies like AI, a few subcategories and hybrid categories have been born.


Image Source: AppviewX

## New Age or Next Generation Operations Titles

- **EdgeOps**- focuses on operations of edge networks and ways to automate deployment, management, and troubleshooting of remote branch infrastructure which can be very manual and lack visibility.
- **CloudOps** – focuses only on cloud-specific provisioning, cloud-migration strategy, cloud configuration and management, performance optimization, compliance, and resource allocation.
- **AIOps** - AIOps combines big data and machine learning to automate IT operations processes, including event correlation, anomaly detection and causality determination.
- **NoOps** –a few steps backward, NoOps recreates the days when development and ITOps were separate. NoOps allows developers to develop within a vacuum and toss it over the wall for deployment and maintenance so they can move on to the next thing without delay. Needless to say, this category has not really taken off...

# Categories of who does what and why?

## Hybrid / Combined Areas of Practice

- **NetOps + SecOps (NetSecOps)** – automates network security testing and deploying it into production. NetOps and SecOps have common goals, they both impact users and resources and work on policy compliance. Security-driven networking is a combination of netops and secops and sometimes called netsecops.

- **DevOps +SecOps (DevSecOps / SecDevOps)** – address the concern that development and innovation outpace the ability to secure these products. Their goal is to integrate security into the development of software and applications from the beginning and throughout the entire development lifecycle, instead of as a reactive afterthought. The belief is that all solutions must consider security from the start to respect data privacy and provide adequate protection.

> “Did you know that 2020 was declared the year of DevSecOps?”

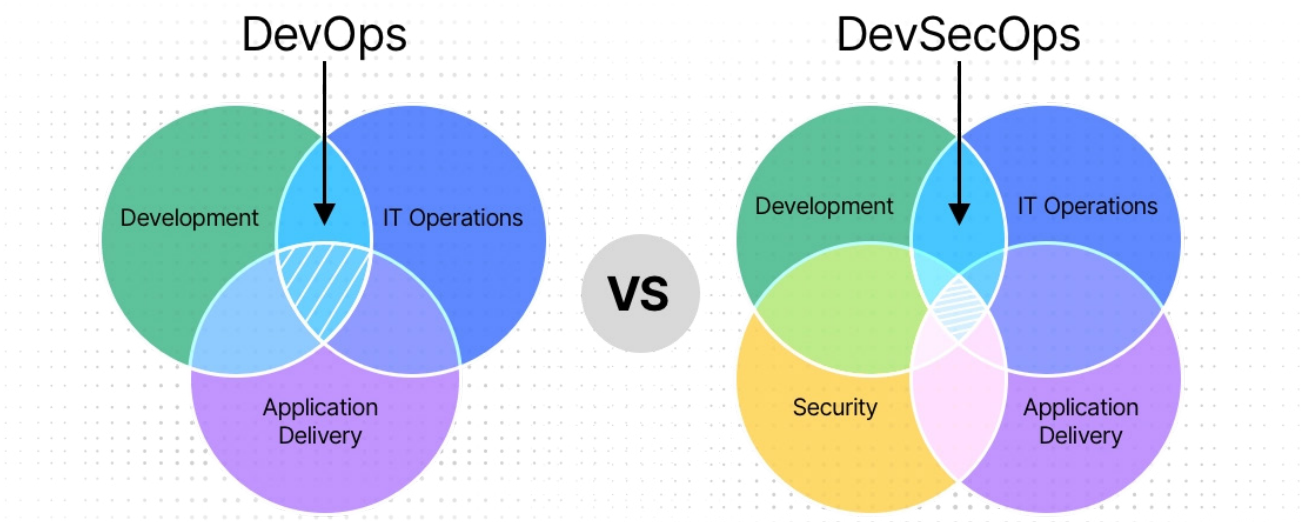



Image Source: imperva.com

# Categories of who does what and why?


Image Source: Cisco

- **NetOps +DevOps** – The combination of NetOps and DevOps is sometimes called NetOps2.0, NetDevOps, and occasionally DevNetOps. This category focuses on automation, agility, observability, and continuous processes. Here are two illustrations that describe the natural overlap of these two categories.

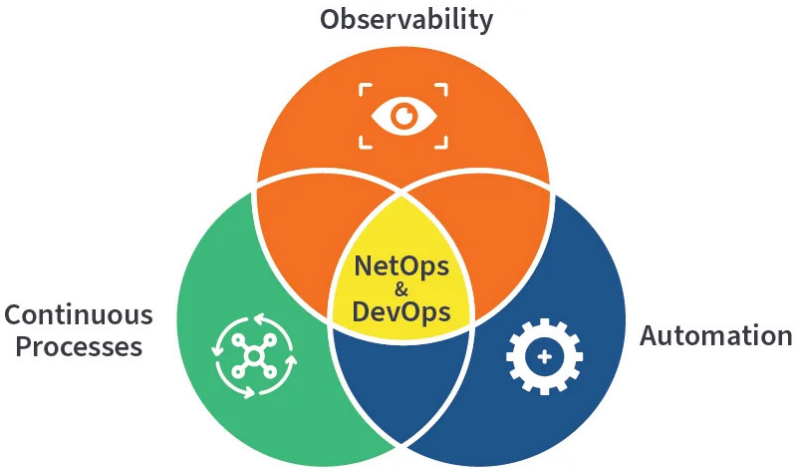



Image Source: Ctfassets.net

- **AIOPs + NetOps** – NetOps are often analytics driven and AI's advancements in analytics, help NetOps make better decisions. NetOps monitoring needs and the growing challenges in network visibility with increasing disaggregated and distributed network models have made AIOps a necessity to add visibility where traditional NetOps monitoring tools fall short.
- **AIOps + DevOps** – DevOps have found that infusing AIOps into their workflow helps automate and accelerate the QA process, monitoring, and troubleshooting. AIOps and DevOps can work together to deploy hybrid and multi-cloud environments and improve observability.

# Conclusion

Despite the differences in philosophy and areas of responsibility, all hybrid Ops teams share the goals of ensuring business operations, standardizing, and automating processes for repeatable results that protect business resources. Each team's success is interdependent upon the other and requires transparency, communication, and visibility into the processes and results on the network.

Visualization of network telemetry and the ability to collect and analyze traffic patterns provides data on bandwidth allocation, application performance, and trouble areas in the network. Selecting a powerful Network Performance Management (NPM) solution gives a way to connect the pieces. Plan, deploy and measure changes across an organization with improved accuracy and precision. LiveAction offers the broadest network telemetry platform on the market, extending network visibility to the WAN edge, into datacenters and the cloud for actionable insights.

LiveAction®


960 San Antonio Rd, Suite 200, Palo Alto, CA 94303
+1 (888) 881-1116

## About LiveAction

Gain visibility into network and application performance, automate monitoring and reporting, and scan for vulnerable network traffic to resolve many of the key objects that DevOps, NetOps, SecOps and AIOps prioritize. LiveAction provides end-to-end visibility for network security and performance from a single source of truth. Find out more today, at LiveAction.com.