Network Operations Centers:
Understanding Your Options

MILESTONE
Strategic IT • Enabling Success

Table of Contents

Executive Summary

As network health and security become increasingly critical components of modern business, companies are looking for a single, viable resolution to address the wide array of challenges they are facing. From simple fluctuations in traffic to advanced attacks by malicious hackers, networks have grown into complex entities that require constant monitoring. Because most companies' internal IT teams often lack the knowledge and resources to handle network monitoring and maintenance on their own, Network Operations Centers (NOCs) have emerged as a powerful, often proactive solution to network management for businesses of all sizes.

NOCs exist in several iterations that vary slightly in form and function—from basic, reactive services to complex, proactive solutions complete with security monitoring. Each of these NOC variations combats challenges, including network downtime, poor performance, alert noise, compliance, and security threats, as well as addressing issues related to missing or incomplete diagnostics and root cause analysis. These challenges affect different companies in different ways, so it is important for IT leaders to evaluate their individual needs when choosing a NOC strategy.

As a result of constant monitoring by expert engineers, the benefits of employing a NOC range from increased uptime to heightened security. In some cases, NOCs also lead to the identification of root causes and the proactive prevention of potential network issues to help networks improve over time. No matter what strategy you choose, implementing a NOC solution is a great way to monitor, maintain, and protect your network.

The Network Landscape Is Changing

On October 21, 2016, companies across the globe were blindsided by a large-scale, distributed denial of service (DDoS) attack. The attack, which pummeled Dyn Inc.'s domain name system (DNS) infrastructure, crippled the networks of a massive number of customers, many of which were household names like Netflix, Spotify, Reddit, Etsy, and Github. The attack also impacted Amazon Web Services (AWS), a cloud-computing platform used by enterprises, startups, and the public sector in 15 geographical regions around the world[1].

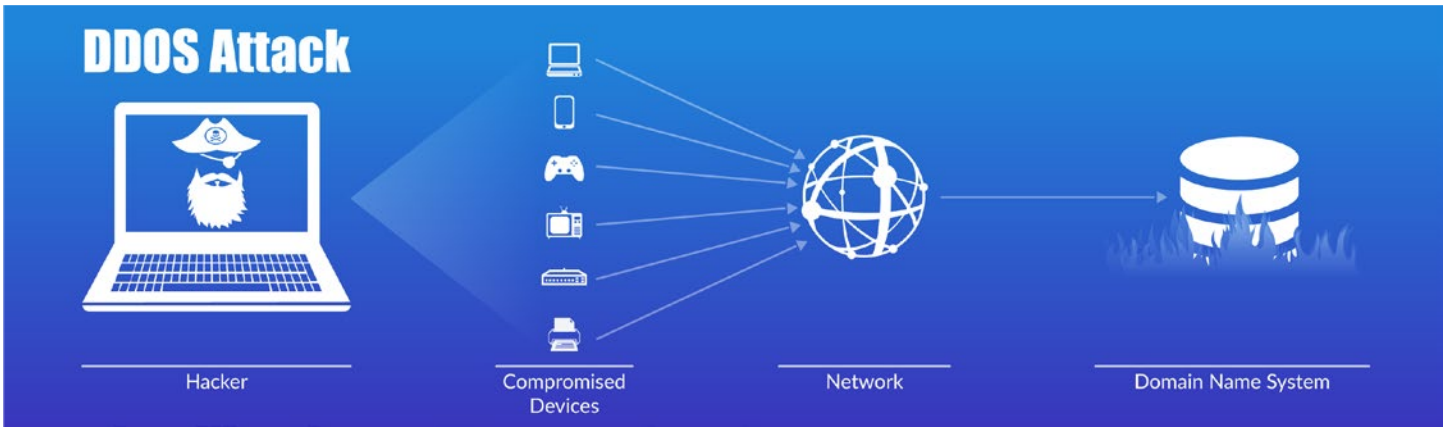
For these Dyn customers, revenue was lost, business continuity grinded to a halt, customer satisfaction plummeted, and internal IT's focus was diverted away from core competencies to manage unfolding network problems.

Unfortunately, attacks like this are not only becoming more common, but also more sophisticated. With the proliferation of mobile collaboration, e-commerce, big data, and internet of things (IoT) devices, hackers have more network entry points available to them, and they are adapting to (and taking advantage of) the changing IT environment faster than many companies can keep up. For example, just one month before Dyn was attacked, hacker 'Anna_Senpai' released the source code for the malware responsible. The malware is called Mirai, and it's a tool that performs continual scans of the internet to find IoT devices and takes control of them through factory default or hard-coded username and password combinations[2].

Despite the known risks behind e-commerce and IoT, both are growing fast. In the third quarter of 2016 alone, retail e-commerce in the US totaled roughly $101.3 billion, an increase of 15.7 percent from Q3 2015[3]. Plus, IHS (Information Handling Services Ltd.) market researchers forecast that the installed base of IoT devices will grow from 17.68 billion in 2016 to 75.4 billion in 2025[4]. That's a lot of money being spent on a lot of devices and services. But if the devices stop working and the services are interrupted, the profits stop, too. Can your business afford the impact?

> **"Network Operations Centers (NOCs) have emerged as a powerful, often proactive solution to network management for businesses of all sizes."**

These days, customers demand reliable, 24/7 accessibility to information, products, and services. And, since information, products, and services rely on a healthy network to work properly, the negative effects of a network outage can be very costly for businesses. As a result, maintaining a healthy and efficient network has become a critical requirement for successful businesses. But how can you ensure that your network not only remains operational, but improves? The good news is your business doesn't have to do this alone. A **Network Operations Center (NOC)** can help.



What Is a NOC?

A Network Operations Center is a physical place where technicians and skilled engineers perform eyes-on-glass monitoring and troubleshooting of a business' network, often on a 24/7 basis. NOCs contain several monitors, and each monitor is connected to a business' Network Management System (NMS), a set of automated software tools that track the status of your hardware and the activity on your network. Most Network Management Systems also include useful features such as: integrated performance, integrated alarm, resource management, fault processing, service quality management, and an integrated dispatching system.

Network Management Systems are typically connected to a broader set of IT Service Management (ITSM) tools to track ticket data and create visualizations. NOC technicians use these visualizations to determine network health by watching for alerts and checking for small anomalies that could grow into bigger problems. If a technician does spot an anomaly and expects that it may lead to a larger issue, such as system failure, they use onsite tools to resolve the issue or escalate it to another tier of engineers, often located offsite. Effective NOC services typically follow a three-tiered escalation path, with each tier focusing on a specific facet of your network

How Does a NOC Work?

Think of a NOC as an air traffic control center that monitors your network's "flight." Air traffic control is a centralized hub of technicians that actively monitor flight patterns, trajectories, and incoming and outgoing traffic to literally prevent crashes while the individual pilots focus on steering their planes. Air traffic control centers help each plane get where it is going safely, while also monitoring and streamlining its flight plan. Similarly, a NOC can help your business stay in flight by monitoring your network activity, rapidly troubleshooting incidents, and even proactively investigating anomalies to prevent incidents. In the same way that air traffic control centers analyze weather conditions, re-routed flights, and active delays, certain NOC services also leverage analytic tools to identify the sources of common problems that your network regularly faces, which ensures that your network not only functions, but also becomes more efficient.

What Challenges Can a NOC Solve?

Although a NOC cannot necessarily prevent a customer from being attacked, it can help to shield the customer from the effects of an attack. For example, it's possible that the impact of the DDoS attacks on Dyn could have been much less severe if they had a NOC to monitor their network more closely, or if their traffic alerts had been robustly filtered to reduce alert noise and trigger only malicious traffic. And while not every business will be the victim of a network attack like Dyn's, most businesses will face a varying degree of common challenges associated with network operation and security. Network Operations Centers can help business resolve—or even prevent—challenges like these:

Network Downtime	A network outage, or downtime, refers to a period of time when your network is unavailable. Downtime is typically caused by one or more contributing factors, such as hardware error, human error, device configuration changes, power outages, natural disasters, or intentional attacks. When a network is down, especially for an extended period of time, businesses experience revenue losses and reduced customer satisfaction.
Poor Performance	Network performance depends on several factors and manifests in a variety of symptoms, such as high latency. Network slowdowns can be caused by malware, high traffic, old or malfunctioning equipment, or suboptimal network configuration[6]. Without a NOC, it can be difficult to determine which of these factors are causing your network to perform poorly.
Lack of Diagnostics	Many businesses have so much networking equipment in place that it can be difficult to pinpoint symptoms and identify where issues are coming from. Without proper diagnostics in place, problems can go undetected and even get worse over an extended period of time.
Lack of Root Cause Analysis	Root Cause Analysis (RCA) is the process of determining why a problem occurred. Without RCA, network management remains purely reactive, meaning that IT addresses symptoms instead of preventing disease. Symptoms tend to resurface continually over time because the reason for the symptoms hasn't been addressed, which ultimately leads to wasted resources.
Security Threats	A business' network is home to its most valuable data, such as confidential files, financial information, and customer data. This makes networks a popular target for hackers, like Lizard Squad, as well as malware and corporate espionage. Managing access control and monitoring suspicious network traffic is time consuming and requires training, but it's critical to identify signs of anomalous network activity or possible security breaches.

Alert Noise	If a company has an expansive network with a large number of users, the sheer volume of alerts can inhibit the ability to manage network traffic, increase the likelihood of network or system failure, and compromise network security.
Lack of Expertise	Network management is an advanced skillset that may fall out of the core competencies of many companies' internal IT teams. Even with an automated system for alerts and network monitoring, it takes a trained eye to spot anomalous activity that can evolve into greater problems down the line.
Excessive Time Spent	For many of the reasons above—including weak diagnostics, lack of RCA, and minimal expertise—internal IT teams may find themselves spending more time than necessary monitoring and addressing network problems. This time can add up and cause outages to last longer than they should, which equates to reduced customer satisfaction and lower revenue.
Compliance	According to a recent survey of 315 network professionals, 76 percent of respondents reported having network compliance requirements in place, but only 20 percent were highly confident that their networks actually met the compliance standards they had defined[5]. With SOX compliance being top-of-mind for many businesses, this lack of confidence around compliance is a big concern.

Understanding Your Options

NOC service models come in a variety of shapes and sizes, each of which provides different approaches to network management and support. A NOC service is widely considered within the industry as a solution to the common network issues highlighted in this whitepaper, but truly effective NOCs provide a proactive approach to maintaining the health of your network. Generally speaking, NOC services can be categorized by the following approaches:

- **"Reactive" NOC**: This level of NOC services primarily utilizes a break-fix model by manually monitoring your network and responding to incidents as they appear.
- **"Proactive" NOC**: This level of NOC services not only manually monitors your network, but also leverages automated software monitoring and Root Cause Analytics (RCA) to identify and analyze trends in your data. With this extra layer of analytics, this variety of NOC services can proactively address the root causes of your network's problems, rather than each symptom, to improve the overall efficiency of your network.
- **"Proactive" NOC with Security Operations Center (SOC)**: This level of NOC services manually monitors your network, leverages automated software monitoring and RCA to analyze data trends, and utilizes a SOC to manage access control, intrusions, and threat intelligence. This added layer helps to prevent costly attacks to your network and mitigates a variety of threats.

Aligning Your NOC Strategy

Each level of NOC services has merits and addresses a specific set of needs. So, it's extremely important that each business clearly identifies their specific network requirements before selecting the NOC service that is right for them.

Reactive NOC Service

If your business is small and rarely experiences high network traffic or significant internal ticket volume, then you may not need a NOC service at all. However, if your IT team is having difficulty maintaining your business' network or managing incidents within your network, then consider leveraging a basic, reactive NOC service. At its core, a simple NOC service manually monitors your network and responds to incidents as they appear. Round-the-clock support ensures that your network remains healthy and minimizes system down time. This reactive NOC service approach is also the most cost-efficient for those who do not need the added security layer of a SOC.

Proactive NOC Service with Data Analytics

If your business is experiencing an overwhelming number of incidents within your network, consider a proactive NOC service that uses data analytics tools. In addition to the platform and manual monitoring that the basic NOC provides, this proactive approach utilizes Root Cause Analysis (RCA) to identify trends in your network data. This allows the NOC to move past the break-fix model and actually assess the overall health of your network. By identifying the root cause of problems rather than responding to each symptom individually, a Proactive NOC service can decrease the number of incidents in your network, which allows NOC engineers to more readily recognize and address larger issues. This process ultimately streamlines your network, and ensures that your business runs more efficiently.

Additionally, a proactive NOC service is especially beneficial to growing businesses. The tiered structure of a NOC service along with its automated platforms allows NOC engineers to accommodate and adapt to changing system demands. Therefore, the flexibility that this structure provides allows a NOC service to scale with your business. For businesses experiencing dynamic growth, a NOC service with data analytics is particularly beneficial. By streamlining your network, this proactive NOC service approach ensures that your network is running efficiently, and capable of handling the stress of your business' evolving needs.

Proactive NOC Service with SOC

Confidentiality and information security are especially relevant in our current era of major cyber-attacks. If your business is concerned about intrusion protection and information security, or if you have experienced data leaks in the past, a NOC service with a Security Operations Center (SOC) is an ideal option. In addition to providing automated platforms supported by tiers of NOC engineers and data analytics, this level of NOC service also includes a SOC that manages access to your business' network, monitors intrusions, and analyzes threat data. This level of NOC service streamlines your network while also providing an additional layer of comprehensive network security. More so, a SOC gives your business unique visibility into the nature of the threats posed to your network.

NOC Options At-A-Glance

Type of NOC	Business Size	Intent to Grow	Security Standards
Reactive	Small - Medium	Minimal	Low
Proactive	Any	Moderate - High	Low - Moderate
Proactive + SOC	Any	Moderate - High	High

What Is the Added Value of a NOC?

NOCs are optimized to recognize, remediate, and prevent an array of network challenges. Because network health and business success are so closely related in the 21st century, the activities performed within a NOC are critical. While it's possible for internal IT teams to manage certain aspects of a network, there are a number of benefits to implementing a professional NOC solution.

Expert Engineers

Investing in a NOC service grants businesses access to experienced, expert-level, and often certified network engineers. This body of expertise leads to rapid identification of root causes and faster resolutions compared to network monitoring activities performed by internal IT teams.

24/7/365 Monitoring

Due to the nature of industries like e-commerce and IoT, it can be tough to predict when a business' customers will need to interact with its network. Round-the-clock monitoring is important because companies that do business online are always open—which means their networks need to be available on-demand. NOCs provide the constant monitoring required to keep business afloat all day, every day.

Increased Uptime

NOC engineers are trained to look for anomalies and stop problems before they start. And, if a network issue does occur, they can resolve it quickly. This means that networks monitored by NOCs are less likely to go down, and if they do, they are down for a minimal period of time.

Heightened Security

NOCs, particularly those with a Security Operations Center (SOC), are well-equipped to help businesses address network issues related to malware and security breaches. In many cases, NOC engineers will notice the first signs of intrusion and prevent potential malicious behavior before threats have the chance to come to fruition.

Root Cause Analysis	The RCA capabilities of an effective NOC service allow engineers to diagnose repeated issues and resolve them once and for all. This not only results in increased uptime, but also allows a network to improve incrementally over time.
Proactive Prevention	Of course, the ideal way to remediate network issues is to prevent them from occurring in the first place. NOC engineers can detect patterns in network activity that typically lead to issues, and then provide steps to correct those patterns before issues develop.

Each of these benefits is inherent to the structure of a NOC service, but depending on the kind of NOC service a business chooses, some of these benefits may be amplified and others may be quieted. It's important to understand the different kinds of NOC services available to maximize your return on investment.

About Milestone

Prem Chand founded Milestone Technologies, Inc. in Fremont, CA in 1997 as an IT relocation company. Nearly two decades later, Milestone has grown into a Managed Services Provider with more than 1,700 employees serving over 200 companies in 18 countries. Our consistent 25% growth rate over the last 9 years has allowed us to open branch offices in Chico (CA), Austin (TX), and Dublin (Ireland).

Our goal is to focus on IT so our clients can focus on their core business, and we believe in customizing our service offerings to the unique needs of our clients. Our IT Managed Services approach includes Platform Engineering Services—a suite of IT solutions including Network Operations Center (NOC), Data Center Operations, Contact Center Services, Internal IT Support, Workforce Solutions, and IT Professional Services. We can fully design, integrate, and optimize your IT infrastructure, as well as support your IT requirements with a 24x7x365 IT Service Desk. Milestone is a trusted reseller of Aruba Networks, Cisco Systems, and Palo Alto Networks as well as a Sumo Logic Partner.

[1] Data Center Dynamics, 2016. http://www.datacenterdynamics.com/content-tracks/security-risk/major-ddos-attack-on-dyn-disrupts-aws-twitter-spotify-and-more/97176.fullarticle
[2] [Sic.]
[3] Census.gov, 2016. http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf
[4] Forbes, 2016. http://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#112677534ba5
[5] http://www.networkworld.com/article/3142838/infrastructure/top-reasons-for-network-downtime.html
[6] http://www.cwims.com/performance/top-10-most-common-causes-for-poor-network-performance/

MILESTONE

Corporate Headquarters
3101 Skyway Ct
Fremont, CA 94539
www.milestonepowered.com
Network Services: http://www.milestonepowered.com/solutions/network-services/network-operations-center-(noc)

Contact Information
Phone: (877) 651-2454
Email: ITsolutions@milestonepowered.com