Progress® Flowmon®

Resilient Cybersecurity with Network Detection and Response

WHITEPAPER

Executive Summary

One of the most important responsibilities of Executive teams in organizations is identifying risk factors across their business and operational landscapes and then mitigating these risks to prevent future shocks or issues that impact operations. In 2023, the threat from cyberattacks is one of the most significant risks faced by organizations.

The cybersecurity threats that organizations of all types and sizes face are numerous, complex, and continuously changing as cybercriminals devise and discover new attack methods. Executive teams need to ensure and be confident that their internal cybersecurity teams or, more frequently in the current landscape, their Managed Security Service Provider (MSSP) are taking all of the cyber defense actions needed to deliver 24*7 protection for staff, clients, data, and IT systems.

Protecting an organization's people and IT systems from cyberattacks requires a multi-layered approach that deploys technology-based solutions and expert knowledge at multiple places. Protections must be in place at network perimeters, on user endpoint devices, on application servers, and for the cloud-based services that are an increasingly common deployment method.

Experience over the last few years where protections have been deployed and used across all of the places listed above has identified another essential component in a complete cybersecurity defense posture. This is the need for 24*7 monitoring of the activity on an organization's network to identify any activity that deviates from the normal, then responding rapidly to prevent cyberattacks from establishing themselves on IT systems and spreading.

Network Detection and Response (NDR) solutions are the tools that have emerged to plug the gap in cybersecurity protection that experience has highlighted. Industry analysts such as Gartner and Quadrant Knowledge Solutions see NDR as essential to cybersecurity defense, not as a cure-all for all cybersecurity threats but as a core part of the multi-layered defense mentioned above.

In the remainder of this white paper, we'll cover the challenges that cybersecurity teams face, outline how NDR helps them defend against attacks, summarize the Gartner and Quadrant Knowledge Solutions' view of the NDR market and solutions, outline the Gartner and Quadrant Knowledge Solutions evaluation of Flowmon's NDR solution provide some color via Flowmon customer case studies, plus outline how you can quickly try out Flowmon Anomaly Detection System (Flowmon ADS) on your network for free (Flowmon ADS is our NDR product).

The key takeaway for Executives? Ask your cybersecurity defense team if they use NDR and how it fits into your broader cybersecurity defense strategy.

Challenges Faced by Cybersecurity Teams

The threats that cybersecurity teams have to deal with and prevent show no signs of diminishing any time soon. Ransomware attacks and data exfiltration are the attack types that most organizations face, with advanced persistent threats (APTs) also used by state-based cybercriminals and for industrial espionage. The Sophos State of Ransomware 2022 report (see references section for link) shows that from 5,600 organizations questioned across 31 countries, two-thirds got hit by ransomware in the past year. Of those attacked, 65% had to deal with data that attackers had encrypted — so 43% of all those that detected a ransomware attack had to clean up the fallout afterward. The average cost to recover after an attack was $1.4 million, with the average payment to cybercriminals reported as $812,360, plus the time needed to recover from the attack averaging a month.

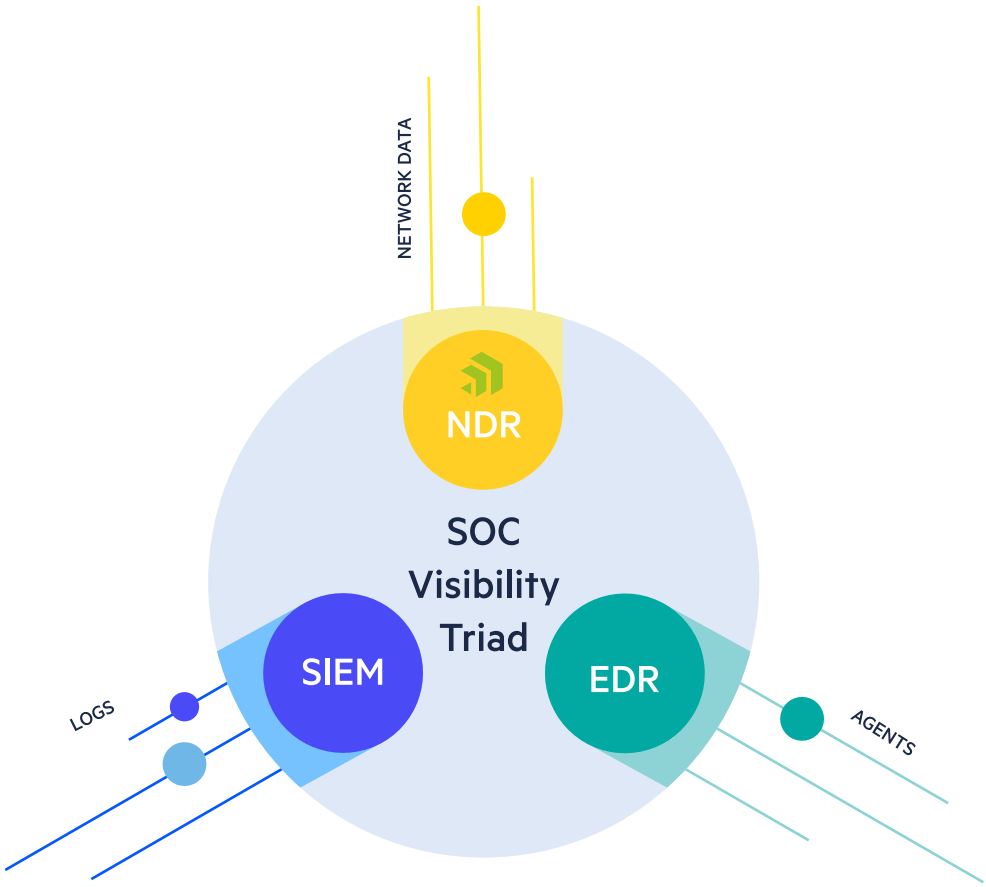
Ransomware is not the only threat that must be addressed, of course. The Sophos report also outlines that organizations questioned saw a 57% increase in volume across all cyberattack types, but ransomware and data theft are the most significant threats at present. The threat landscape that needs defending has increased significantly since 2020. Many more people are working remotely now, and this change looks like it will be a permanent shift in how people work. Hybrid working is the new normal. What this means for networked IT systems and their defense is that more traffic comes from external network sources (often called north-south traffic) than comes from internal/corporate network sources (called east-west traffic).

Cybersecurity professionals have deployed many technology-based tools to help defend against attackers. These include perimeter and edge protections such as Firewalls, device protection via EDR (Endpoint Detection and Response) or SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) solutions to automate the collection of security events and logs from across an organization's IT systems to spot anomalies that might be indicators of compromise from cyberattack activity and respond on them.

These existing defensive tools are still required as part of a comprehensive defense strategy. But the threat landscape is constantly changing, and attackers are always looking

for new ways to bypass existing cybersecurity protections, and new zero-day exploits are frequently discovered and patched by software and hardware suppliers. Every time a new zero-day vulnerability is published, attackers try to exploit it before IT teams have had a chance to update their systems to patch the vulnerability. Plus, the data showing the high number of successful attacks that bypass existing security measures and then persist on IT systems for a long time before detection shows that more is needed to bolster cybersecurity defenses.

Gartner analysts created the SOC Visibility Triad to explain how NDR is now a crucial component of a cybersecurity defense strategy and how it fits with the more widely known SIEM and EDR. SOC is an acronym for Security Operations Centre. SOCs are essential for the 24*7 protection that modern networks require, as they are focused on monitoring networks & systems and responding to any attack or suspicious activity. SOCs can be staffed 24*7 using shift working patterns and allow protection around the clock to thwart cyber attackers who work globally and not just during office hours in a particular time zone.



As the diagram above shows, NDR targets the analysis of network data. In contrast, SIEM analyses log data (and other system information), and EDR monitors and protects endpoint devices with agents and other technology. NDR solutions have emerged from existing network monitoring solutions to add another crucial layer to defenses by providing SOC teams with real-time metrics about network traffic and behaviors, plus alerts on suspicious activities coupled with automated responses to stop potential attack activity before it can do extensive damage.

How NDR Enhances Cybersecurity Defense and Response

Given the high costs and lost operational time when dealing with a ransomware attack, it is imperative that any attack activity is detected and dealt with as rapidly as possible. You don't want your organization to be in the 43% who had to clean up after a successful ransomware attack. The same is true for other cyberattack methods like different malware types, APTs, and more.

NDR works in tandem with SIEM, EDR, and other technologies deployed at various layers and locations within an IT deployment infrastructure. NDR monitors both north-south and east-west traffic to highlight network anomalies that indicate malicious activity from external or insider threats undetectable by perimeter and endpoint security tools. The best NDR tools operate by combining packet data and flow data for the most accurate detection and assisting with the feasibility of deployment. They can also switch to full network packet capture and analysis when an abnormal event occurs. Full packet capture requires large amounts of storage and compute power on modern high-bandwidth networks and should only get used when flow data analysis doesn't capture the necessary data.

An NDR solution should deliver the following functionality to work with the other tools within the SOC Visibility Triad to enhance overall security:

Threat Detection

Using both non-signature-based and signature-based techniques together to identify and highlight suspicious and anomalous network traffic and activity. Rapid detection is vital to prevent attacks from spreading via lateral movement from infected nodes to others, enabling the movement of malware and other attack software onto compromised

IT systems. Threat detection occurs via analysis of the network traffic, and as malware or botnet will need to communicate on the network at some point to spread or exfiltrate data, NDR eliminates any blind spots in the IT infrastructure that other protection solutions miss.

Threat Hunting

NDR solutions actively look for threats on the network in real time. Theat hunting looks for abnormal behavior, unknown devices, and other additional threats that pose a risk. Active threat hunting on the network is closely tied with the gathering and consumption of threat intelligence information:

- **Threat Intelligence -** A lot of threat intelligence is available about known threats on the internet. NDR solutions ingest this threat information and can use it to identify activity related to known cybercriminal sites and can block activity based on reputation or other metrics. Threat intelligence comes from trusted open-source lists, Government lists, and commercial providers.

- **Human Expertise** - Nowadays huge volume of anomalies is not able to investigate manually. Machine learning and heuristics-based intelligence deliver rapid time savings regarding repetitive events occurring and threat hunting. Having analysts with high experience to focus on events of interest is crucial. This is where human expertise comes into play to examine and analyze behaviors flagged by the algorithms manually. That combination is still the best way to deliver comprehensive threat detection and appropriate response.

Incident Response

Real-time responses to detected activity are vital to minimize the impact of any attackers who bypass other security measures. NDR solutions can trigger pre-defined response measures in other protection solutions in addition to their alerting functionality.
Real-time Alerting to let cybersecurity teams about any suspicious activity detected as soon as possible is an essential part of NDR. This needs to be done in a way that reduces false positive alerts, usually via machine learning and advanced algorithmic threat analysis procedures.

Digital Forensics

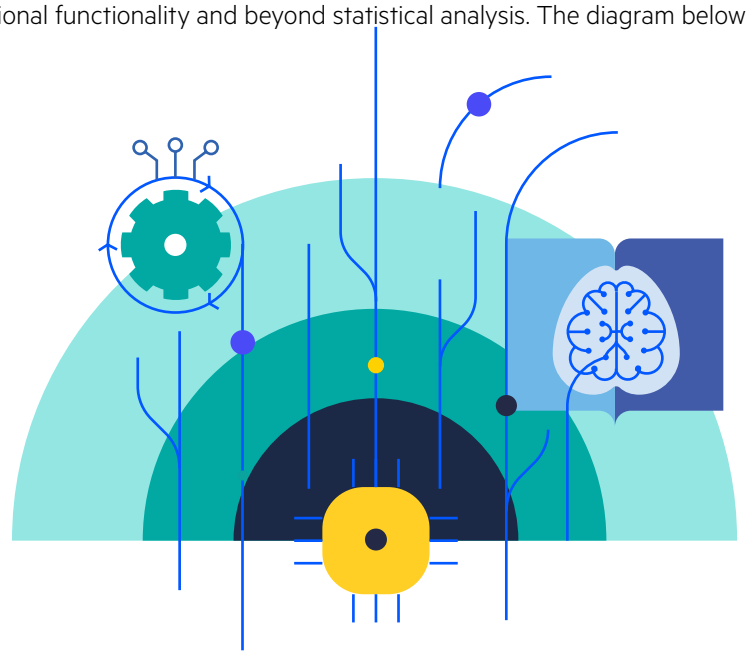
NDR solutions monitor and store information about all network activity between network nodes. The recorded information is typically the network addresses of the two nodes communicating, the duration of their network link, ports in use, the amount of data

transmitted, and extracted layer 7 metadata. The information recorded by NDR does not include the data passed between systems unless this is intercepted explicitly via packet capture in response to an abnormal event. In most cases the Flowmon ADS solution will not need to do full packet capture. Because of this it is more flexible, easier to scale, and cheaper to deploy and operate than an NDR solution that relies on packet capture. NDR data that is captured can be used for later network analysis via dashboards and custom reporting. Digital Forensics also includes post incident analytics in order to get the complete picture on how cybercriminals gained access to the network, so that any security gaps can be addressed.

System administrators can deploy NDR solutions in various ways that match the network infrastructure that an organization is using. Deployment on-premise, in the cloud, and a hybrid mix of both is typical, as is the deployment of software-based data collectors at strategic points across the network to gather telemetry data for analysis.

What Sets Flowmon ADS Apart from Previous Network Monitoring

Tools that monitor network traffic and use statistical algorithms to highlight deviations from baseline behavior have been available for some time. These tools work well for significant anomalies that manifest in large volume of traffic and deviation from the baseline. Modern threats slip under the radar of statistical algorithms and thus being unnoticed. Flowmon ADS is an evolution of these analysis tools that goes beyond traditional functionality and beyond statistical analysis. The diagram below outlines what



Machine Learning

A detection engine using various machine learning (ML) techniques to detect suspicious irregularities in network traffic. The ML-based engine can use both supervised and unsupervised learning in training scenarios to learn about typical network activity and therefore be able to spot and alert on anomalous activity. Flowmon used the following machine learning approaches:

1. Unsupervised Learning - using this technique, Flowmon learns directly on the monitored network, without the data flowing over the network being marked or labelled in advance. This is done using these approaches:

- **Prediction based on historically collected data** - Flowmon builds a linear regression algorithm to fit a linear curve with historical data values, and over time fits new data to the curve and looks at how things should look according to that curve in the next time interval. Any data that falls outside the mathematical model will be flagged as an alert.

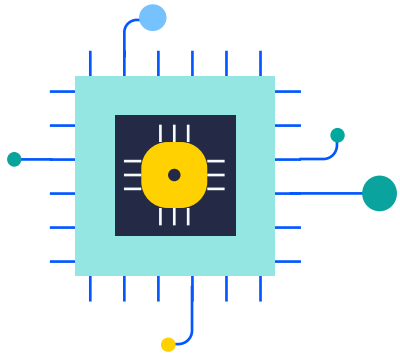
Flowmon also uses four techniques to detect anomalous data types:

- **Clustering algorithms** - Flowmon creates data clusters from collected data activity on the network, which is marked as correct data for regular network activity. If any future data collection includes data that falls outside of this defined norm, then it is flagged as an anomaly.

- **Probabilistic automatons** - Network status is modelled using states and transition probabilities using normal network data. Algorithmic probability automatons take network activity as an input to compare to the models that have been built up. If there is a mismatch, then an anomaly is flagged.

- **Statistical modeling** - A statistical model of the network is created, and if the future activity doesn't fit this model, Flowmon reports it as an anomaly.

- **Entropy modeling** - This method is used to create a picture of the network, and if this entropy value changes in the future, an anomaly is generated.



2. Supervised learning - This technique takes existing known threat information as labelled data and the Flowmon machine learning engine uses it to look for known threats and bad actors & domains. Supervised learning enables:

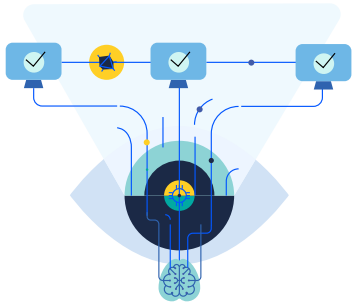
- **Detection of random domains** - the system uses a probabilistic language model trained to recognize legitimate internet domains. If any access request or connection attempt comes for a domain that does not fit the model, or if it looks to be trying to mimic a legitimate domain, this is detected, and alerts generated.

- **Detection of the use of DNS over HTTPS** - encrypted DNS requests on HTTPS is a common attack vector. A supervised learning model using a decision tree inspects the input DNS over HTTPS using historical behavior data in the training set to identify legitimate use or possible attack activity.

3. Adaptive Baselining - Not to be confused with the baselining that's part of traditional network behavior analysis tools. Flowmon Adaptive Baselining works at the individual network host level and learns how each host typically behaves in respect to the other hosts it communicates with. By doing this, the Flowmon can rapidly spot if a host has a sudden change in behavior — such as transmitting a lot of data, which is often a sign of data copying for exfiltration to cybercriminal-controlled servers on the Internet.

4. Heuristics - Heuristic algorithms home in on a particular set of behaviors so that system admins can detect them if they occur on a network. For example, when a user on a network is using a client to talk to an unapproved peer-to-peer network like BitTorrent, there are multiple telltale symptoms that this activity generates, that are recognized and evaluated using a probabilistic model. Heuristic algorithms created to pinpoint specific activities like this allow them to get shut down almost immediately.

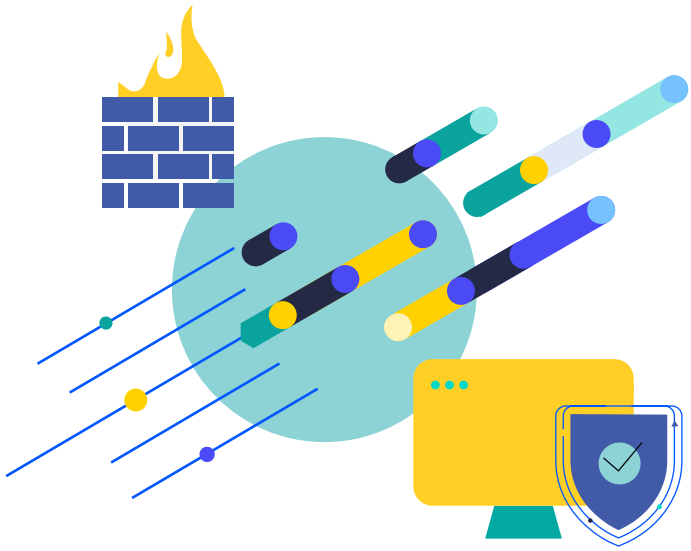
5. Threat Intelligence - As mentioned previously, intelligence data from various trusted sources is incorporated into Flowmon ADS analysis. The ingested information can be from open-source (such as MISP), commercial, and Government reputation feeds and include data on known malicious IPs, hostnames, domain names, security certificate signature impersonation, and more. This data is part of the threat intelligence outlined previously and can include known signatures and other data that highlight known indicators of compromise when Flowmon ADS detects them on a network. Additionally, Flowmon ADS also incorporates technology from Suricata to detect and highlight IDS events.



ADS surfaces alerts and other analysis information in ways that make the detected threat easier for people to understand. For example, it provides context-rich incident visualization based on the categories within the MITRE ATT&CK framework to make it easier to keep technical and non-technical people aware of the scope, severity, and future requirements to respond to current threats using language they will understand. Framing alerts and reports within the MITRE ATT&CK framework also provides the ability to compare results on the security picture from multiple security systems in a coherent manner. This overall taxonomy of the activities of attackers helps defenders to understand better what type of activity a particular detection represents.

How NDR Fits into Overall Cybersecurity Defense

Logically NDR fits into an overall cybersecurity strategy between perimeter defenses and endpoint security, as shown in the diagram below.



By continuously monitoring all network activity that passes between nodes on the network and traffic flowing into and out of the private networks to the Internet, NDR is positioned as a single source of truth for all network traffic. Coupled with the ability to monitor and analyze even encrypted network traffic, NDR delivers anomaly detection in real-time, threat analysis, and then alerting. The ability of NDR to enable rapid responses to detected threats enables stopping cyberattack activity much earlier than possible if NDR wasn't in use.

By enabling this holistic view of the network, combined with perimeter security, SIEM,

and EDR solutions, NDR contributes to enhanced visibility and observability of network operations. SIEM and EDR are essential, but they leave blind spots where attackers can hide their malicious code after slipping past perimeter defenses. Plus, not all devices on the network can have EDR deployed to them. For example, IoT devices are frequently a significant security issue, and many can't be protected by EDR. By taking a network-based approach instead, NDR fills these critical visibility and coverage gaps. The combined toolsets take cybersecurity defense to a whole new level by delivering:

NetSecOps Observability

Observability delivers an outstanding network visibility and applications that are running on it. For NetSecOps teams Flowmon provides Network Performance Monitoring and Diagnostics (NPMD) for NetOps and NDR for SecOps. This means that there are no barriers or data silos between these groups, enabling them to work together from single pane of glass, with same aggregated network data and deliver on the promises of NetSecOps. It enables cross-departments to provide effective MTTR, prevent cyber security incidents, outages and interruptions, and finally helps to reduce many downtimes and security breaches.

Regulatory Compliance

Organizations across most sectors have to implement and comply with regulatory measures and obligations. The network intelligent monitoring, data collection and archiving alertingand reporting that Flowmon provides is required by many regulatory frameworks. Flowmon can assist organizations with meeting their regulatory requirements. For example:

- **Europe**
  - Network and Information Security Directive (NIS2)
  - Resilience of Critical Entities Directive (RCE)
  - Digital Operational Resilience Act (DORA)

- **USA**
  - Health Insurance Portability and Accountability Act (HIPAA)
  - California Consumer Privacy Act (CCPA)

- **Saudi Arabia**
  - Essential Cybersecurity Controls (ECC)

Plus, many other existing and emerging regulatory frameworks at the national and industry levels (for example, PCI DSS in the finance sector).

Enable SOC and CSIRT Adaptive Security Architecture

Having robust SOC provision and the expert team to operate the SOCs 24x7 is core to delivering a good cybersecurity strategy and day-to-day defense. As mentioned above, the best cybersecurity defensive solutions combine smart automation with human expertise. Flowmon ADS enables human cybersecurity experts working in CSIRT teams in SOCs to operate an automated adaptive security architecture that detects threats and anomalies, identifies those that are false positives, and highlights those that should be investigated by human experts. It is a fundamental part of Incident Response cycle where Detection and Analysis is important for Containment, Discovery and Eradication followed by post-incident activities with deep capability for Digital Network Forensics. It all helps to be better prepared regarding Incident Handling procedures.

The Analyst Market View of NDR

As shown by their inclusion of NDR in the SOC Visibility Triad, Gartner analysts see the

use of NDR as a crucial part of a broader cybersecurity defense posture. In their **Market Guide for Network Detection** and Response market briefing (updated in December 2022), Gartner says:

> *"The network detection and response market grows steadily and expands to new use cases, such as IaaS. Security and risk management leaders should prioritize NDR as complementary to other detection tools, focusing on low false positive rates and detection of anomalies that other controls don't cover."*

In the Quadrant Knowledge Solutions (QKS) **SPARK Matrix™: Network Detection and Response (NDR), 2022** report published in August 2022, QKS says:

> *"Network Detection and Response (NDR) technology has evolved out of the need to detect and mitigate threats that can slip past traditional security solutions. The need for such solutions has accelerated following the COVID-19 pandemic and the subsequent spike in remote work. This spike is witnessing different non-secure devices connecting to organizational networks and endpoints, making them vulnerable to various types of cyber threats, including malware and ransomware attacks. The NDR solutions help alleviate the situation by providing the organizational SOC teams with real-time, advanced management, exposing threats, and response to curb such threats."*

They also add this definition of an NDR solution:

> *"a solution that leverages non-signature-based techniques, including ML and other analytical techniques, to detect malicious and suspicious traffic in the enterprise network. The tools monitor the network and raise alerts for suspicious traffic in the network. Furthermore, the NDR solutions provide automated as well as manual responses to threats. These responses consist of threat-hunting and incident response tools that continuously ingest and correlate large volumes of network traffic and security events across multiple assets and hops."*

Market Analyst's Evaluation of Flowmon ADS

The QKS Spark Matrix report evaluated and reported on the capabilities of the leaders in the NDR solutions space. From the 22 vendor solutions that QKS included in the Spark Matrix, the Progress Flowmon ADS solution was placed in the Technology Leaders segment due to its high scores for customer impact and technology excellence. To quote from the Spark Matrix report:

"Progress Flowmon ADS offers a complete detection and mitigation of cyber threat in the user's network by adding the network-centric layer with the SOC visibility triad. Progress Flowmon ADS offers an ML-powered detection engine, which combines multiple detection mechanisms to reveal malicious behavior, data breaches, and attack against mission-critical applications of the threat lifecycle. Progress Flowmon ADS offers a custom dashboard based on severity rules across levels to prioritize and report security and networking. Additionally, it enables integration with SIEM, big data platforms, network access control, authentication, firewall, and other incident response tools while ingesting data from various sources like AWS, Google Cloud, Progress LoadMaster, and others."

The QKS Spark Matrix report is linked from the references section at the end of this white paper.

What Flowmon Users Are Saying

About 800 organizations worldwide have adopted the Flowmon ADS solution to enhance their cybersecurity, network detection, and response. Case studies and comments from many of these Flowmon customers are available via the Our Customers page (also linked from the references section below). We'll highlight two with quotes and encourage you to explore others.

Orange Swiftly Solves Multiple Pain Points for Their Security and Network Operations Teams by Scaling Flowmon - Quoting Henrich Snajder (Information Security Manager, Orange Slovakia):

"Network operations uses Flowmon on a daily basis. For example, they are monitoring the engineering network for planning and capacity in order to see the structure of different protocols in the network. They are also using dashboards to get a visibility about network services and applications to locate outages to facilitate quicker responses to solve those problems."

Coop Deploys Progress Flowmon to Observe and Report Data Traffic of its 1300 Subsidiaries - Roberto Abeledo Alonso, Network Administrator at Coop, said:

"We found that Flowmon could handle our data traffic and present the information much faster than our current solution, and there was the usability of the Flowmon portal, which was easier to use than what we had."

The full details of these case studies and many more are on the Our Customers page.

The Analyst Market View of NDR

Comprehensive details of Flowmon ADS are available from that link and via the references section. On those pages, you will find detailed information on how Progress Flowmon provides an industry leading NDR solution that scales from SMBs up to the needs of the largest Enterprise level businesses without being too complex for IT and Cybersecurity teams to use.

Also, on our website, you can sign up for a fully functional free trial of Flowmon, and if you want to speak to an expert to find out more or get help with your trial, use our Contact Form.

References

Links to reports, product pages, and data sources mentioned in this white paper.

Progress: Progress Named a Leader in Network Detection and Response by Quadrant Knowledge Solutions

SPARK Matrix™: Network Detection and Response (NDR), 2022

Sophos: The State of Ransomware 2022

Gartner: Market Guide for Network Detection and Response (Account Required)

Progress Flowmon: Our Customers

Flowmon NDR

Flowmon ADS

Flowmon Free Trial Signup Page

Flowmon Contact Form

Request your FREE trial of Flowmon for 30-days

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to build the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com

/progresssw
/progresssw
/progresssw
/progress-software
/progress_sw_

Progress