Next-generation Visibility and Security with DANZ Monitoring Fabric

Drivers and Benefits

Overview

Network owners need to continuously monitor and secure their networks to ensure the security, performance, and integrity of their mission-critical infrastructure. But as the enterprise network has expanded to accommodate higher speeds, densely deployed campus/data center, IoT and cloud-native services, and scaled-out multi-cloud workloads many enterprises are challenged to operationally and architecturally scale their visibility and security infrastructure.

Traditional methods of gaining deeper visibility into the network, primarily using Network Packet Brokers and SNMP polling for network statistics, are difficult to scale, create visibility silos, and require time-consuming per-device management, ultimately resulting in compromised visibility and security posture for the enterprise. Worse, they represent a misuse of critical infrastructure funding that is needed to protect from application downtime and cyber-attacks.

Today's enterprise networks demand a next-generation approach to network visibility and security – one that allows them to see every network, workload, and location – and to deploy, to operate, and to scale faster, without increasing CAPEX and OPEX.

Drivers for Next-Generation Monitoring Approach

The factors influencing the need for next-generation visibility and security are as diverse as the mission-critical architectures deployed within the enterprise. These factors include:

Business Velocity: The IT organization is expected to roll out services and applications on demand. Service delivery is often tied to SLAs and organizational policies, making the speed of execution critical. Network and security teams are expected to deploy, scale and troubleshoot faster, but are constrained by traditional network monitoring components, such as NPBs, which need to be managed manually, per box—a laborious, error-prone process that slows service rollout and stunts innovation.

Growing Application Complexity: The emergence of virtualized and cloud-native applications, microservices, and containers has driven up east-west traffic within the data center, constraining existing network architectures optimized for north-south traffic. Increasing rack density and more workloads mean that enterprises must scale monitoring and security coverage to match. To maintain application SLA and security, visibility and security solutions must be applied to every packet and flow in the data center and campus—every rack, every location, and every virtual machine (VM), container, and cloud workload. Monitoring at scale and ensuring consistent policies for traffic from different sources is challenging in terms of both costs and operational complexity. Adding to the complexity are tool silos, which slow down troubleshooting and lead to visibility gaps.

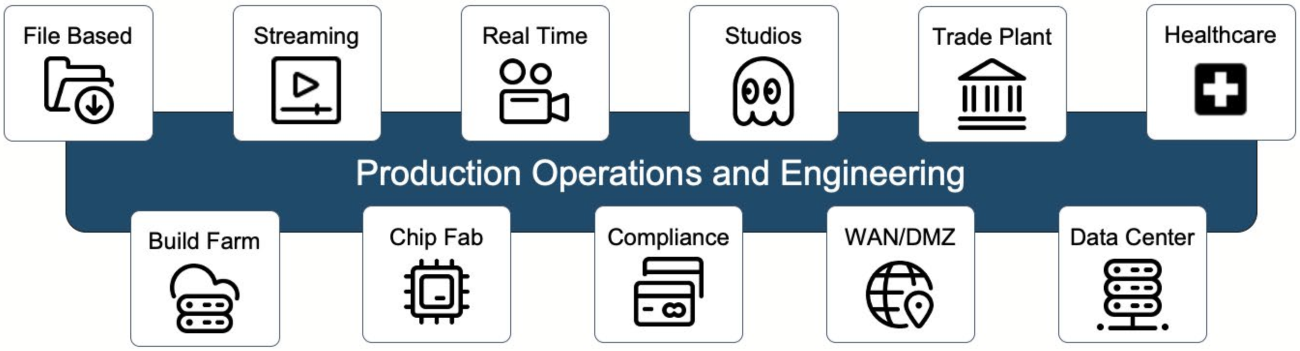

Figure 1: Growing Complexity of Modern Enterprise Infrastructures

Increasing Persistent Cyber-Attacks: The rise of cybercrime and attacks from state and non-state actors has created a permanent threat landscape across every location in the enterprise and invalidated perimeter security as a singular solution. In response, network owners have adopted a pervasive security approach, requiring visibility across the data center, campus, and cloud. Active security measures that detect and block malicious traffic are increasingly important, as is the speed of response.

Stagnant Budgets: Enterprise IT budgets, previously bloated by legacy architectures and tools, have largely stagnated and are projected to remain flat in the near-term amidst political and economic uncertainty. Stagnant budgets create pressure on network and security teams to optimize capital expenditures, adopt modernized architectures, and improve operational efficiency to accomplish more with existing resources.

Traditional network visibility and security architectures – which rely on Network Packet Brokers (NPBs) to provide deep network visibility and traffic delivery – are unable to adapt to today's enterprise requirements. Instead, they pose a barrier to network and security teams as they attempt to successfully monitor and defend the network.

In response to the confluence of these factors, today's operations teams must learn to work smarter, faster, and more efficiently to ensure business continuity.

The Evolution of Network Monitoring

Network monitoring and approaches have historically determined the ability of network owners to scale network and security tools, as they determine the network visibility and security protection potential of each tool.

First Generation Network Monitoring - 1990s

Legacy network-monitoring architectures relied upon coarse-grain telemetry like SNMP-polling or log/flow analysis and later began to use optical TAPs and SPAN (mirror) ports to deliver traffic to the more advanced network and security tools. This provided deeper visibility for monitoring performance, security, and troubleshooting. But, tools for analyzing and troubleshooting network traffic were costly and effectively static, often dedicated to a few mobile crash-carts used in larger data centers and limited security monitoring deployments in the DMZ by static firewalls.

Any change to a tool's view of the network required the tool and it's connections to the network to be physically redeployed, relocated, and reprovisioned. Tools were often over or undersubscribed, as TAPs and SPAN ports were not able to optimize traffic specifically for each tool. Reprovisioning of TAP and SPAN ports led to network outages and often was impossible in production infrastructures outside of infrequent maintenance windows. Ultimately visibility and security budgets could not accommodate the number and placement of tools required to support mission-critical infrastructure.

Network migration from 1Gbps to 10Gbps and beyond created further barriers to enabling or maximizing tool performance. This legacy visibility deployment model quickly became untenable as networks grew in capacity and the number and type of tools used to monitor and secure the network increased.

Second Generation Network Monitoring - Early Network Packet Brokers - 2000s

TAP or SPAN-only architectures with coarse-grain telemetry were eventually supplemented with smarter traffic capture and delivery appliances—the early NPBs. NPBs allowed multiple network tools to share access to the same network links—solving the problem of access contention that network owners experienced with SPAN ports and simple TAPs. They also acted as intelligent optimization and delivery layers between the network and the monitoring tools, allowing each tool to receive only traffic of interest, which ensured it could operate at peak efficiency—neither over nor undersubscribed.

Many enterprises deploying monitoring and security tools used early NPBs to introduce pervasive real-time packet visibility into their networks. NPBs offered granular control over how network packets are manipulated before offloading to tools, and network or security teams could configure these changes remotely, as needed.

Early NPB Capabilities

Packet handling functions considered standard across early NPB vendors included: traffic aggregation, flow replication, L2–L4 filtering, and tool load balancing. Some NPBs supported additional, advanced functions that delivered more ingestible forms of traffic or tools, or to support inline tools. These include packet deduplication, packet slicing, packet masking, header stripping, flow generation, and deep packet inspection. These NPB capabilities significantly enhanced monitoring and security architectures by reducing or eliminating delivery of irrelevant traffic to tools, improving the scalability of tool investments, and allowing tools to be redeployed on-demand to trouble hotspots. Ultimately, this promised to reduce the time needed to discover and address performance and security issues.

Early NPBs operated as standalone appliances, where each one must be configured and managed individually (per-box). Tools connected to an NPB only have access to traffic connected to that NPB, or else require a complex, manual reconfiguration to route the appropriate traffic through multiple NPB layers. Each tool is bound to the visibility potential of the physically attached legacy NPB. The result is fragmented visibility that is sensitive to network changes. If the network grows or its architecture is reconfigured, the tools may need to be physically reconfigured. Traffic is segmented by NPB, which creates rigid visibility architectures that are slow to change—impacting the ability of network and security operations to respond to performance or security incidents.

Silos, Complexities and Costs

Some early NPBs also supported limited clustering or stacking, where multiple NPBs could be interconnected into a "visibility fabric"; however, these clusters did not follow industry-standard or SDN approaches that network engineers were familiar with, and they provided limited visibility into their internal health and performance. They were complex to configure and manage, used rudimentary topologies, and had limited ability to scale. Further, their designs created traffic processing hot-spots that reduced the reliability of traffic monitoring due to undetected packet-loss and corruption. Finally, due to their scaling limits, they led to visibility silos, as different groups of NPBs provided access to different selections of network links.

Because all of the early NPBs promoted silos that are static, time-consuming to manage, unreliable, and difficult to scale, they created new challenges for customers as they tried to operate faster, more efficiently, and more cost-effectively. Siloed, static visibility increases management load, which can lead to inconsistent implementation of visibility and security policies, thus preventing network operators from achieving an overarching view of the network.

Also, just as new technologies allowed enterprise networks to benefit from the lower costs of software-defined networking (SDN) approaches and industry-standard merchant-silicon hardware designs—as pioneered by the mega-scale cloud providers—the early NPBs continued to drive up the cost of enterprise visibility and security using monolithic and proprietary RISC/FPGA architectures. Often, the cost to deploy NPBs came at the expense of investment in advanced analysis and security tools or an increased overall cost to the enterprise IT organization.

The inherently high-cost of early NPB platforms, combined with the box-by-box design limits of early NPBs, has limited their success and produced yet another challenge in dealing with these complex, time-consuming, and error-prone "monitoring fabrics".

Table 1: Problems that Early NPBs Introduced and New Requirements

Early NPBs	Limitations and Challenges	New Requirements
Static Designs • Physically-bound, inflexible • Require manual or physical intervention to make changes	• Changes to tool views require physical reconfiguration or manual box-by-box management • Lack of resilience increases the risk of visibility loss/gaps	• Make changes on-demand, in software, without box-by-box management or physically reconfiguring/redeploying tools • Resilient SDN design to ensure continuous monitoring
Siloed Visibility • NPB-tool groups have different visibility profiles	• Visibility gaps across silos • Inconsistent monitoring/ security protocols • Time-consuming to manage separate NPB/tool groups	• Persistent and on-demand visibility throughout the data center—every rack, location, VM, container,and cloud
Per-box Management • Box-by-box functionality and management	• Slow, complex, error-prone management • No automation/programmable workflows	• Single pane of glass • Easy to manage, fast to provision, upgrade & operate
• Proprietary Hardware • Expensive • Vendor lock-in	• High CAPEX • Cost-prohibitive to scale • Large up-front commitment	• Enable hardware choice • Independent linear scalability • Subscription pricing

Next-Generation Network Visibility and Security – Today's Requirements

Today's enterprises require intelligent, agile, and flexible monitoring and security architectures that provide pervasive visibility, single-pane management, zero-touch scale, automation, and hardware choice. The capabilities previously assumed by legacy NPBs are still required; however, the distributed, proprietary, per-box design of legacy NPBs no longer suits the data center or enterprise in general, which demands solutions that can be operated quickly and efficiently.

Network owners need a dynamic solution that enables tools to have access to traffic from any rack, any location, any VM, any container, and any cloud—and scale-out as needed—without physical reconfiguration or box-by-box management. Such a solution would simplify and accelerate change management and time to troubleshoot issues and mitigate attacks while reducing OPEX and CAPEX.

A next-generation visibility and security architecture must be able to deliver the following benefits to the enterprise:

- See everywhere, across the organization (every rack, workload, edge, campus, data center, cloud and remote site)
- Deploy, scale, and remediate faster and more efficiently
- Optimize OPEX & CAPEX

To deliver these benefits, what's needed is a visibility and security architecture that operates as one logical NPB enabling tools to be physically anywhere, but logically everywhere, so they can dynamically monitor and defend the network in real-time. A logical "super-NPB," operating as a fabric, would also give network and security teams the single point of management needed to operate and scale efficiently.

To achieve this next-generation NPB architecture, cloud principles must be applied to legacy NPB functionality. By introducing a software-defined, controller-based, open-hardware design, data centers can gain a complete view of the network and a single point of configuration and management. This approach contrasts with the traditional, "legacy" approach to network visibility—where appliances operate box-by-box and architectures are rigid and expensive.

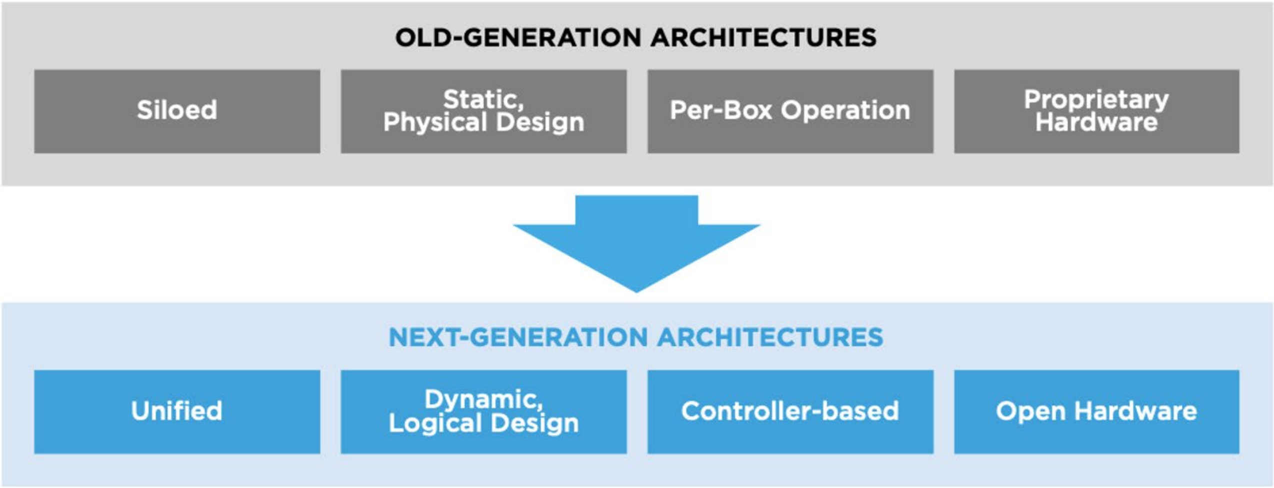

Figure 2: Old-Generation versus Next-Generation Architectures

Software-based design enhances visibility and security architectures. Rather than a proprietary, box-by-box architecture, a controller-based SDN fabric enables auto-discovery and configuration of visibility nodes, zero-touch scale-out, single-pane management, built-in resilience, and hardware choice, allowing network and security teams to operate with greater agility and flexibility.

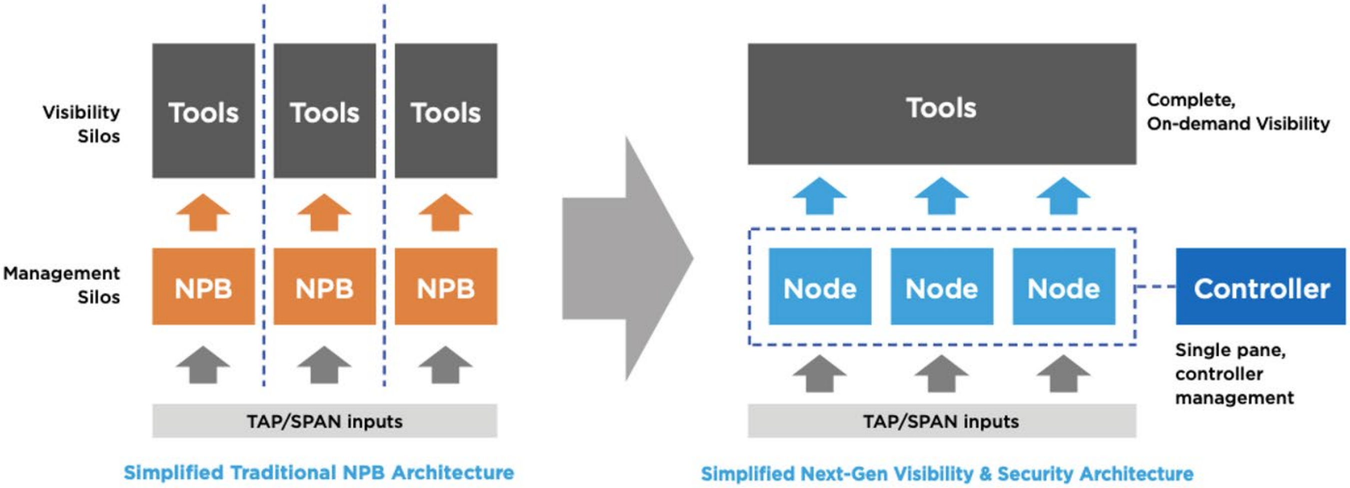

Figure 3: Legacy NPB versus Next-Generation Visibility and Security Architectures

Next-generation visibility is an advancement over box-by-box packet brokering. Standalone NPBs and limited NPB clusters cannot provide a comprehensive view of the network. Instead, these legacy NPBs create silos of visibility that are challenging to manage and often require tools to be uprooted and moved if they need a different view, or if there are changes to the network infrastructure. In contrast, next-generation visibility uses a software-defined model, where the underlying nodes are centrally controlled and can change their state dynamically, without physical intervention.

Introducing Arista DANZ Monitoring Fabric

Arista DANZ Monitoring Fabric (DMF) is a next-generation logical network packet broker (NPB) architected for pervasive, organization-wide visibility and security, delivering multi-tenant monitoring-as-a-service. DMF enables IT operators to pervasively monitor all application traffic at every location in the enterprise network. Deep hop-by-hop visibility, predictive analytics, and scale-out packet capture—integrated through a single dashboard—enables simplified network performance monitoring (NPM) and SecMon workflows for real-time and historical context.

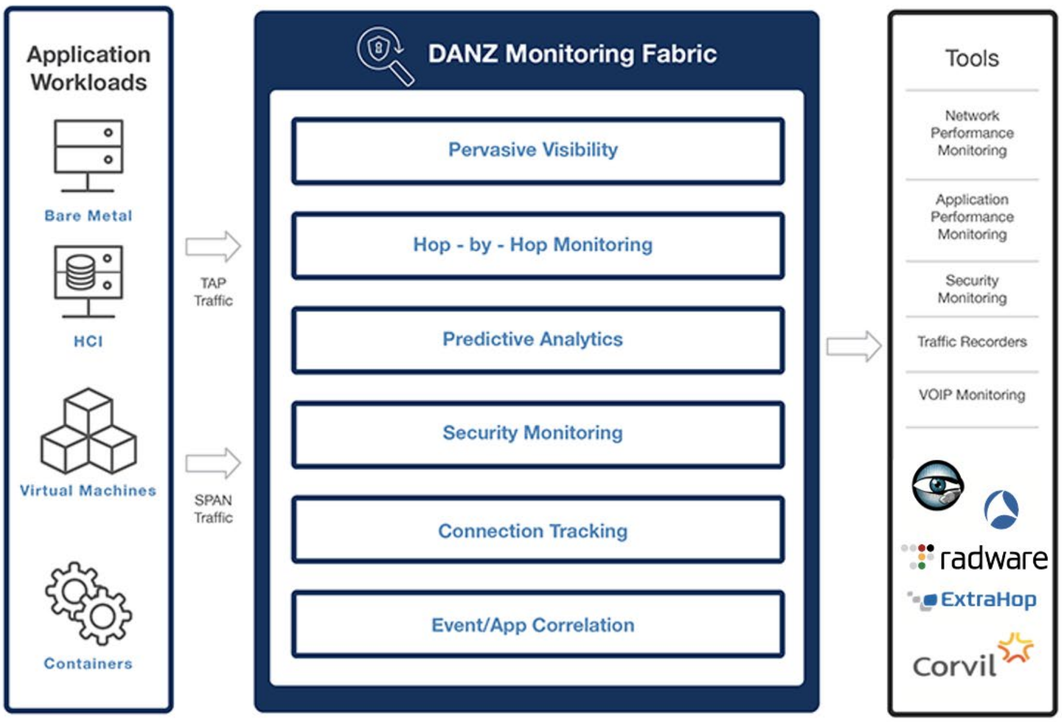

Figure 4: Predictive, App-aware, Flow Intelligence for Pervasive Analytics

DMF networking platforms are deployed adjacent to the production network by connecting them to SPAN and TAP ports from the production network, much like early NPBs, to form an intelligent out-of-band monitoring platform. By visualizing all application to application and application to end-user communications, DMF provides the ability to discover application dependencies and to minimize the adverse business impact of outages.

Architecture

DMF is architected for pervasive, organization-wide visibility and security, delivering multi-tenant monitoring-as-a-service. Based on a model leveraging horizontal scale-out fabric architecture, and using industry-standard switches and servers, DMF allows IT to institute an open "build-as-you-grow" visibility and security platform economically across the entire enterprise.

DMF enables IT operators to pervasively monitor all application traffic by gaining complete visibility into physical, virtual, and cloud environments. Deep hop-by-hop visibility, predictive analytics, and scale-out packet capture — integrated through a single dashboard — enables simplified network performance monitoring (NPM) and SecMon workflows for real-time and historical context. It delivers a one-stop visibility solution for on-premise data centers, enterprise campus/branch, and 4G/5G mobile networks.

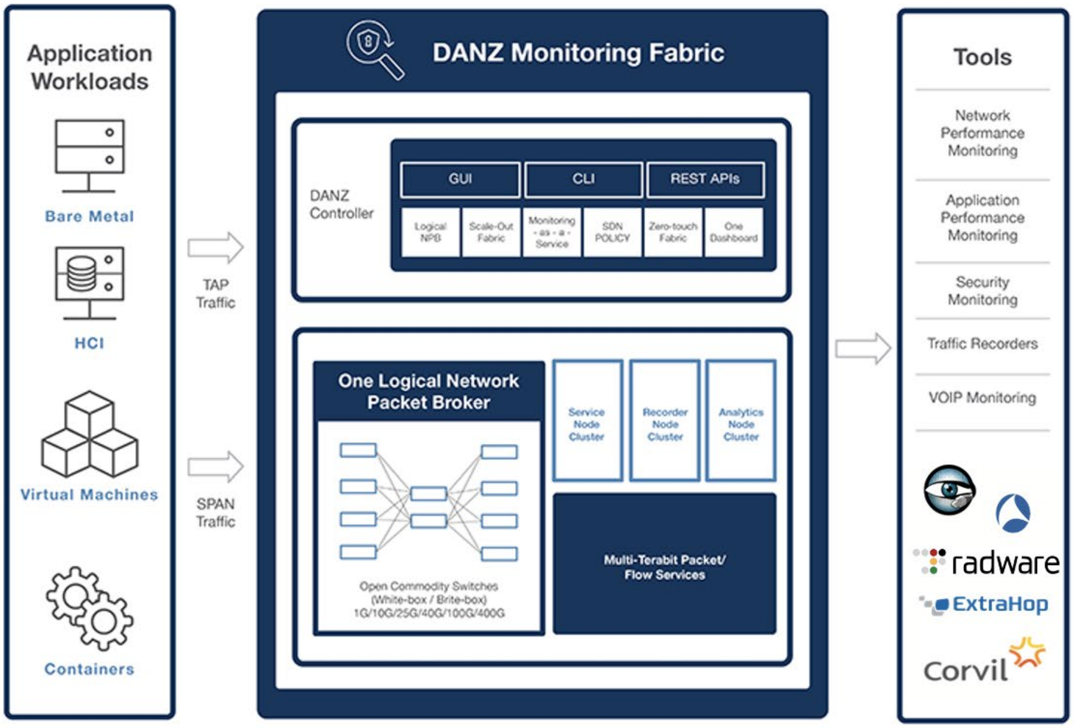

Figure 5: DANZ Monitoring Fabric – Logical Software-Defined NPB

Arista DMF is inspired by modern cloud-inspired networking designs and leverages cloud-first principles such as open merchant silicon and x86 processing nodes to architect a new class of software-defined Network Packet Broker (NPB). DMF provides a scale-out modular fabric design based on merchant silicon hardware, including third-party and Arista EOS-based networking platforms, with integrated analytics and packet recording intelligence for pervasive hybrid-cloud visibility.

DMF – A Complete Platform for Modular, Automated Insights

Unlike early NPBs, DMF empowers IT with the only complete solution for pervasive visibility and security across the enterprise by incorporating a centrally managed scale-out monitoring fabric with integrated replay and analysis capabilities, automation built with open programmable REST-APIs, and third-party tool integrations that allow network and security operations teams to perform hop-by-hop and network-wide troubleshooting and forensics.

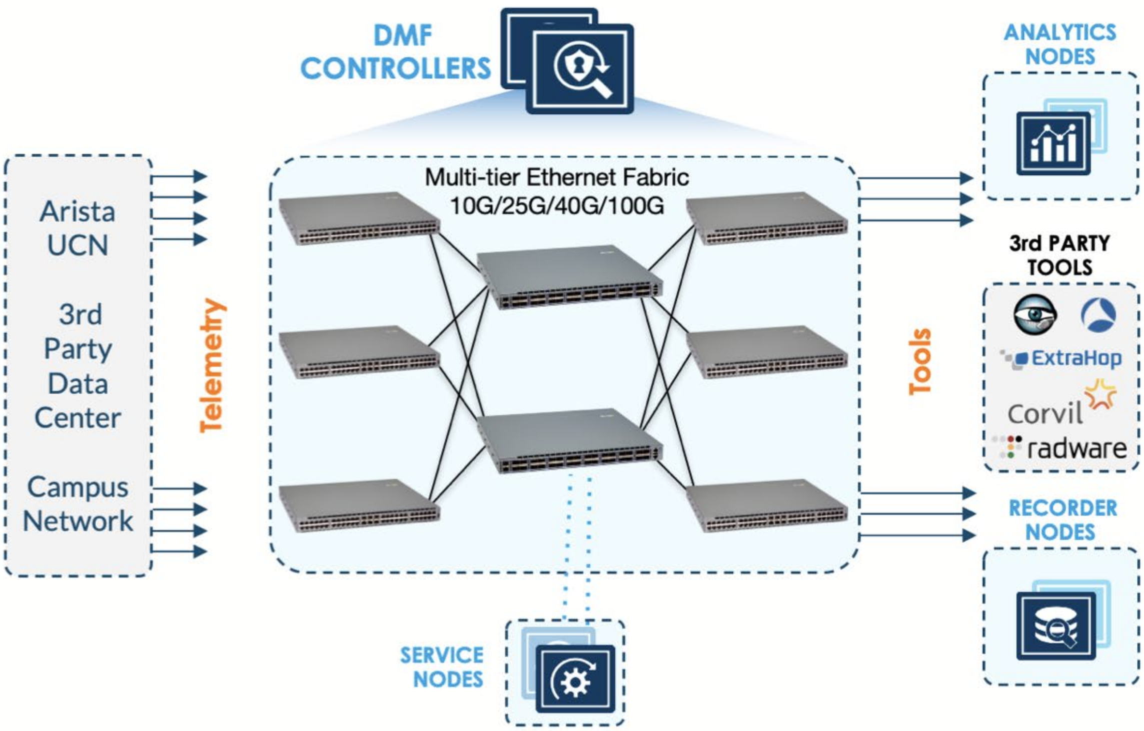

Figure 6: DANZ Monitoring Fabric Platform

At the core of the DMF platform is a multi-tier ethernet fabric that supports the auto-discovery of switches, service nodes, and analytic/recorder platforms with the ability to automatically bring-up every device on the monitoring network from bare-metal configurations. Centralized DMF controllers, with the capability of multi-tenant role definitions, provision the core fabric and provide provisioning of monitoring policies while correcting for any device or link-service errors to maintain 100% uptime of the monitoring fabric without operator intervention. Besides, device replacements and software upgrades are performed without service interruption as needed.

Device and application telemetry in the form of flow logs and packet data can be ingested by DMF for correlation and analysis, or generated by DMF for consumption by third-party tools if needed.

Unprecedented Ease-of-Use with Zero-Touch Automation

The DANZ Monitoring Fabric is a powerful platform that scales up to 1000's of ports of 1/10/25/40/100G monitoring with independent linear scale-out for fabric switches, service nodes, recorder nodes and analytics.

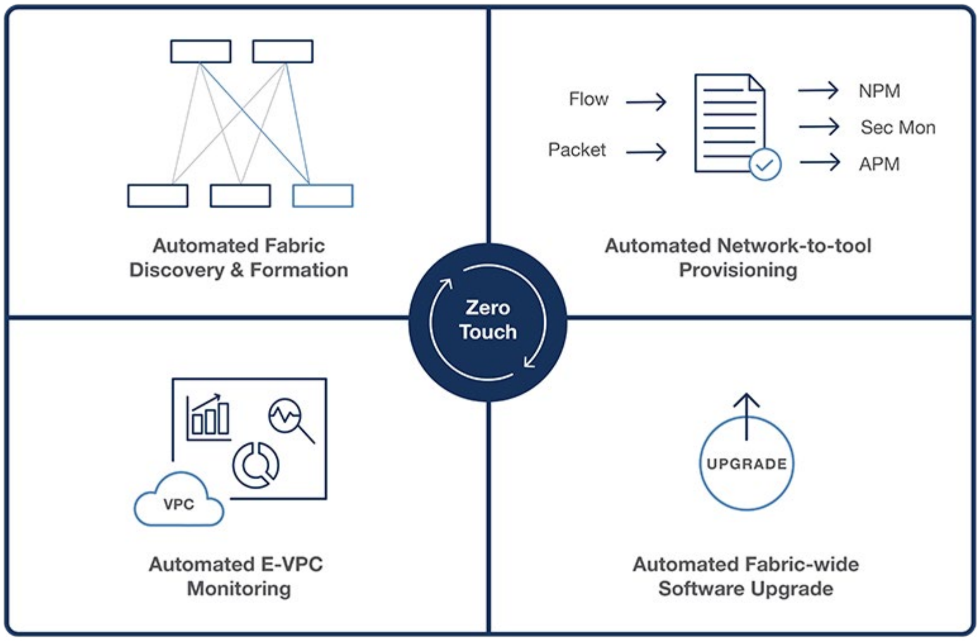

Figure 7: Zero Touch Fabric Operation

The fabric can be scaled up or down, upgraded, and enhanced with additional smart nodes, as needed, without interruption of service. Deployment is easy with automatic fabric discovery and formation, which also prevents configuration errors that could lead to visibility gaps. Finally, software is automatically updated with automated fabric-wide software upgrades managed by the centralized fabric controller.

Comprehensive Centralized Visibility Fabric Controller

The DMF controller serves as the single, central point of management for the shared monitoring infrastructure. The controller enables pervasive security and visibility for physical, virtual, and container workloads – for single, multi-site, and multi-cloud deployments.

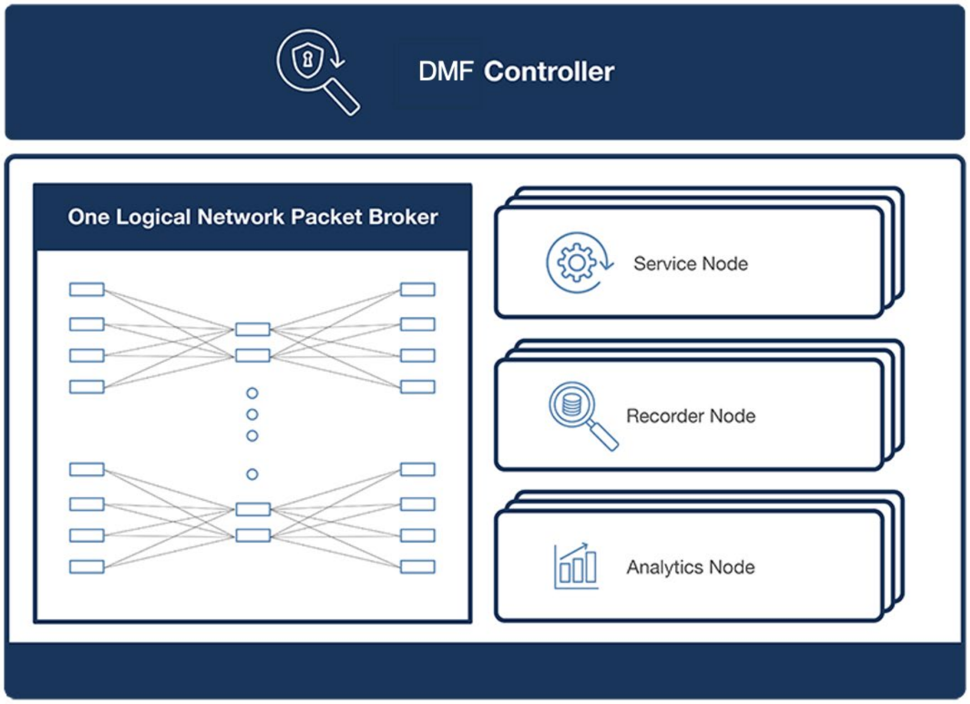

Figure 8: Scale-out Visibility and Security

Using the DMF Controller, customers can monitor the fabric, add switches and service nodes into the fabric, attach recorder and analytics nodes, create and configure interfaces, build monitoring policies, configure advanced services and monitor interfaces and traffic volumes. The DMF Controller provides a single pane-of-glass for managing all aspects of the DMF visibility and security fabric and its attached services.

Smart Service Nodes

When needed, advanced packet-processing functions–such as packet deduplication, packet slicing, packet masking, header stripping, flow generation, and deep packet inspection–are provided by separate x86 Service Nodes deployed as fabric attached scale-out components. By distributing these features onto separate fabric-attached compute platforms, the scale of the processing capability can be matched to the peak processing requirement of the monitored environment. The overall economy and fidelity of the entire monitoring solution can be tuned to achieve previously unachievable efficiency, economy, and performance.

Smart Recorder Nodes

The DMF Recorder Node performs full packet capture, query and replay. The Recorder Node has native on-board storage scaling to hundreds of terabytes, and uses a high-speed SSD for index data. Queries use the index SSD to find the packets of interest, and then the Recorder Node reaches into packet storage to retrieve the packets. Recorder Nodes can be added as scale-out components on the fabric–for greater storage capacity or to optimize storage locations. The DMF Controller will search all Recorder Nodes attached to the DMF fabric based on a query and return a single aggregated result. The Recorder Nodes also support off-appliance storage using NFS mount to Dell Isilon (both packet data and index data), where the Recorder Node provides the ingest, query and retrieval.

Smart Analytics Nodes

The DMF Analytics Node (AN) enables the visualization and analysis of network traffic flow data or telemetry captured in real-time or replayed from Recorder Nodes. Network administrators can use AN to discover traffic on the network, perform network troubleshooting and capacity planning. Security analysts can use AN for security incident response and security threat hunting, with the ability to query packets recorded at the optional DMF Recorder Node.

The Analytics Node and Recorder Nodes are managed from the DMF Controller. Analytics Node has its own Graphical User Interface (GUI) for dashboards, visualizations and analytics-specific policy configurations, such as Machine Learning Jobs or Watchers.

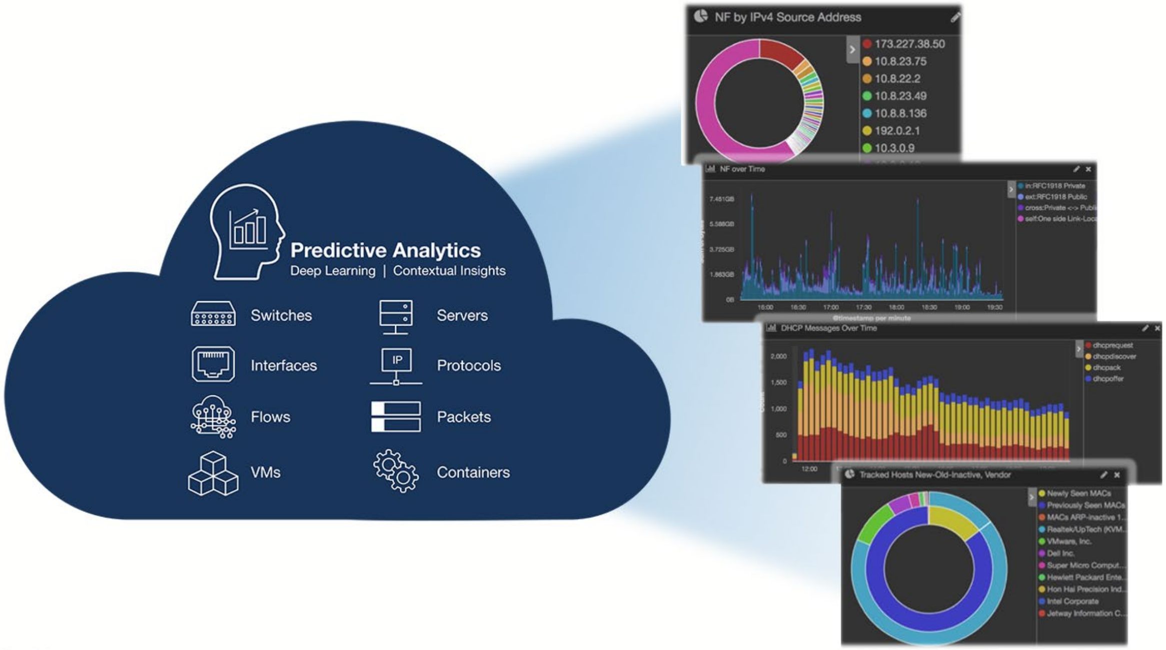

Figure 9: DMF Powerful Analytics Platform

DMF intelligent analytics and recorder capabilities empower NetOps/SecOps with simplified end-to-end discovery workflows driven by a single GUI dashboard. The modern, scale-out analytics architecture delivers plug-and-play extensibility for essential monitoring capacity and performance, assuring that the insights are complete, uncompromised, and trust-worthy.

Application-aware drill-down, with built-in machine learning and advanced statistical modeling, can pinpoint unexpected connectivity and performance issues caused by network contention or connectivity failures and can uncover previously invisible network hot-spots.

Integrated Network Time Machine

With the intelligent DMF Analytics and Recorder Node features, operators can quickly analyze and respond to complex application and security issues that otherwise would be difficult or impractical to discover. Combined, these features provide the ability to record, pin-point, and replay network traffic and telemetry data–including sFlow, Netflow (v5 and v9), IPFIX, TCP, DNS, DHCP, ARP, ICMP, and others–so that operators can achieve a comprehensive response capability for some of the most complex network challenges.

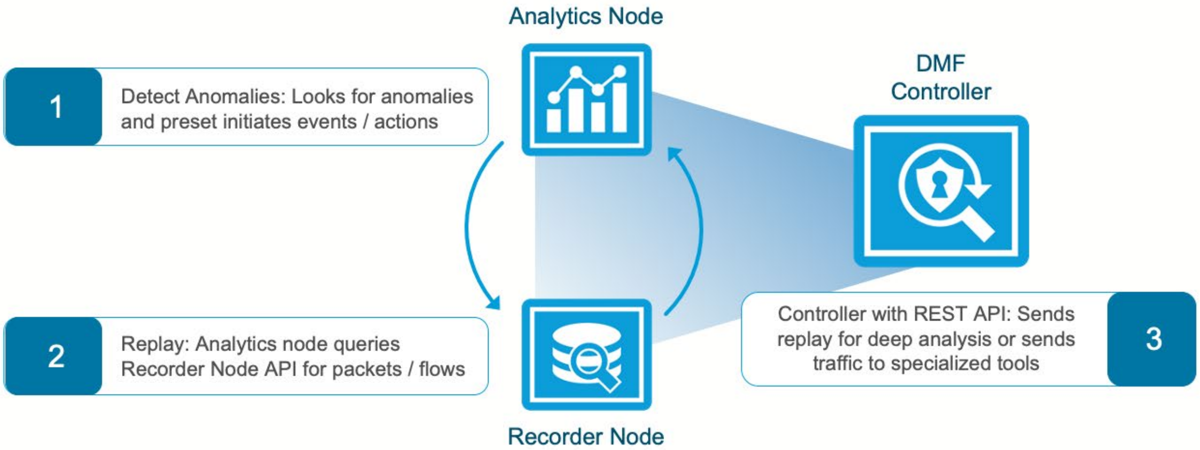

Figure 10: The DMF Network Time Machine

The integrated DMF Analytics and Recorder Node platforms provide unmatched real-time and historical analytics that can provide continuous contextual insights and application trends allowing the enterprise IT organization to meet business uptime needs with a reliable and secure infrastructure.

Spotting and Mitigating Network Anomalies with Machine Learning Analytics

The DMF Analytics Node supports Machine Learning with anomaly detection and automatic alerting. You can create jobs that baseline network flows over time and define watchers to detect traffic anomalies or deviations that trigger automatic alerts. The alerts can be sent via email, REST API or Slack integration.

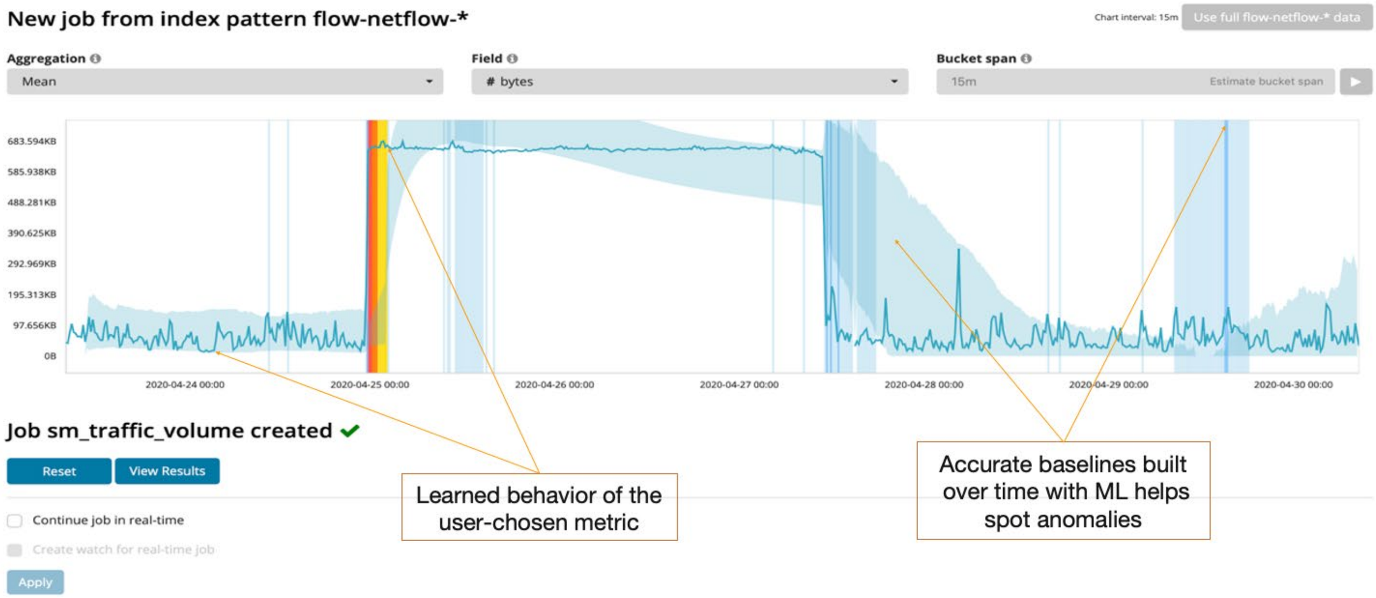

Figure 11: Machine Learning Detects and Pinpoints Anomalies

Use the Anomaly Explorer to visualize when traffic anomalies have been detected over time, and to drill down into the behavior that caused the anomalies. An example of the Anomaly Explorer view for a set of Machine Learning jobs is shown in the Figure 11.

With DMF analytics, you can create jobs that baseline network flows over time and define watchers to detect traffic anomalies or deviations that trigger automatic alerts. The alerts can be sent via email, REST API or Slack integration. Use the Anomaly Explorer to visualize when traffic anomalies have been detected over time, and to drill down into the behavior that caused the anomalies.

Detect Service Availability Problems with Application Dependency Mapping

Enhanced application troubleshooting agility is driven by integrated DMF Application Dependency Mapping (ADM) with historical data. Automation within this capability detects and alerts operators to developing service-availability problems within complex multi-tiered applications so that they can be proactively analyzed and averted regardless of how and where applications are deployed - monolithic apps, remote sites, virtualized, containers, and hybrid.

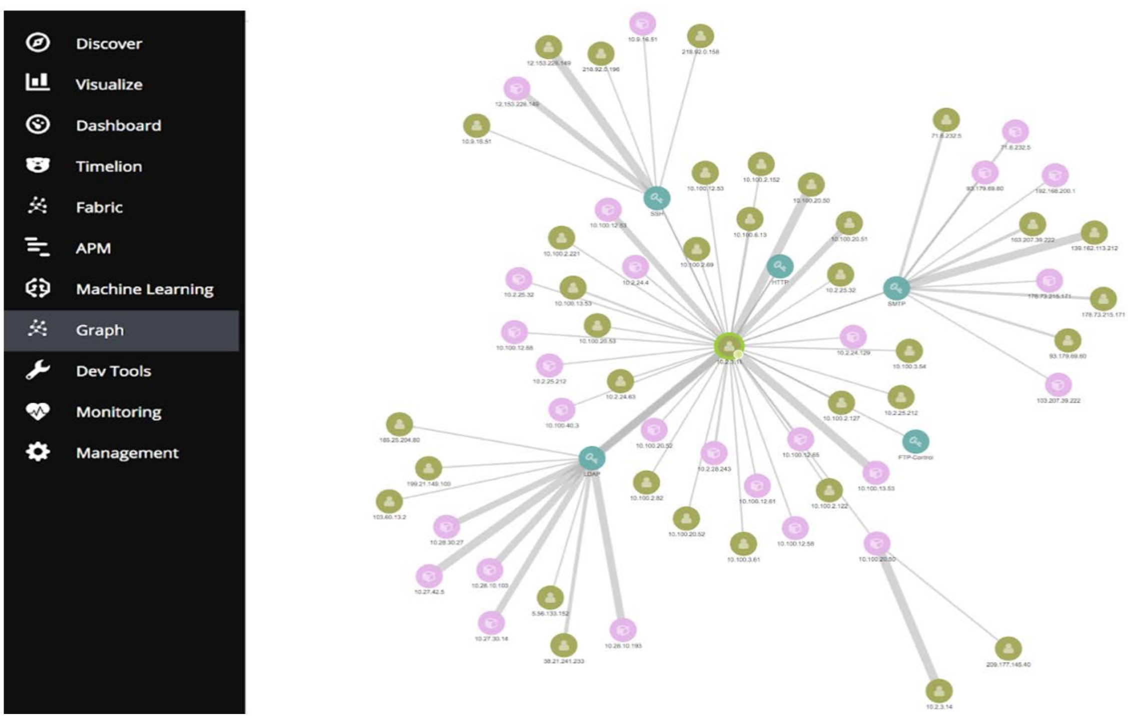

Figure 12: Impact Analysis with Application Dependency Mapping (ADM)

DMF Analytics Node provides a foundational toolbox to discover, visualize and optimize critical business service and application dependencies so that network operators can minimize adverse business impacts of service interruptions or downtime. The ADM feature also improves troubleshooting agility by visualizing application dependencies so that network and security engineers can locate service performance issues quickly. It also gives operations teams a role in proactive capacity planning by leveraging ADM with historical data to identify potential choke points.

Integration and Automation Built on REST APIs and Event-Driven Alerts

DMF analytics and recorder also provide richer and actionable insights by rapidly correlating real-time events with historical data in a single unified and programmable platform. The intelligent alert and notification engine provides real-time issue tracking and dramatically improves mean time to resolution while making it possible to automate deeper analysis through event-driven triggers and alerts.

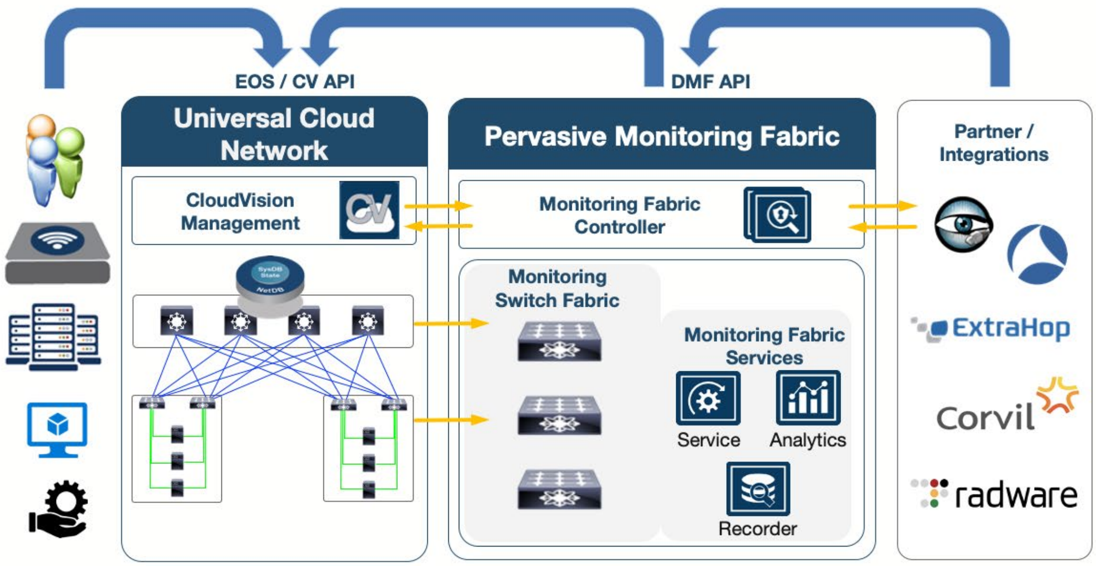

Figure 13: Automation with Real-time Events and REST APIs

Like all of DMF, the intelligent analytics and recording platform is built entirely on an open REST-first principle, providing both a CLI and GUI that are REST clients, and with all third-party and internal integrations based on a consistent API-driven approach. This provides individual SecOps and NetOps teams with the ability to quickly automate and filter monitored traffic and applications to adapt to changing workload and dynamic cyber-attacks in real-time. These unique capabilities have become fundamental in maintaining enterprise-wide service reliability, security, and availability.

Summary of Issues and new DMF Benefits

Unlike early "legacy" NPBs, DMF is designed to provide automated scale-out network visibility with the integrated deployment of switches, service nodes, analytics nodes, and recorder nodes using a centralized controller-based architecture.

Traditional "Early" Network Packet Brokers	DMF – First Logical Software-Defined NPB
• Legacy - Inflexible - Incomplete • Siloed, Box-by-box operations model creates visibility gaps • Scale-up, hardware-constrained designs are difficult to deploy and upgrade • Chassis refreshes extremely complex and require expensive forklift replacements • Dependent on 3rd-party tools for packet analysis and cannot automate operations and security workflows • Proprietary, leading to vendor lock-in	• Automated - Software Driven - Complete • Pervasive visibility architecture using a modular scale-out fabric design and industry standard x86 hardware • Zero-touch operation for seamless scaling and refresh brings up monitoring environment in minutes, not days • Advanced services modularity provides economical scale-out and investment protection • Integrated analytics and recorder features provides a complete turnkey solution for end-to-end visibility

Next-generation visibility and security with DMF offers architectural, operational, and business benefits for the business, for network and security architects, and operations – resolving the architectural and operational complexity of early "legacy" NPBs, erasing visibility and security silos and accelerating operations following essential cloud-principles.

For the business: Accelerate service and application delivery and improved availability with dramatically lower CAPEX and OPEX – DMF provides a next-generation, intelligent, agile, and flexible monitoring and security architecture that provide pervasive visibility, single-pane management, zero-touch scale, automation, and choice of open hardware.

For the network and security architect: Accommodate all tools (active and passive) and scale visibility and security as needed across the global network, regardless of expansion or changes to the network or tools.

For operations: Automate repetitive and error-prone tasks and programmatically integrate tool or team workflows to save resources, reduce time-to-service for new applications and remote sites, and enable faster response to performance and security issues.

Conclusion

In the past, network owners have had no unified solution for managing the delivery of observational visibility and security tools, whether inline or out-of-band. The only way to achieve visibility and optimization for costly tools was to deploy legacy NPBs or leverage TAP or SPAN ports at a very limited scale. However, the emergence of cloud networking and software-driven platforms like Arista DANZ Monitoring Fabric (DMF) has created a blueprint for the creation of next-generation architectures that scale and adapt for enterprise and service provider environments and radically simplify management.

The DANZ Monitoring Fabric is a software-driven network monitoring and observability solution that leverages best-in-class merchant silicon hardware to create a logical "super-NPB" and can deliver the benefits experienced by hyperscale companies to every organization—at any scale. Enterprises can now achieve the next-generation visibility and security needed to troubleshoot, maintain and defend everywhere, accelerate and sustain service delivery during their digital transformations, and optimize budgets.

DMF is, in essence, the first next-generation logical "super-NPB" fabric with leading price performance for the whole enterprise, including:

- Multi-tenant design with role-based access controls
- Ethernet and x86 economics for lower TCO build on cloud-principles
- Uniquely designed based on a software-driven architecture
- Zero-touch operation via intelligent controller and networking platforms

- Scale-out, universal fabric design for any size enterprise or service provider network
- Integrated analytics and recorder functions with a single-pane-of-glass GUI
- Fabric modularity simplifies change management and autonomic scale

At Arista, we understand the issues faced by modern enterprises that are engaged in their own digital transformations. Our mission is to deliver next-generation networking, operations, and monitoring solutions for any place in the cloud – data center, campus, WAN/edge, and private or public clouds – thus enabling our enterprise customers to realize the benefits of reliable and secure end-user productivity with a dramatically improved TCO. At the core of this mission is our unique software-driven approach to providing monitoring and visibility capabilities with a platform that addresses the needs of the modern enterprise.

To learn more about Arista DANZ Monitoring Fabric, please visit our website at https://www.arista.com/en/products/danz-monitoring-fabric.

To take a test-drive and learn how to use the DANZ Monitoring Fabric, please visit https://dmf-labs.arista.com and register with your work email.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062