Unlocking the Network with Enterprise SONiC Distribution by Dell Technologies with Augtera AI Network Pulse

Next-generation Network Operating System and AI Platform for End-to-End Network Visibility and Operations

Contents

Introduction

This document is intended for technical professionals who want to learn about the Enterprise SONiC Distribution by Dell Technologies, and Augtera AI Network Pulse. This white paper discusses the network operations challenges that are addressed by using Dell Enterprise SONiC and AI Network Pulse. The integrated solution covers key features and attributes, specific use cases, and business benefits.

What is SONiC?

SONiC is an open-source software project under Open Compute Project (OCP). SONiC was created by Microsoft and is running today in production on Azure, Microsoft's public cloud offering. A few years back, Microsoft decided to make it open, to contribute SONiC to the Open Community. Saying that a network operating system is up and running in production on over 40,000 Azure switches tells the world that SONiC is very stable, very robust, and is built for scalability. SONiC has all the necessary ingredients to make it the prime choice for Dell Technologies as an open-source network operating system.

Key features and attributes

- **Modular container-based architecture:** The architecture is based on containers, or modules, so it has modularity built in. The different core processes and base applications on SONiC are set up as containers that isolate each process. From a security and operational perspective, containers help scale processes without consuming a lot of resources on the switch. It also allows the processes to be created and brought down independently without affecting other services. Containers makes SONiC a highly scalable and secure NOS.

- **Open and standards-based API:** It provides extensibility through open APIs. We try to reduce the number of standards by using open APIs, so as not to reinvent the wheel if there is already something available. We prefer to take something that is available and provide interfaces. For example, the OpenConfig project by Google and Microsoft, provides a standard data model for networking. There is also gNMI, a northbound interface programmatic API from Google. We embrace open-source if there are open source components available. The data models for all applications on the switch and counters are based on open-config YANG models.

It also uses gRPC/gNMI-based telemetry which can be dialed out or dialed in. Enabling access to all the data from the switch makes it easy for AI Network Pulse to detect and visualize anomalies in real time.

- **Running custom applications on the switch:** Using unmodified Linux, SONiC allows you to install custom services, applications, and containers on the switch to meet custom requirements. This ability streamlines certain operational functions, and the applications on the switch can be maintained using the automation used to manage the switch. For example, AI Network Pulse can install a NetSonar probe service on the switch which enables real-time connectivity validation of the network using the AI Network Pulse software.
- **Using Open Source applications for core functions:** SONiC uses Free Range Routing (FRR), an open-source routing software, as its routing stack. SONiC encourages the community to contribute new features to the FRR software so that the NOS can be used to run a modern data center using open-source software.
- **Portability:** SONiC has a clear division between silicon and software. This clear separation—the abstraction among the ASICs, the platform, and the operating system—allows for faster development. When a feature is developed in SONiC, it uses the switch abstraction interface, so it is easier to port software to other silicon vendors. This provides differentiation for SONiC with respect to other offerings and an architectural advantage.

Enterprise SONiC Distribution by Dell Technologies

Enterprise SONiC Distribution by Dell Technologies (also known as Enterprise SONiC) is an enhancement of the SONiC community version. Enterprise SONiC is based on the open-source SONiC OS. Enterprise SONiC includes feature enhancements, hardening, and support targeted for the demanding data center leaf and spine fabrics while maintaining the open-source spirit.

Horizontally, Dell Technologies is adding more PowerSwitch platforms. Vertically, it is also adding more feature capability. Dell Technologies is seen as thought leaders in terms of the community, contributions, and representation.

Enterprise SONiC Distribution is a next-generation Network Operating System (NOS) that simplifies modern data center deployment and integration with the cloud. Dell Technologies has taken the open-source seed software and productized it for enterprise customers with end-to-end support.

Another value-add is the Dell Technologies ecosystem. Dell Technologies had the opportunity not just to look at SONiC as a stand-alone project, but also to look at how we can provide an ecosystem for life cycle management, and integration into other business units.

Dell Technologies SONiC Cloud and Enterprise options

SONiC provides users with two offerings. One is the Cloud offering that provides the functionality and containers that cloud-oriented customers need. The second is the Enterprise package that includes all containers for SONiC. For example, if your customer wants to have a VxLAN, run multicast or MLAG, then the Enterprise bundle would fit their needs.

Each bundle contains Premium content. Premium is for customers who want to have deeper analytics or support for a Linux precision time protocol. There is no difference in price between the Cloud and Enterprise bundles. This is simply a customer choice depending on whether they want to run everything, or a limited subset based on the use cases that they want to deploy. Since SONiC is an open-source project, this is sold based on a subscription. The subscription is based on three things:

- Time (one, three, or five years)
- Native port speed
- Tier type (Standard or Premium)

Customers can choose the best combination for their needs.

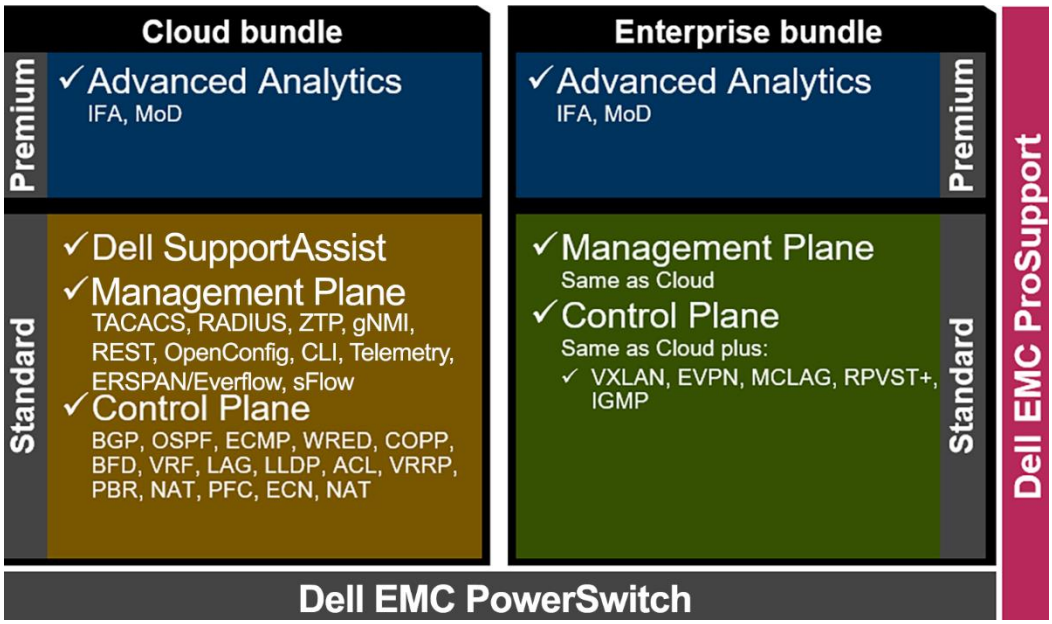

Figure 1. Standard and Premium bundles

Supported platforms

The Enterprise SONiC Distribution operating system supports the following system models:

- Dell EMC PowerSwitch N3248TE-ON
- Dell EMC PowerSwitch S5212F-ON
- Dell EMC PowerSwitch S5224F-ON
- Dell EMC PowerSwitch S5232F-ON
- Dell EMC PowerSwitch S5248F-ON
- Dell EMC PowerSwitch S5296F-ON
- Dell EMC PowerSwitch Z9264F-ON
- Dell EMC PowerSwitch Z9332F-ON
- Dell EMC PowerSwitch Z9432F-ON

Network Operations Challenges

As enterprise, cloud, and telco service providers continue to adopt software-defined networking (SDN), data center fabric designs, hybrid cloud, and white box switches, networks have become complex,

fragmented, and difficult to operate. As a result, network designers and operators are looking for ways to maximize business agility and network uptime, while minimizing capital and operational expenses.

With the evolution of networks over the last decade, the rapid network transformation has driven the need for lower costs, adoption of cloud services, and an increase in scalability.

- **High-speed networks at low cost:** As we enter a new decade, enterprise, cloud, and service providers are implementing 400-Gigabit Ethernet switches. The overall cost of building a network has plummeted over the last decade, with increased commoditization and more competition from NPU silicon vendors to traditional networking switch giants. However, there are still multiple NOS from traditional OEMs and open networking vendors that enforce some level of proprietary behavior while adding costs.

- **White box in every sense:** Switches and routers were traditionally black boxes. Cloud companies have led the effort to make networking ASICs more transparent while exposing data at granular levels to make troubleshooting easier. The vast amounts of data collected are being shared using standards-based streaming techniques like gRPC and gNMI using open config-based YANG models rather than relying on traditional methods like SNMP.

- **Simplified protocols and overlay networking:** Datacenter Networking protocols have been simplified to a standards-based, single control plane protocol for the data center fabric - primarily Layer 3 and BGP. Overlay networks are used for virtualization and other functionality on the switches, or by using centralized controller-based solutions. With a simplified protocol stack, the need to have a unifying, low cost, open-source NOS that provides ease of deployment and monitoring is required.

With these network transformations, new operational challenges have arisen. Combined with the amplification of the older challenges, traditional Network Monitoring Systems (NMS) are not able to handle these obstacles. Examples of these challenges include:

- **Multivendor and multi-technology environments:** With the evolution of network design, some parts of the network have become simplified. On the other hand, parts of the network have become more complex with the adoption of multilayer and multivendor technologies. For example, Data Center (DC) fabric is moving further towards a standardized BGP as the control plane protocol. However, the complexity has shifted to the overlay layer, which results in the increased adoption of diverse technologies such as EVPN/VXLAN, NSX, and SD-WAN.

- **Spine leaf networks and east-west traffic:** Virtualization and containerization have led to massive amounts of east-west traffic. New designs like leaf and spine fabrics have increased performance and resiliency, however, it has created issues such as ECMP polarization, and the ineffectiveness of traditional tools like traceroute.

- **Networks at scale means monitoring data at scale:** As large-scale networks are built, large amounts of data are being generated, which requires increased support for telemetry streaming. Existing monitoring systems are not capable of collecting all the data, therefore it is lost and not analyzed. The existing mechanisms of manual inspection of this data, coupled with threshold monitoring, pose some challenges which result in:

    - Network operators being more reactive than proactive in detecting failures

    - Increased time to root cause analysis

    - Increased mean time to innocence (MTTI) where the infrastructure group blames the network for any issues until proven otherwise

- Inability to isolate and measure the impact of failure or maintenance
- Exacerbation of traditional problems, such as gray failures
- Complexities in the tracking of changes in large networks, and the intent of the changes made by the operators
- The manual and time-consuming remediation of an issue

- **Tool sprawl:** NMS tool sprawl occurs when network operators across organizations attempt to reactively address complex issues using traditional monitoring technology. With the cost of network devices shifting to complex network management, monitoring systems are unable to keep up with operator requirements.

Augtera AI Network Pulse

Augtera AI Network Pulse is a multi-vendor and multi-technology solution that provides monitoring and anomaly detection of Enterprise SONiC Distribution networks in a greenfield or brownfield environment using standards-based configuration and monitoring techniques. AI Network Pulse uses machine learning on networking data and helps keep the focus on the business while minimizing expenses.

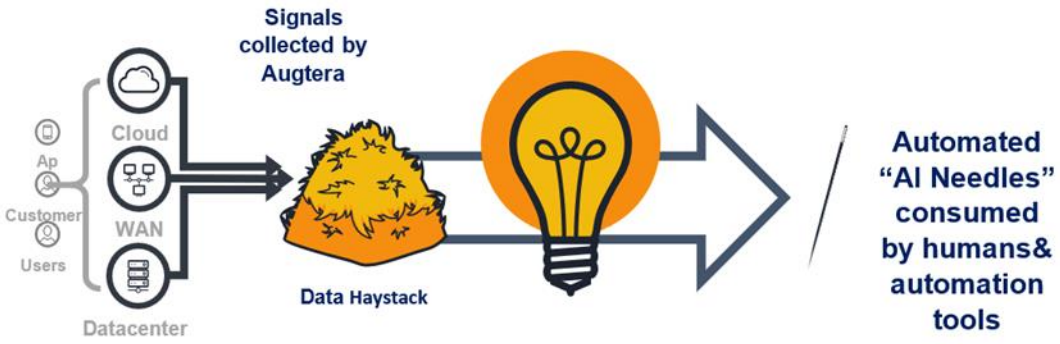

Figure 2. Augtera AI Network Pulse

To tackle the network operations challenges mentioned previously, Augtera Networks tapped into Artificial Intelligence (AI) and Machine Learning (ML). The effort to incorporate AI and network management resulted in the industry's first AI platform for networks called AI Network Pulse. AI Network Pulse provides a holistic solution in addressing network operations challenges.

AI Network Pulse brings the benefits of AI-augmented operations to physical, virtual, and cloud network environments. AI Network Pulse achieves the following outcomes:

1. Integration with Enterprise SONiC Distribution by Dell Technologies: As Datacenter networking moves towards Open Networking with the implementation of open-source NOS, Augtera works with Enterprise SONiC Distribution to make it easy to configure and manage SONiC using AI Network Pulse. Some key integrations include:
    - Integration with Enterprise SONiC Distribution telemetry models for comprehensive monitoring and AI-based anomaly detection
    - Integration and advanced classification of Enterprise SONiC Distribution syslog to generate alarms
    - Integration with Enterprise SONiC Everflow for on-demand flow analysis

- Integrations with Enterprise SONiC Mirror on Drop (MOD) for root cause analysis
- NetSonar integration for continuous and on-demand connectivity validation
- Integration with Enterprise SONiC sFlow for holistic flow analysis across the data center

2. Advanced Machine Learning applications: ML is suited to automatically recognize patterns from data with minimal human intervention. With network devices supporting telemetry streaming, large amounts of data are produced and collected however the backend systems are not able to analyze this amount of data. The collected data leaves operators searching for needles in a large data haystack. However, network infrastructure is a specialized and complex source of data that makes it hard to apply Machine Learning to this data while deriving operational value.

   AI Network Pulse incorporates proprietary algorithms developed with several years of research and development, that applies machine learning to the networking domain while leveraging Augtera's deep domain knowledge of networking technologies. These algorithms have matured using production data from several large-scale networks. AI applications, including anomaly detection and autocorrelation, leverage these algorithms that are custom built for networking constructs. AI applications powered by the AI Network Pulse platform, provide the data plumbing, network models, scale, visualization, ecosystem integration needed to bring the benefits of AI to complex and dynamic networking environments. As a result, AI Network Pulse can:

   - Pick out the hard to detect anomalies such as gray failures, in the large collection of data, which results in faster root cause analysis.
   - Predicting failures before they happen.
   - Faster remediation and event correlation
   - Real-time change verification in large-scale networks
   - Correlate network events across the multiple data center layers.

3. Comprehensive converged monitoring and automation solution: AI Network Pulse can visualize the topology, metric charts, tables, and graphs of the devices, logs, and events which enable AI Network Pulse to generate alerts and notifications, in the network. Thus, it can substitute the functions of a traditional NMS while providing the key differentiation of identifying highly complex correlated anomalies using AI/ML. AI/ML makes AI Network Pulse the "single pane of glass" for visibility of the entire network. Augtera pulls data not only from the network devices, but also from other tools in the environment, which helps in the consolidation of data, and prevents further tool sprawl. Some key converged monitoring capabilities which Augtera can provide are:

   - Fault and Performance Management
   - Topology Visualization
   - Flow Analytics
   - Impact Analysis

Key Figures and Attributes

The figure below depicts the primary components of the AI Network Pulse platform, and how these components interact with the network and Information Technology (IT) ecosystem.

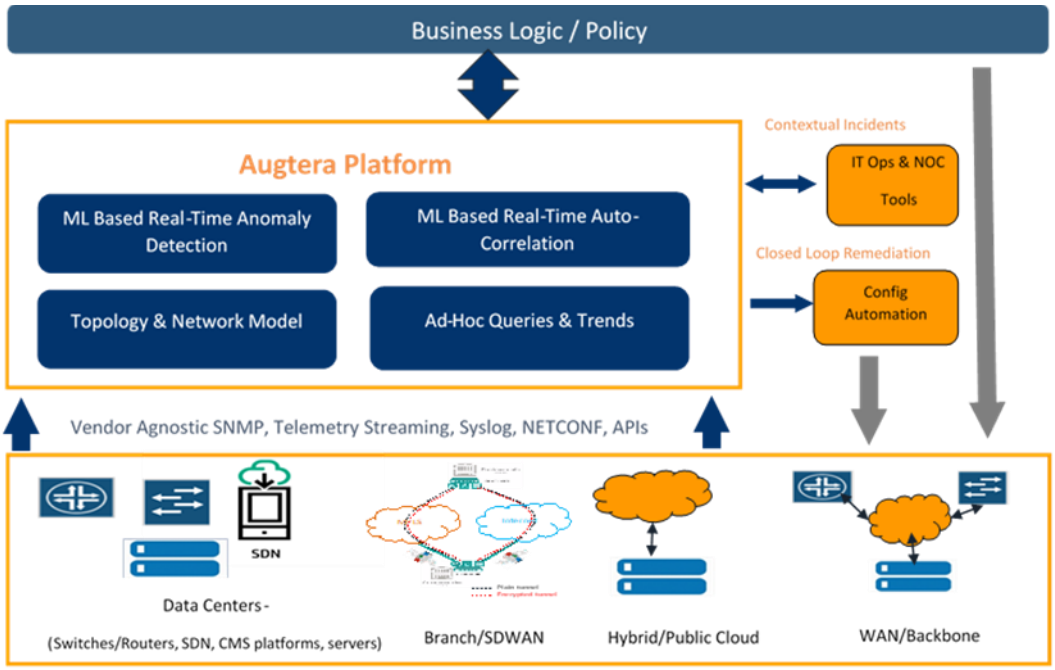

Figure 3. Primary components of the Augtera AI Network Pulse platform

Ingestion framework

AI Network Pulse has one of the most comprehensive data ingestion frameworks in the industry. This framework enables AI Network Pulse to build a comprehensive network model and gives an edge to its ML algorithms to leverage the richness of the network data. The ingestion of key differentiated technology attributes of the AI Network Pulse platform includes:

- Agentless platform: Does not need any agents on source devices
- Vendor agnostic: AI Network Pulse is completely vendor agnostic, which makes it ideal for multivendor environments
- Custom on-demand views: Operator defined customizable topology, anomaly, and trend views to consume and interpret AI-generated insights
- Heat map generation: Highlights hotspots and areas of significance
- Time machine capabilities: Build a cohesive story of anomalies across multiple days, months, or years
- Scalability: AI Network Pulse is highly scalable and can scale horizontally to support hyperscale networks. In one specific production deployment, AI Network Pulse is processing half a billion events in one day and providing real-time anomaly detection and correlation.

Business Benefits of Enterprise SONiC Distribution with AI Network Pulse

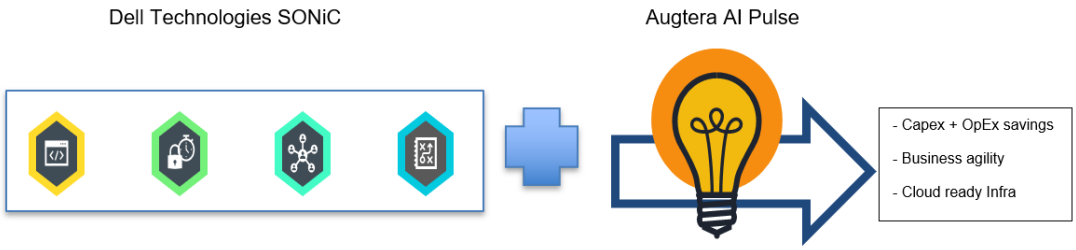

Figure 4. Scalability of Enterprise SONiC and AI Network Pulse

Enterprise SONiC Distribution by Dell Technologies with AI Network Pulse provides a highly scalable network that reduces the upfront capital costs of software, and the long-term operational costs of maintaining the network. The business benefits of Enterprise SONiC Distribution with AI Network Pulse are as follows:

- Enterprise SONiC Distribution streamlines the configuration and management of switches using standard protocol, configuration, and management models. Enterprise SONiC Distribution makes it easy for a business to integrate into a data center infrastructure, and a dev-ops based operational model that results in cost savings.
- The flexible licensing models that Dell Technologies provides allows customers to choose the roles, such as Enterprise or Cloud, that can operate with the standard version, and which roles in the data center need more advanced features for an additional cost. This license model results in capital savings with higher spend for software only in niche areas.
- The operational costs of doing critical security patches along with server Linux updates provides cost savings to a business.
- Enterprise-grade support from Dell reduces the risk for a business allowing it to move forward with this open-source model without any worry.

By taking advantage of ML and autocorrelation of large amounts of data, AI Network Pulse can provide business benefits to traditional network operations seen as an OPEX expense. Some key business-positive outcomes which an IT organization can expect to see are:

1. Reduction in OPEX costs tied to the work hours spent on troubleshooting network issues, and NMS tool configuration, and tuning.
    - High visibility for daily operations
    - 50%+ prevention of incidents
    - 90%+ reduction in detection time
    - 60%+ reduction in human spent for root cause analysis and resolution of incidents
2. An increase in business applications uptime.
    - Reduction in unplanned down time by providing maintenance visibility
    - AI/ML predicting future failures results in lower downtime
    - Custom views into every aspect of network infrastructure on the same dashboard with real-time notifications linked into business tools helps to keep the business running 24/7. Quick notifications result in a reduction in calls to NOC

3. Better business decisions regarding IT infrastructure spend.

    - Analyzing anomalies and trends from different equipment in the network using ML allows CIOs to compare the performance of the network, assess failure rates, and improve decisions for purchases.

    - Make informed decisions on business criticality, by leveraging data generated by Augtera, on where to spend more money, and where minimal spend can still give optimal business outcomes.

The following are examples of how AI Network Pulse can transform a traditional network operation, and increase business efficiencies:

1. Static Thresholds using traditional NMS compared to AI Network Pulse with no thresholds:

    - Human network operators spend hundreds of work hours configuring and tuning thresholds of various metrics in the network searching for anomalies when those thresholds are crossed.

    - Thresholds can result in many false positives. The constant adjusting of these thresholds results in hours spent unable to find operational issues as operators are lost in a deluge of data.

    - It is difficult for operators to understand the semantics of certain metrics like those from optics and hardware components and to come up with thresholds for these metrics. It becomes problematic for existing tools to predict when equipment is approaching failure.

    - With AI Network Pulse, ML removes the need for configuring thresholds of metrics which can be difficult to baseline and tune. ML learns changes in behavior and patterns pointing out true anomalies rather than relying on thresholds. AI Network Pulse can result in up to 10x work hour savings.

2. Manual correlation compared with Auto autocorrelation of network data and anomalies:

    - When critical issues such as packet drops occur in the network, network operators spend hours comparing data from hundreds of ports and across different roles in the network. Network operators perform data comparison evaluations to find where the issue that is causing the drops originated from, which affects business continuity.

    - It is difficult to get a holistically correlated figure of complicated issues, such as network congestion, even when using sophisticated NMS tools.

    - With AI Network Pulse, network operators can reduce the hundreds of work hours spent narrowing down complex issues, to sometimes less than an hour using autocorrelation, which results in business savings.

3. Syslog Classification to generate instrumental alarms for operations:

    - Enterprise SONiC Distribution uses syslog messages instead of SNMP traps to issue alarms from the system.

    - AI Network Pulse classifies Syslog messages using attributes of the message, such as the application, facility, severity, and the message text. AI Network Pulse also extracts and populates the relevant dimensions, such as categories to sort and mine data by, from the text and creates enriched syslog-based alarms.

- With AI Network Pulse, network operators can operate Enterprise SONiC with instrumental alarms derived from the syslog data source, and use machine learning to detect automatically abnormal rates.

4. With Enterprise SONiC Everflow and MOD integration, AI Network Pulse increases business efficiencies by:

    - Using AI to diagnose areas of the network needing analysis rather than a 24x7 collection of flows from all over the network that delays in finding the root cause.
    - Analyzing the flow from a particular area and providing results on the root cause.
    - Doing in minutes what once took hours or days, resulting in increased network uptime and high business critical application availability.

Conclusion

Augtera combined with Dell Technologies delivers AI-driven network anomaly detection to our customers. By deploying Enterprise SONiC Distribution with AI Network Pulse, operators can run a network that meets high availability levels while simplifying ongoing maintenance and troubleshooting their data center network.

To learn more about Augtera, see https://augtera.com/ or contact your Dell Sales representative.

For more information about Enterprise SONiC Distribution by Dell Technologies, see the Enterprise SONiC Distribution by Dell Technologies Spec Sheet.

Contact us

To learn more, contact your local representative or authorized reseller.

Author: Atanu Mandal (Dell Technologies)
Contributors: Jean-Marc Uze (Augtera) and Dennis Dadey (Dell Technologies).