Solution White Paper

Using the Power of Artificial Intelligence to Monitor Today’s Multi-Cloud Networks

How the network plays a vital role in digital transformation

Table of Contents

Executive Summary

Creating and managing digital transformation can be challenging and time-consuming. Today, IT organizations must move forward or risk not being agile enough to support the IT requirements of their business. The network plays a significant role in the modernization of IT, providing the foundation for enterprises to remain competitive.

This white paper explains:

- How the network has evolved to meet the demands of complex digital services
- Support your multi-cloud network with 5 technology imperatives for modern network management. This includes best practices for configuration, discovery, topology, and path analysis.
- The intersection of network data analytics and AIOps for proactive pattern identification via machine learning

THE CHANGING NETWORK

The Network Has Grown Complex

Enterprise networks have evolved radically in composition, behavior, and usage over the past couple of decades. It previously was located solely on-premises, and its configuration was static with few changes. Furthermore, it had low complexity, easily enforceable network access control, and significantly limited business impact.

Modern networks, in comparison, are highly dynamic with frequent manual and automated reconfigurations, and have IT assets both inside and outside of the enterprise. Many of these assets are virtual rather than physical in nature. Modern networks also expose a much wider range of network connectivity options, are highly complex with multiple network overlays, and are critical to successful minute-by-minute operation of the entire organization.

These changes in network complexity and composition have been driven by the increasing use of the network to provide business-critical IT services. With modern businesses relying on their IT services to remain competitive, providing these services is not possible without a secure, robust, and optimally performing network. With the advent of the digital enterprise, the network carries critical data and is the lifeblood of the business.

NETWORKS MUST SUPPORT MODERN INFRASTRUCTURE AND APPLICATIONS

Multi-Cloud Initiatives Make the Network More Critical Than Ever

Virtualization has become ubiquitous, spanning server virtualization (i.e., virtual machines), network function virtualization (i.e., virtual switches, routers, load-balancers, and firewalls), network topology virtualization (i.e., software-defined networking, software-defined WAN, MPLS, and VXLAN) and the adoption of cloud-based architectures (i.e., private, hybrid, public, and multi-cloud). Many enterprises are now actively embracing a “cloud-first” approach to workload deployment, with more workloads being migrated from physical, business-owned, or private cloud servers to the public cloud. Performance and availability of public cloud resources has become adequately proven. Furthermore, the agility, elasticity, and the ability to “right-size” cloud resources better suits the modern enterprise environment with its rapidly changing requirements linked directly to business initiatives.

With the relentless migration of internal and customer-facing services to the cloud, internet connectivity has become a business-critical network service. To provide high bandwidth and highly available internet access, many enterprises are deploying SD-WAN solutions (physical or virtual). SD-WAN also enables improved security with end-to-end line-speed encryption and cost reduction through bandwidth reduction, by using cheaper broadband links, data compression, and caching and performing traffic breakout to avoid internet backhaul costs and incurred latency.

Network Overlays for Security and Performance

In addition to transporting traditional application flows, the network is now responsible for supporting a wide range of applications for business operations, including unified communications and the exacting, dynamic demands unified communications places on the network, network storage, IoT, remote telemetry, and closed-circuit television (i.e., CCTV used in video surveillance). To achieve the diverse quality of service requirements for each traffic class (i.e., bandwidth, latency, reliability) and to enforce network level security, network overlays are widely deployed. Traffic is identified, categorized, and transported over the appropriate virtual overlay network, thus segmenting each traffic class and making its security and performance management more efficient.

Enterprise-wide wireless connectivity is expected to provide high quality, high bandwidth connectivity for corporate equipment, employees’ devices, and IoT devices. Associated with the plethora of device connectivity and the expanded attack surface is the need to provide appropriate access rights to users, stringent network security, network segmentation, and traffic monitoring to identifying malicious, naïve, and security vulnerabilities (and the exacting, dynamic demands unified communications places on the network).

THE NEXT GENERATION OF NETWORK MANAGEMENT

In parallel with the developments in network technologies, network monitoring and management tools have become proficient at providing insight into the network's behavior. These are the five capabilities that a modern network management solution must do to be able to support the ever-growing use of multi-cloud environments.

5 Technology Imperatives for Modern Network Management

1. **Reveal the configuration and performance of multi-cloud infrastructure (i.e., virtual switches, routers, load balancers, firewalls, cloud devices)**

   The depth of information that can be garnered from each platform depends on the types of objects being monitored and the amount of information available via the relevant API(s). For example, much greater breadth and depth of data is available from private clouds and privately-owned NFV than from public clouds and from NFV (network functions virtualization) provided within the public clouds. Network management solutions also need to provide integrations with multiple cloud providers' solutions to adequately support the growing use of multi-cloud.

2. **Discover and display network segmentation (i.e., overlays) using VLANs, VXLAN, SDN, MPLS, or any other technology.**

   Identification of devices and ports comprising each overlay is important for enabling assessment of security (e.g., PCI DSS), traffic prioritization, multi-tenancy, virtual network performance, etc.

3. **Configuration change detection**

   With the increased frequency of network device configuration changes, detection is an important feature that enables timely policy violation detection and the ability to correlate changes in configuration with changes in network performance and availability.

4. **Rapidly discover network topology**

   Given the dynamic nature of modern networks, especially in the context of SDN or with autonomously reconfiguring traditional networks, it is important that users can rapidly and accurately discover network topology (physical and virtual). This allows users to view the current network topology and ideally view a history of the topological changes, enabling historical correlation of topology changes with observed network behavior.

5. **Network path analysis**

   With the presence of business-critical and commercially sensitive data flowing over the network, the actual paths taken by the traffic becomes important. For instance, sensitive data should not be on the same network as IoT devices. This form of path analysis is difficult to achieve, although some vendors, such as Entuity, have novel techniques which illuminate traffic paths as well as highlight real-time deviations in paths to unexpected or insecure devices, or identifying bottlenecks. Whereas path analysis will expose the full path taken by specific traffic through the network, traditional flow analysis techniques, including NetFlow, sFlow, and JFlow, are useful in identifying which flows are passing through specific individual points in a network.

BREAKING DOWN TECHNOLOGY SILOS THROUGH ANALYTICS

The interdependence of networks, applications, servers, and security is leading to increased interaction between the various teams, and is driving the need for end-to-end support within the various toolsets or shared use of common tools. Meaningful integrations and analytic insight is needed to support this cross-functional need for a holistic view of the network.

Simple Network Management Protocol (SNMP) Monitoring Isn't Enough Anymore

With traditional networking technologies and equipment, SNMP was universally used to build a complete picture of network inventory, topology, and performance. With the adoption of newer networking devices and non-networking devices (e.g., servers, hypervisors, IoT devices), SNMP is often insufficient or unavailable. Consequently, NMS (network management systems) vendors must rapidly integrate with a growing range of disparate APIs, implemented using a range of different technologies. This additional complexity can easily lead to a lack of visibility where an NMS has not kept pace with the network equipment deployment or a stifling of network development as new network deployments are delayed waiting for device support by the NMS.

When SNMP monitoring increases in network complexity, scale (i.e., increased number of network presences) and breadth of technologies, the amount of data being gathered and stored by NMS continues to increase significantly. **When viewed at an enterprise scale, the quantity of data becomes too large for humans to interpret. Network management solutions must be able to undertake intelligent processing**. For example, this could be consolidating a large number of "raw" events into a small number of ongoing incidents which users can effectively address.

The Software-Defined Network

The software-defined network is gaining traction. It is the optimal technique for provisioning networks in response to frequent changes in network requirements and workload locations, driven by the flexibility of multi-cloud infrastructure and modern application architectures. The software-defined network approach helps IT control and visualize network performance and changes in resource availability. Furthermore, the ability to dynamically segregate multiple, distinct overlay networks provides a valuable underpinning for organizations practicing DevOps.

Bringing Order with Network Data Analytics and Artificial Intelligence for IT Operations

This new level of complexity has led to the appearance and growth of network data analytics (NDA) and artificial intelligence for IT operations (AIOps), whereby high velocity and high volume data feeds containing detailed network performance data are processed to identify higher level insights into network behavior necessary for proactively managing the network.

One key technique used in network data analytics is machine learning, a key tenant of AIOps. Key metrics are monitored and analyzed, and characteristic patterns are identified. In conjunction with automatic event correlation and symptomatic event suppression, this significantly reduces the amount of "noise" produced by the network management solution and generates valuable, actionable information.

To optimally manage the network from the business perspective and, in particular, to prioritize network remediation, it is necessary even with ITOA's (IT operations analytics) automatic interpretation of data and event reduction to supplement the network information with business specifics that allow the network data to be presented in a business context and related to specific business units and initiatives. It should be noted that **the network management solution cannot automatically discover which servers and network devices are key to the business**. Therefore, the construction of business service models which can be used to contextualize, enrich, and prioritize the information presented to the user are necessary.

AIOps is invaluable for bringing greater understanding to the past, present, and future of infrastructure and application health. Analytics such as setting dynamic thresholds through machine learning, performing root cause analysis, and service impact analysis, is all in the context of what is happening now or what happened in the past. Predictive analytics tells you about the expected future state, through the correlation and extrapolation of data, the application of statistical models and artificial intelligence, and interpretation of the projections to predict what might happen in the future.

For example, a pattern may be recognized whereby a specific set of circumstances routinely precedes an undesirable event. Once this has been identified, similar circumstances beginning to manifest elsewhere in the network can be identified with an alert-generated warning of a similar undesirable outcome likely to occur in the future. Related to predictive analytics is the ability to perform "what-if" analysis. By artificially changing the input to the prediction algorithms, one can observe the effects on the predicted outcomes. For example, "What happens to my network traffic and application performance if I migrate a VM from one hypervisor to another?"

By combining predictive analytics with automated system reconfiguration, AIOps enables autonomous responses to predictions of the future by reconfiguring network components to avoid undesirable predicted outcomes from occurring. With AIOps, the aim is to increase MTBF (mean time between failures) as well as to reduce MTTR (mean time to repair). Again, this needs to be undertaken in the context of business significance. Thus, if only a competing subset of situations can be remediated, the most business-critical services must take priority.

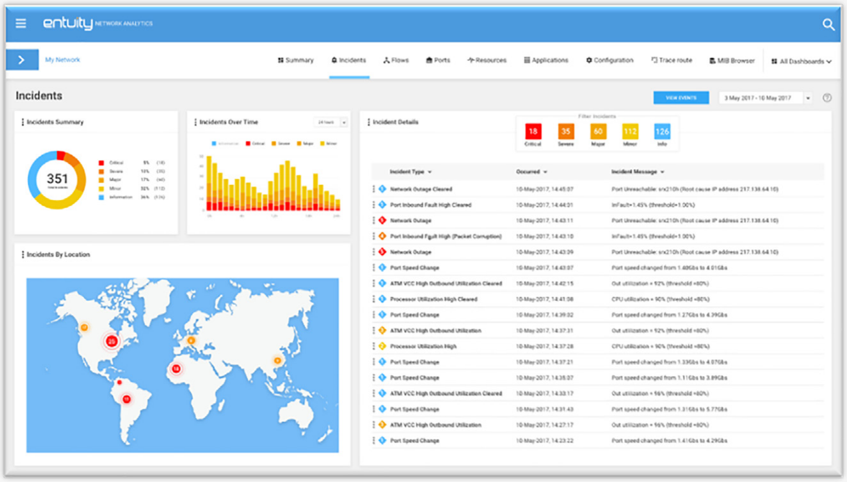
CHOOSING THE RIGHT NETWORK MANAGEMENT SOLUTION

As networks have matured, they have become significantly more complex and dynamic in nature, as have network management solutions. These solutions span an increasing range of technologies and given the rapid adoption of new technologies, **NMS vendors should be assessed on their ability to swiftly and proactively include support for new technologies, provide timely device support, and rapidly accommodate customers changing requirements.**

Entuity Network Analytics for TrueSight delivers network visibility and key analytics to support evolving digital environments.

For enterprise network management, there continues to be a need to employ disparate tools to manage the network, servers, applications, storage, security, wireless, and other areas. Network management solutions should offer standards-based, well-documented, and open APIs to facilitate data mining and automated network management solution configuration, and allow for the creation of custom integrations to share data. It should also offer deep, meaningful, out-of-the-box integrations with other relevant management applications. With the increased dynamics of modern networks, network management solutions must be able to rapidly monitor changes in physical and virtual inventory, configuration, topology, application flows, and performance.

With the enormous quantities of data gathered about the network, application flows, and server performance, network data analytics is becoming increasingly important in providing high value, actionable information rather than simply informing users of every event occurring in the network, regardless of severity or business context. Yet, however sophisticated the network analytics algorithms and machine learning are, the results will be unreliable if the underlying raw data is not accurate, comprehensive, normalized, and timely. **A robust, accurate data feed is paramount**.



Incident Type	Occurred	Incident Message
Network Outage Cleared	10-May-2017, 14:45:07	Port Unreachable: srx210h (Root cause IP address 217.138.64.10)
Port Inbound Fault High Cleared	10-May-2017, 14:44:01	InFault=1.45% (threshold=1.00%)
Network Outage	10-May-2017, 14:43:11	Port Unreachable: srx210h (Root cause IP address 217.138.64.10)
Port Inbound Fault High (Packet Corruption)	10-May-2017, 14:43:10	InFault=1.45% (threshold=1.00%)
Network Outage	10-May-2017, 14:43:09	Port Unreachable: srx210h (Root cause IP address 217.138.64.10)
Port Speed Change	10-May-2017, 14:43:07	Port speed changed from 1.40Gbs to 4.01Gbs
ATM VCC High Outbound Utilization Cleared	10-May-2017, 14:42:15	Out utilization = 92% (threshold =80%)
Processor Utilization High Cleared	10-May-2017, 14:41:08	CPU utilization = 90% (threshold =80%)
Port Speed Change	10-May-2017, 14:39:02	Port speed changed from 1.27Gbs to 4.39Gbs
ATM VCC High Outbound Utilization	10-May-2017, 14:37:31	Out utilization = 92% (threshold =80%)
Processor Utilization High	10-May-2017, 14:37:28	CPU utilization = 90% (threshold =80%)
Port Speed Change	10-May-2017, 14:37:21	Port speed changed from 1.33Gbs to 4.07Gbs
Port Speed Change	10-May-2017, 14:35:07	Port speed changed from 1.11Gbs to 3.89Gbs
ATM VCC High Outbound Utilization Cleared	10-May-2017, 14:33:17	Out utilization = 96% (threshold =80%)
Port Speed Change	10-May-2017, 14:31:43	Port speed changed from 1.31Gbs to 5.77Gbs
ATM VCC High Outbound Utilization	10-May-2017, 14:27:17	Out utilization = 96% (threshold =80%)
Port Speed Change	10-May-2017, 14:23:22	Port speed changed from 1.41Gbs to 4.29Gbs

The Incidents Dashboard can be easily customized to monitor what matters to an IT team.

CONCLUSION

TrueSight for network performance management brings in data from Entuity Network Analytics to provide users with a seamless view of their entire IT estate, including detailed network performance and network analytics. This data can then be used alongside additional feeds from APM (application performance management) solutions and security and wireless management tools to produce even more insightful, fully integrated views of network activity, paths, and relationships that drive appropriate decisions and actions.

With the advent of mobile connectivity, big data, predictive analytics, cloud-based architectures, IoT, and unified communications, the network is now enabling digital transformation. TrueSight supports these technologies to make digital transformation a success.

FOR MORE INFORMATION

To learn more about Entuity for TrueSight Operations Management, visit **here**.