Case Study

Fortune 500 Enterprise Transforms Data Center Network Operations

Architecture change has been disruptive to data center network operations. Data Centers are the core of the public, private, and hybrid cloud disruption. Underlays, overlays, SD-WAN, fixed form factor switches, dense topologies, an explosion of interfaces, and more. Nowhere is the urgency for network operations transformation greater than in the data center.

Network Operations teams must reduce the workload. The ability to add people is not infinite, yet the ability for noisy tools and processes to create incidents is. Or at least, can grow much faster than the number of people that can be added. When this happens, a fundamental shift is required to reduce the workload, so constrained resources can be effective.

For multiple years Augtera Networks has been refining its Data Center solution with multiple customers. An important customer along that journey was an innovative Fortune 500 enterprise who realized they could no longer operate in a reactive mode. To achieve desired customer and application team outcomes, they had to prevent incidents before they occurred – they had to lower the total number of incidents.

The main challenge they faced was focusing their skilled employees on operationally relevant incidents. Like everyone else, they were drowning in a sea of noise, trying to work faster to keep up. However, there comes a point when working faster does not make progress. At that point, incident workload must be reduced.

Augtera

The First Network AI
for the Modern Enterprise

A platform that eats incidents for breakfast.

The Augtera Platform

- **Automate or go home**

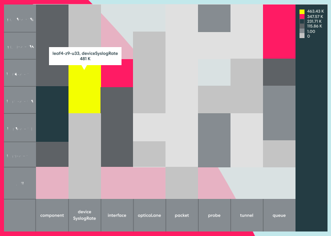
  With the decision to automate network operations made, the customer engaged Augtera Networks to implement our next generation Network AIOps platform.

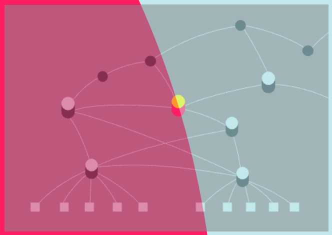
- **Results**

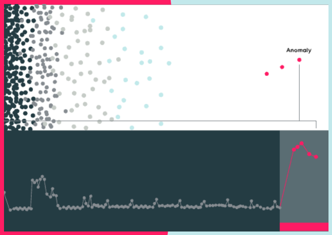
  The daily outstanding trouble tickets reduced from thousands to hundreds – an order of magnitude improvement in the ineffective approach to coping by running faster.

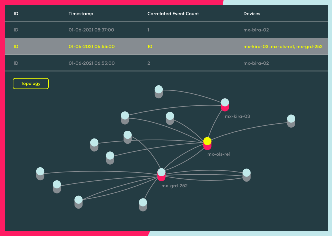
  Customer and application team experiences improved significantly. MTTD declined by over 90%, MTTM by over 50%, and mean time to repair by over 40%.

  Noise was eliminated, the network operations team was able to focus on what was operationally relevant, and network experiences improved significantly.

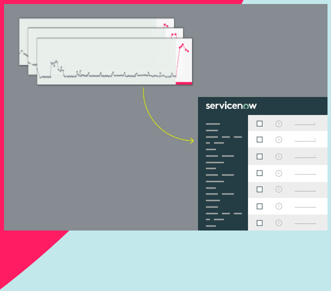








ID	Timestamp	Correlated Event Count	Devices
ID	01-06-2021 08:37:00	1	mx-bira-02
ID	01-06-2021 06:55:00	10	mx-kira-03, mx-ols-re1, mx-grd-252
ID	01-06-2021 06:55:00	2	mx-bira-02



Problem Statement

The amount of noise generated by existing tools created alert fatigue which manifested as slow mean time to detection, action, mitigation, and remediation. For example, mean time to action was over 40 minutes and mean time to mitigation over sixty minutes. The customer experience was being impacted because the operations team could not respond fast enough.

Company Profile

A Fortune 500 brand with multi-billion USD cash flow. A leading brand in its segment, IT, and specifically Networking is core to its business.

Discussion

The customer network comprises multiple data centers with a modern, dense-topology, L3 BGP Clos architecture with many thousands of switches and a very large number of interfaces. The equipment vendors for switches and routers include Arista Networks, Cisco Systems, Juniper Networks, and Dell Enterprise SONiC on Whitebox. MPLS is used for data center interconnects (DCI).

The Augtera platform was deployed on-premise. Augtera also supports hybrid deployments and recommends the SaaS deployment for most customers.

Ingest and Store Data

The customer required that Augtera perform SNMP polling for metrics and topology, in addition to receiving SNMP traps. While Augtera supports newer interfaces such as gRPC / gNMI, it is still the case that SNMP is sometimes the most mature and widely deployed approach in a network. While many approaches to SNMP data collection have suffered from scaling, and other issues, Augtera’s comprehensive implementation handled the scale of this Fortune 500 Enterprise with ease and efficiency.

Another data ingestion requirement was syslog, which Augtera handled at scale, processing hundreds of millions of messages per hour. Augtera supports classifiers to catch known anomaly signatures, rate of change detection, and rarely seen messages through the Zero Day Anomaly feature. New/rare syslog messages are often the precursors of future failures.

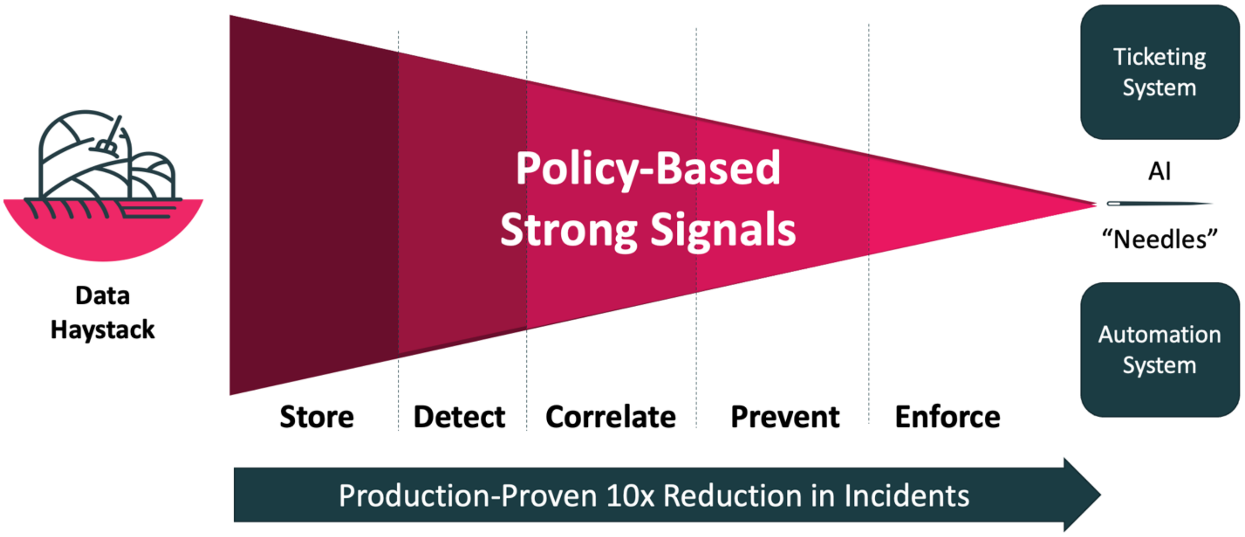


Figure 1. Augtera's comprehensive approach to noise reduction

Anomaly detection occurs at many points in the pipeline and through multiple approaches:

- Classifiers
- Machine Learning (ML) models
- Rate-based Anomalies
- Zero Day Anomalies
- Gray failures

The customer in this case study made use of all the above, except for Zero Day Anomalies, which was released after deployment.

Classifiers look for specific anomaly symptoms / signatures. When there is a match the network operations team is notified. Classifier notifications are high-fidelity because they have been learned by the Augtera platform across the customer base. Classifiers are disseminated to all deployments.

Machine learning models use network-specialized algorithms to detect anomalies relative to known networking patterns. Models eliminate the false positive noise created by thresholds, and false negatives – anomalies that should be alarmed but are not.

Rate-based anomalies detect changes in the rate of specific data. For example, rate-based anomalies may detect that a specific syslog message is occurring much more frequently than usual, indicating something has changed, and a likely new anomaly.

The Augtera platform can detect that degradation is occurring, even though an actual failure has not. Network operators are notified of gray failures, so they can be proactively addressed.

For more information on classifiers, rate-based and zero-day anomalies, read Real-Time Syslog.

Correlate

Topology-based auto-correlation makes a significant contribution to both noise reduction and the identification of an incident root.

The customer in this case study would regularly get 100+ alarms when a switch failed. In addition, they had an outstanding queue of thousands of trouble tickets. By using Augtera's auto-correlation, the customer was able to reduce 100+ alarms for a switch failure to just one (zero if it was a maintenance event) and reduced outstanding trouble tickets to hundreds of parent tickets, with related child tickets for documentation.

Augtera's real-time, multilayer topology-aware auto-correlation utilizes a comprehensive network model to analyze both relationships and network object hierarchy, to determine the network object at the root of an incident. With the incident root identified, network operators can initiate mitigation and repair workflows. The Augtera customer reduced mean time to mitigation (MTTM) by over 50% and mean time to repair (MTTR) by over 40%.

Prevent

Many times, anomalies may be detected by software, but they roll off a screen so fast, they are never noticed and never acted on. Action is critical. The customer reduced MTTD & Action by well over 90%. Anomalies are now addressed much faster, with the aim of mitigating anomalies before customers or application teams raise a trouble ticket for a failure.

Another aspect of prevention is acting proactively so an incident never occurs. The Augtera platform's ability to detect gray failures and other emerging trends empowers customers to prevent incidents before they occur.

Combined, operations teams remain ahead of customers and application teams, either preventing incidents before they occur, or mitigating incidents before they are noticed.

Policy Enforcement

The Augtera platform allows customers to define policies, which the platform enforces. Policies define what analysis should be performed, and what notifications should be done.

Augtera Spaces are a way for Augtera customers to define what object types correlations should be executed for. This reduces resource usage by the Augtera platform, as well as narrowing analysis to what the customer defines as being operationally relevant. Spaces reduce noise.

Augtera Views, on the other hand, define what types of objects the operator should be notified about. Views work for console alerts, the Augtera UI, ticket generation, and automation systems. Augtera Views are a powerful way to construct visualizations, in addition to defining what is notified. Train once, apply many places. Views reduce noise.

Maintenance Suppression

Alerts and tickets generated by maintenance events are a significant challenge for operations teams. Firstly, they do not need to be acted on because they are known, pre-determined outages. Secondly, they train operations teams to ignore large alert bursts, assuming they are maintenance events.

Learning lifecycle state has not traditionally been performed by NetOps tools. There are numerous ways the Augtera platform can do this. An emerging approach is for customers to push the information via an Augtera-supplied API. Meta-data for devices AND interfaces is updated in real-time and used to trigger or suppress notifications. For example, on a single device, notifications for some interfaces in maintenance can be suppressed, while others on the same device can be triggered.

Trouble-Ticket Creation

Creating trouble tickets is not difficult. It involves calling the API of a platform like ServiceNow, which the customer uses. The difficulty is eliminating all the noise and ensuring that trouble tickets are ONLY created for operationally relevant anomalies.

Augtera has passed the trust barrier because the platform:

- Uses ML models that are less noisy than thresholds.
- Does high-fidelity detection through classifiers, based on known anomaly “signatures”.
- Discovers gray failures so proactive action can be taken to prevent a future incident.
- Dramatically reduces the number of notifications through auto-correlation.
- Identifies the incident root for rapid mitigation, through automated multilayer topology-aware auto-correlation.
- Enables customers to define what they believe is operationally relevant through Augtera Spaces and Views.
- Suppresses maintenance alarms.
- Suppresses duplicate incident notification.

Hi-fidelity ticket creation requires more than just calling an API. It requires an end-to-end, comprehensive approach.

Conclusion

By implementing the Augtera Network AI platform, this Fortune 500 Enterprise has reduced MTTD by 90%+, MTTM by 50%+, MTTR by 40%+, and increased the time between incidents by a factor of 4. This is only achievable by transforming operations from being manual, reactive, and noisy to automated, proactive, and relevant.

Contact: https://www.augtera.com/contact-us/

Investors

BainCapital VENTURES

DELL Technologies CAPITAL

intel capital

Acrew