



# DX Operational Intelligence 21.3.1

## What's New



# Shifting from Monitoring to Observability

## Monitoring

Collection of Data

Individual Component Status

Keep The Lights On

## Observability

Connections in Data

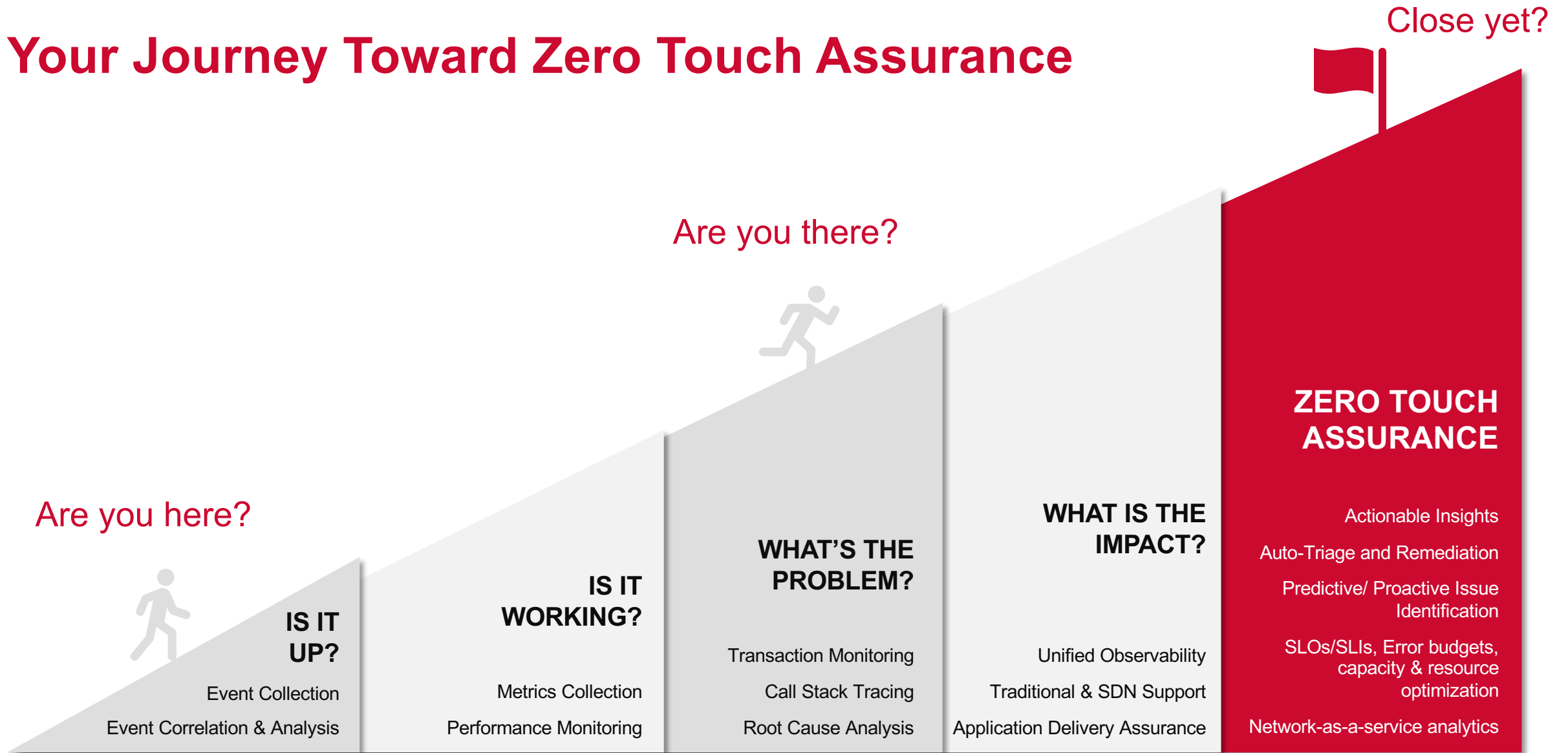
End-to-End Digital Service Health

Prioritizing Against Business Impact

“ How do I monitor the **health and performance** of infrastructure and applications in a way that meaningfully considers **user experience** and other critical **business objectives**?”

Gartner, *Solution Path for Modern Infrastructure and Application Monitoring*, 30 November 2020, Gregg Siegfried and Venkat Rayapudi, ID: G00720254

# Your Journey Toward Zero Touch Assurance



# The AIOps Platform from Broadcom

## Digital Experience Monitoring

Glassbox	dynatrace
BROADCOM	catchpoint

## Application Monitoring

BROADCOM	New Relic
dynatrace	APPDYNAMICS

## Infrastructure Monitoring

BROADCOM	splunk
DATADOG	Microsoft System Center Operations Manager

## Network Monitoring

solarwinds	splunk
BROADCOM	NETSCOUT

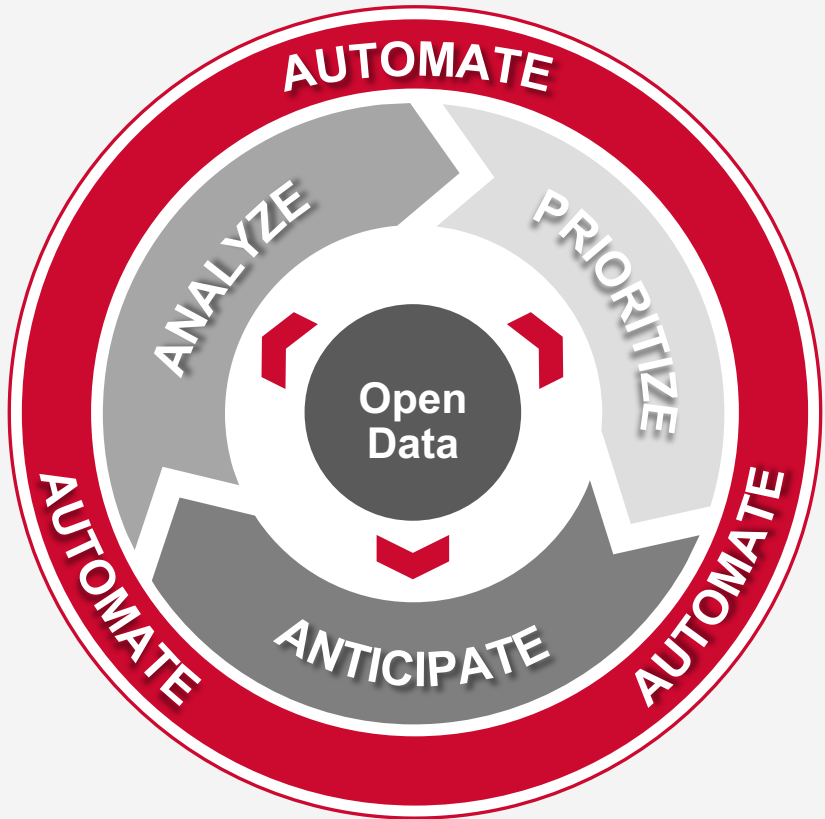
## Mainframe Monitoring

BROADCOM
----------

+ Other 3rd party tools

(Machine Data: Metrics, Alarms, Topology, Logs, Text & Wire Data)

## DX Operational Intelligence



Open | Extensible | Hybrid

Root Cause Analysis
Unified Visibility
Collaboration and Planning



Remediation  
Workflows

ITSM



# DX Operational Intelligence

## Smarter IT Operations Through Actionable Insight

### Root Cause Analysis

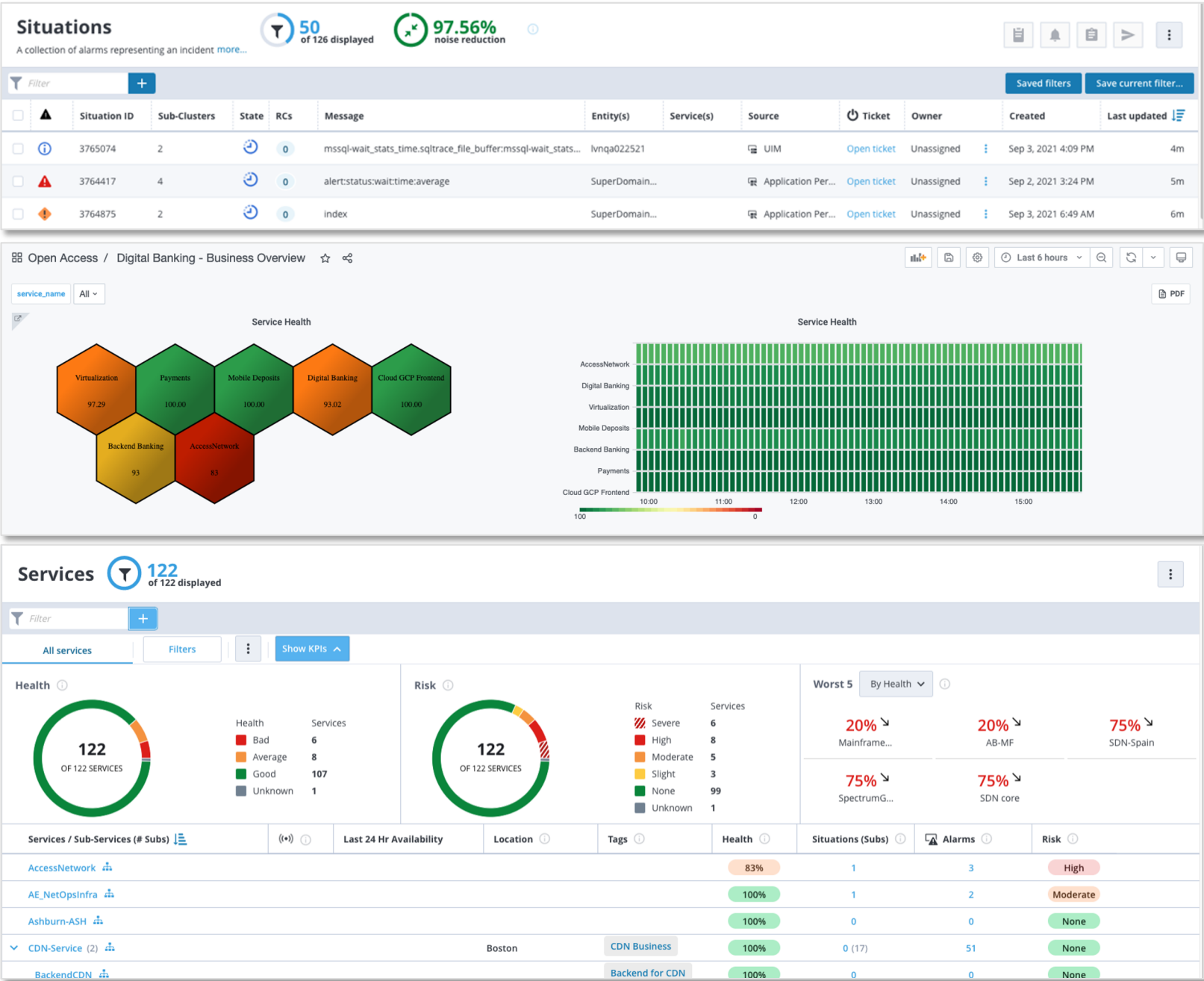
- Alarm Noise Reduction
- Alarm Management
- ITSM Ticketing
- Intelligent Remediation

### Unified Visibility

- Tools and Data Consolidation
- Dashboarding
- Reporting
- Single Pane of Glass

### Collaboration and Planning

- Capacity Planning and Forecasts
- Inventory Monitoring
- Cross Domain Observability
- Service Assurance



OverviewAlarmsTimelineAnnotation

Evidence

3

Entity(s)

...found by monitoring applications, network, infrastructure

30

Raw AlarmsAnomalies

...were generated

4

Clusters

...created by de-duplication using Natural Language Processing (NLP)

3765019

Situation ID

Critical

Severity was assigned based on criticality distribution

A single situation was generated based on time, topology and text analysis (NLP)

95.83%

Noise Reduction

...was achieved

<input type="checkbox"/>		Situation clusters	Message	Entity(s)	Service(s)	Source	Ticket	Owner	Created	Last updated
<input type="checkbox"/>		ID:3765019:0	The alert z/OS Alerts Status has breached the CRITICAL ...	SuperDomain...		Application Per...	<a href="#">Open ticket</a>	Unassigned	Sep 3, 2021 3:45 PM	1h 19m

OverviewLifecycle EventsAnnotation

Alarm Details

Alarm ID

669802.dxi-na1.saas.broadcom.com-31e814f1-b722-417c-a97d-9ea993693807-MVSDE25

Alarm type

Application

Alarm message

The alert z/OS Alerts Status has breached the CRITICAL threshold of 3

Monitoring Details

Group

Metric

SuperDomain | MVSDE25 | Cross-Enterprise APM Process | Cross-Enterprise APM Agent | z/OS Metrics | Alerts | J...

Owner Details

Assigned To

Acknowledged

Recommended automation actions (Confidence)

List Files Workflow

73%

Policy

Cr

La

Time since last update

an hour

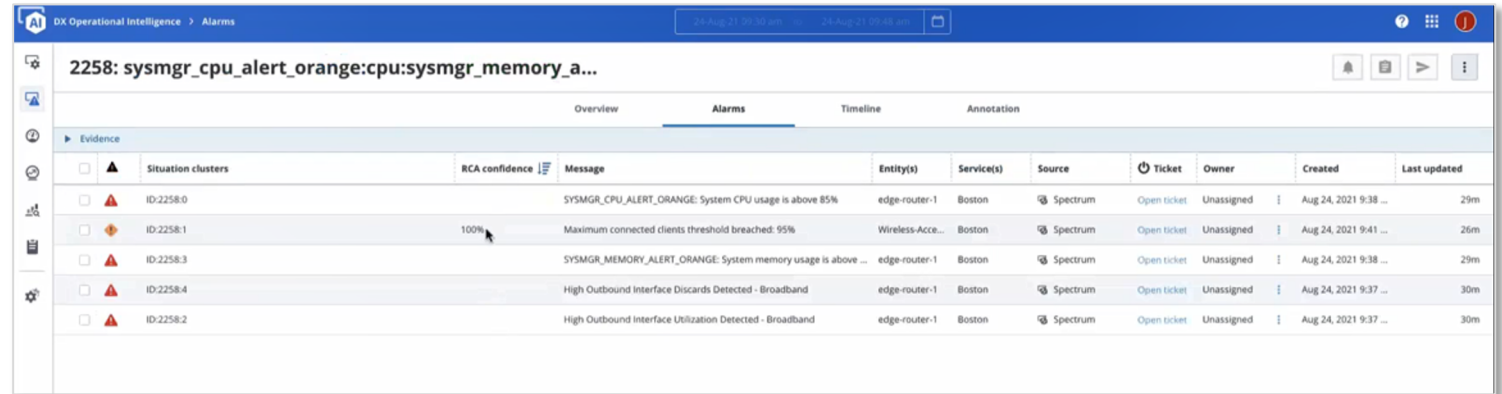
Identify and Address Problems Faster



# Leverage Situations to Start with the Right Alarm

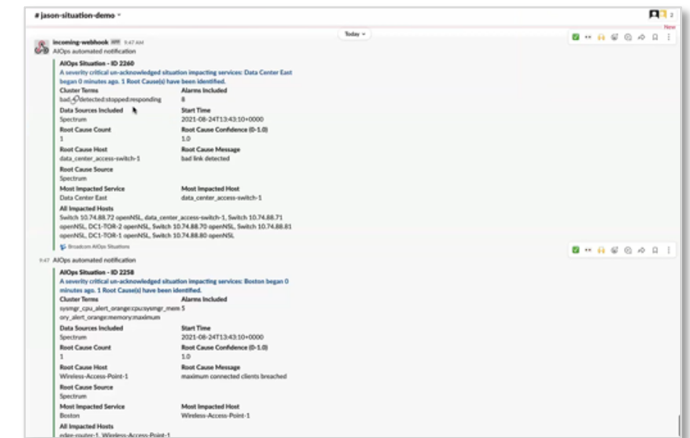
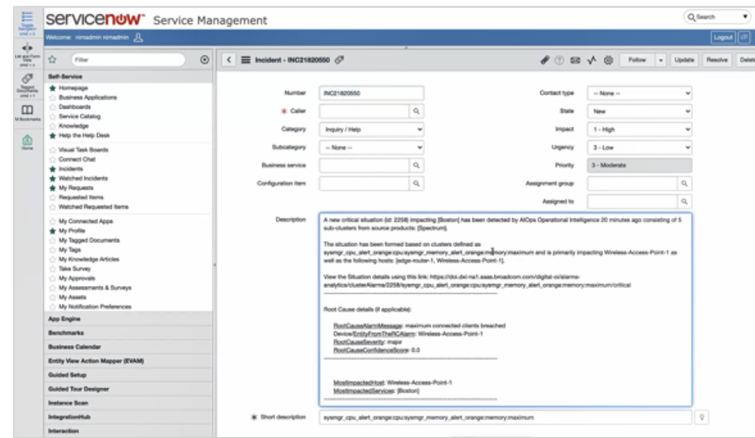
- Situations based on configurable Text, Time, Service and Host dimensions
- Network based root cause from DX NetOps root cause analysis
- Filter using Situations and alarm attributes
- Actions supported to open ticket, send a notification, add annotations, assign to troubleshooter and acknowledge or close
- [APIs](#) to configure and trigger programmatically

## Alarm Correlation and Probabilistic Root Cause



2258: sysmgr_cpu_alert_orange:cpu:sysmgr_memory_a...										
Evidence			Overview	Alarms	Timeline	Annotation				
	Situation clusters	RCA confidence	Message	Entity(s)	Service(s)	Source	Ticket	Owner	Created	Last updated
<input type="checkbox"/>	ID:2258:0		SYSMGR_CPU_ALERT_ORANGE: System CPU usage is above 85%	edge-router-1	Boston	Spectrum	Open ticket	Unassigned	Aug 24, 2021 9:38 ...	29m
<input type="checkbox"/>	ID:2258:1	100%	Maximum connected clients threshold breached: 95%	Wireless-Acce...	Boston	Spectrum	Open ticket	Unassigned	Aug 24, 2021 9:41 ...	26m
<input type="checkbox"/>	ID:2258:3		SYSMGR_MEMORY_ALERT_ORANGE: System memory usage is above ...	edge-router-1	Boston	Spectrum	Open ticket	Unassigned	Aug 24, 2021 9:38 ...	29m
<input type="checkbox"/>	ID:2258:4		High Outbound Interface Discards Detected - Broadband	edge-router-1	Boston	Spectrum	Open ticket	Unassigned	Aug 24, 2021 9:37 ...	30m
<input type="checkbox"/>	ID:2258:2		High Outbound Interface Utilization Detected - Broadband	edge-router-1	Boston	Spectrum	Open ticket	Unassigned	Aug 24, 2021 9:37 ...	30m

## Actions through UI or API



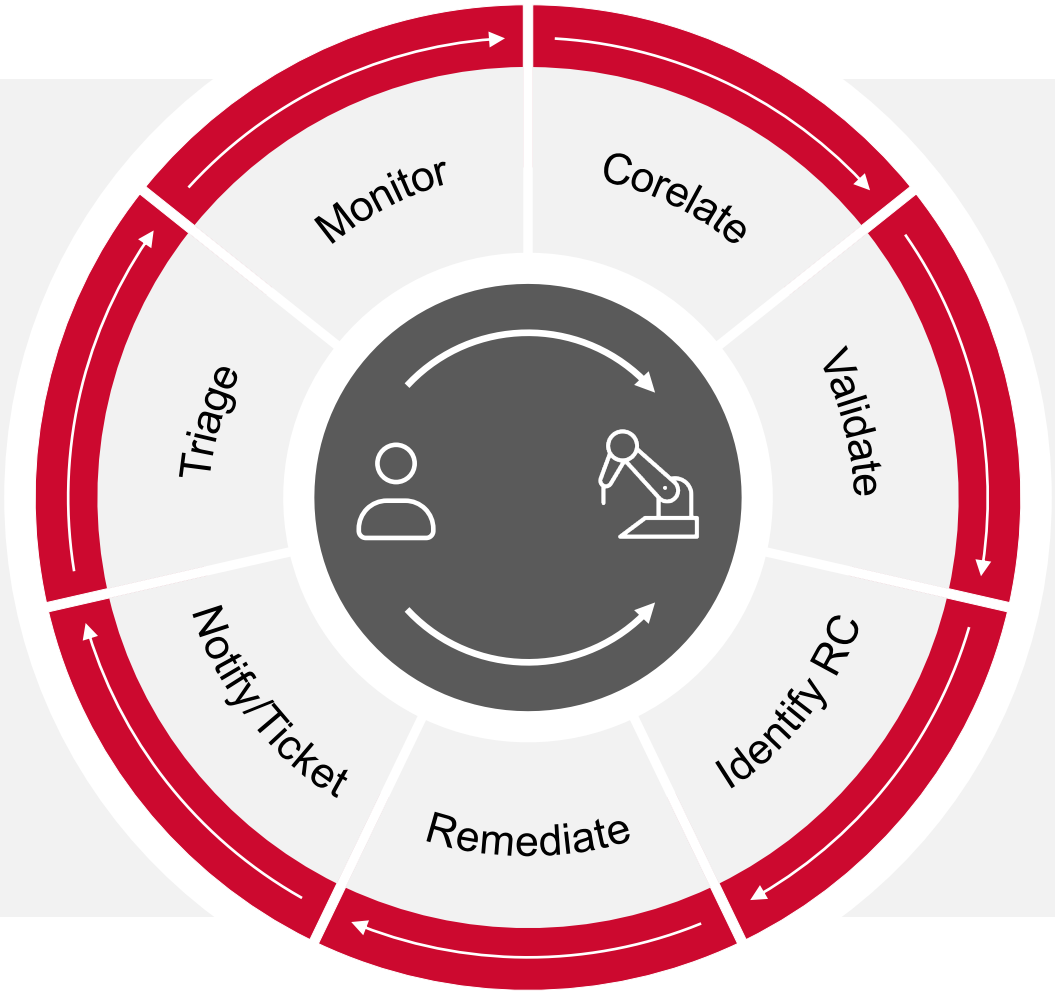
# Ticketing & Triage Model

Traditional Ops vs AIOps



## TRADITIONAL OPERATIONS

- Manual Process
- Error Prone
- Costly
- Repetitive
- Time-intensive

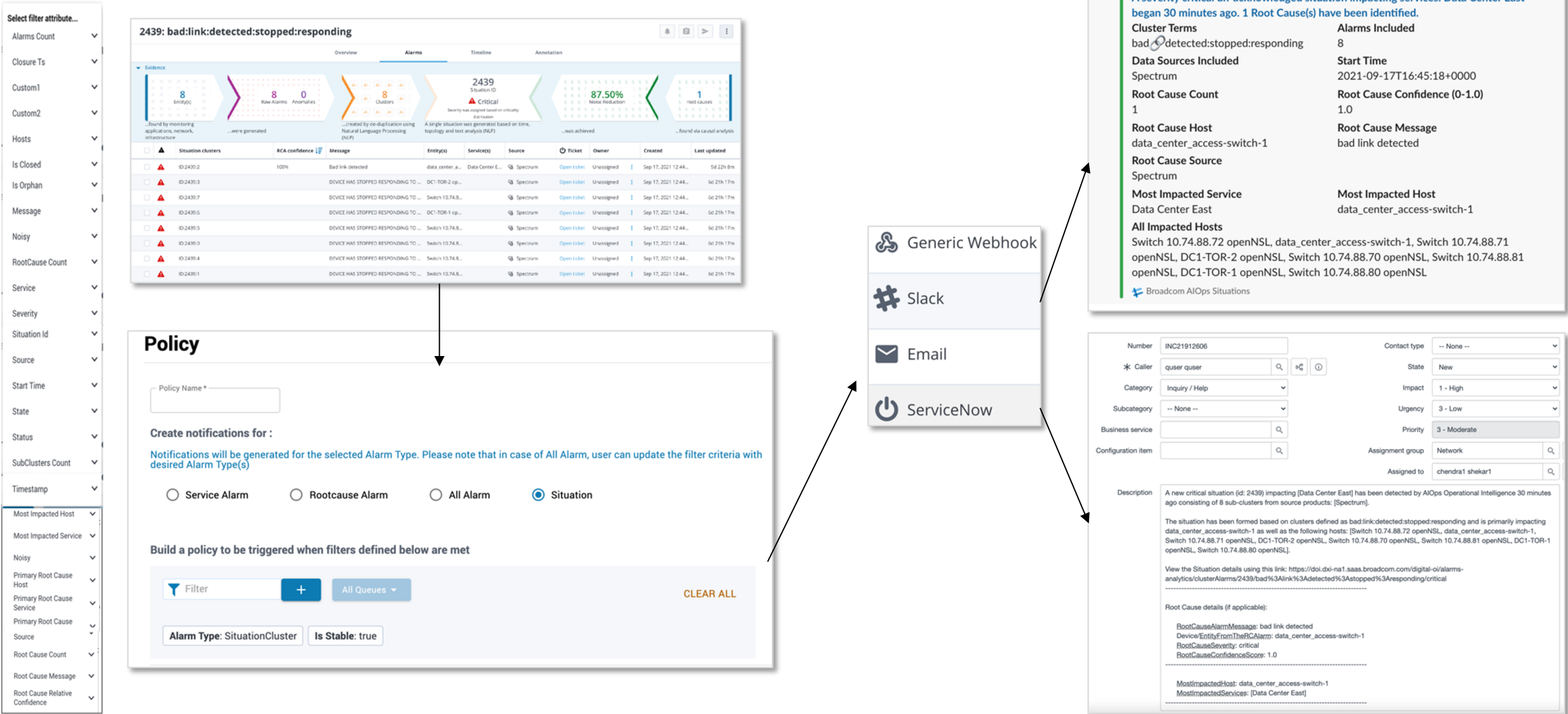


## DX OPERATIONAL INTELLIGENCE

- Automated Processes
- Consistent And Continual
- Reduces Operator Load
- Improves Accuracy and Efficiency
- Reduces Costs & MTTR



# Flexible ITSM and Notification Rules



# Identify Performance Issues with Anomaly Detection

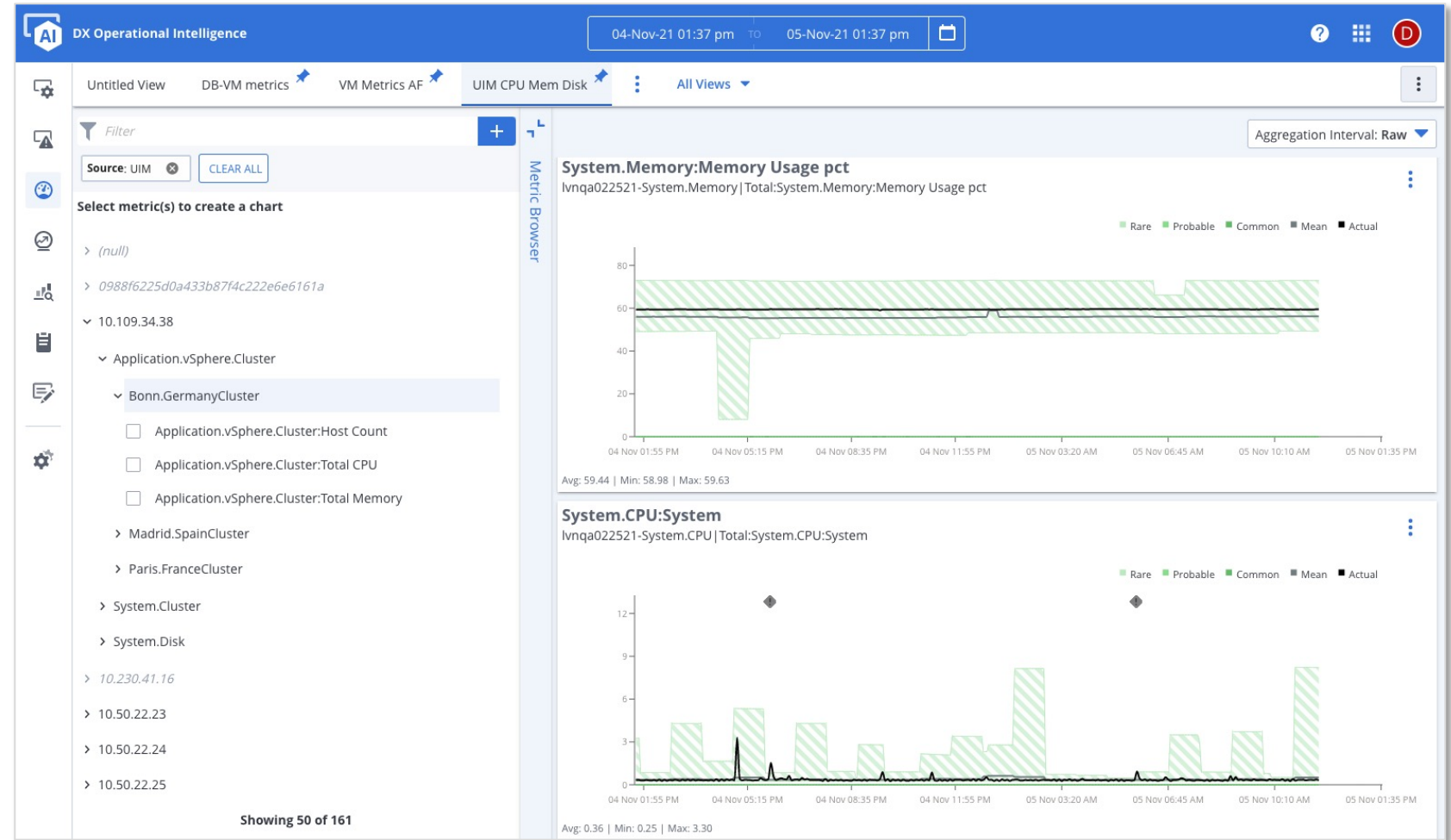
- Improved anomaly detection algorithm to reduce false positives
- Increased scale handled – upto 5M metrics per tenant
- Intuitive configuration for metrics to be enabled for anomaly detection
- Configurable alarms for identified anomalies

The screenshot displays the 'DX Operational Intelligence > Settings' interface. The main panel is titled 'APM Avg Response Time' and shows a configuration for 'Product name' (Application Perfo...) and a 'Filter' button. Below this is a table with columns 'Metric name' and 'Source'. The table lists several 'Average Response Time (ms)' metrics from 'SuperDomain | Custom Metric Host (Virtual) | Cust...'. A 'Delete' button is at the bottom left. A 'Configure Alarms' dialog is open on the right, showing options to 'Enable Detection' and 'Use System Settings'. The 'Alarm' section is configured with 'Alarm when anomaly is' set to 'Above threshold' and 'Alarm if anomaly' set to 'Count over threshold is 5 in 6 occurrences'. The 'Alarm Message' field contains a template: `\${metric\_name} has breached threshold for \${countOverThreshold} out of \${observationCount} times for \${host}`. The 'Select Alarm Notification Policy' dropdown is set to 'Choose an Alarm Notification Policy...'. The dialog has 'Cancel' and 'Done' buttons at the bottom right.

Metric name	Source
Average Response Time (ms)	SuperDomain   Custom Metric Host (Virtual)   Cust...
Average Response Time (ms)	SuperDomain   Custom Metric Host (Virtual)   Cust...
Average Response Time (ms)	SuperDomain   Custom Metric Host (Virtual)   Cust...
Average Response Time (ms)	SuperDomain   Custom Metric Host (Virtual)   Cust...
Average Response Time (ms)	SuperDomain   Custom Metric Host (Virtual)   Cust...
Average Response Time (ms)	SuperDomain   Custom Metric Host (Virtual)   Cust...

# Performance Analytics for Deep Dive Triage

- Cross domain performance metrics visualization for analysis and saved views for future references or evidence in a triage cycle
- Near real time data to stay on top of any performance issues in the monitored environment
- Intuitive filters on entity or metric to narrow down the analysis



# Monitored Inventory for Consolidated View of Monitored Environment Across Domains

- Near real time updates for the correlated monitored elements across the monitored environment
- Contextual information and workflows for operators to view alarms, performance metrics, services impacted and capacity projections from a single view
- Filters to identify a critical device or entities belonging to a service or entities in maintenance, etc.
- Manage maintenance windows in context of an entity, a service or a group of devices

The screenshot displays the Broadcom DX Operational Intelligence v21.2 interface. The main window shows the 'Monitored Inventory' table with columns for Entity, Path to CI, IP Address, and Source. A list of entities is shown on the left, including apollo.acme.com, zeus.acme.com, athena.acme.com, jupiter.acme.com, vulcan.acme.com, hermes.acme.com, aphrodite.acme.com, bacchus.acme.com, dionysus.acme.com, ceres.acme.com, demeter.acme.com, venus.acme.com, artemis.acme.com, hephæstus.acme.com, helios.acme.com, neptune.acme.com, mars.acme.com, bacchus.acme.com, diana.acme.com, and minerva.acme.com.

An inset window shows the 'Entity Details' for 'apollo.acme.com', displaying 53 total attributes. The details include Aliases (apollo.acme.com, LV-1256.acme.com), Role (App Server), IP Addresses (IPv4: 193.210.196.102, IPv6: 2001:0db8:85a3:0000:00:8a2e:0370:7334), MAC Addresses (42:26:40:92:F0:7F, C7:2E:68:2E:EC:35), Operating System (Windows Server 2 (10.0.17763)), Hardware Details (Intel Xeon E5-240, Lenovo ThinkServ), and Geographic Location (Las Vegas Data C).

Another inset window shows the 'Set a Maintenance Window' dialog, which allows users to suppress alarms during planned downtime. It includes fields for Name, Description, Start (04:09 AM), End (05:09 AM), Time zone (UTC-05:30), and Repeat (Does not repeat).



# Unified Dashboarding and Reporting

- Built in data connectors for alarm, metric, inventory and topology store to create joint views for dashboards providing end to end view
- Drill downs from overview dashboards to detailed views combined with contextual launches of the product features like alarm analytics or service analytics, etc.
- More data granularity supported for widgets in a dashboard to help time based analysis
- Performance improvements to handle large scale of data



Filter +

All services Filters ⋮ Show KPIs ^

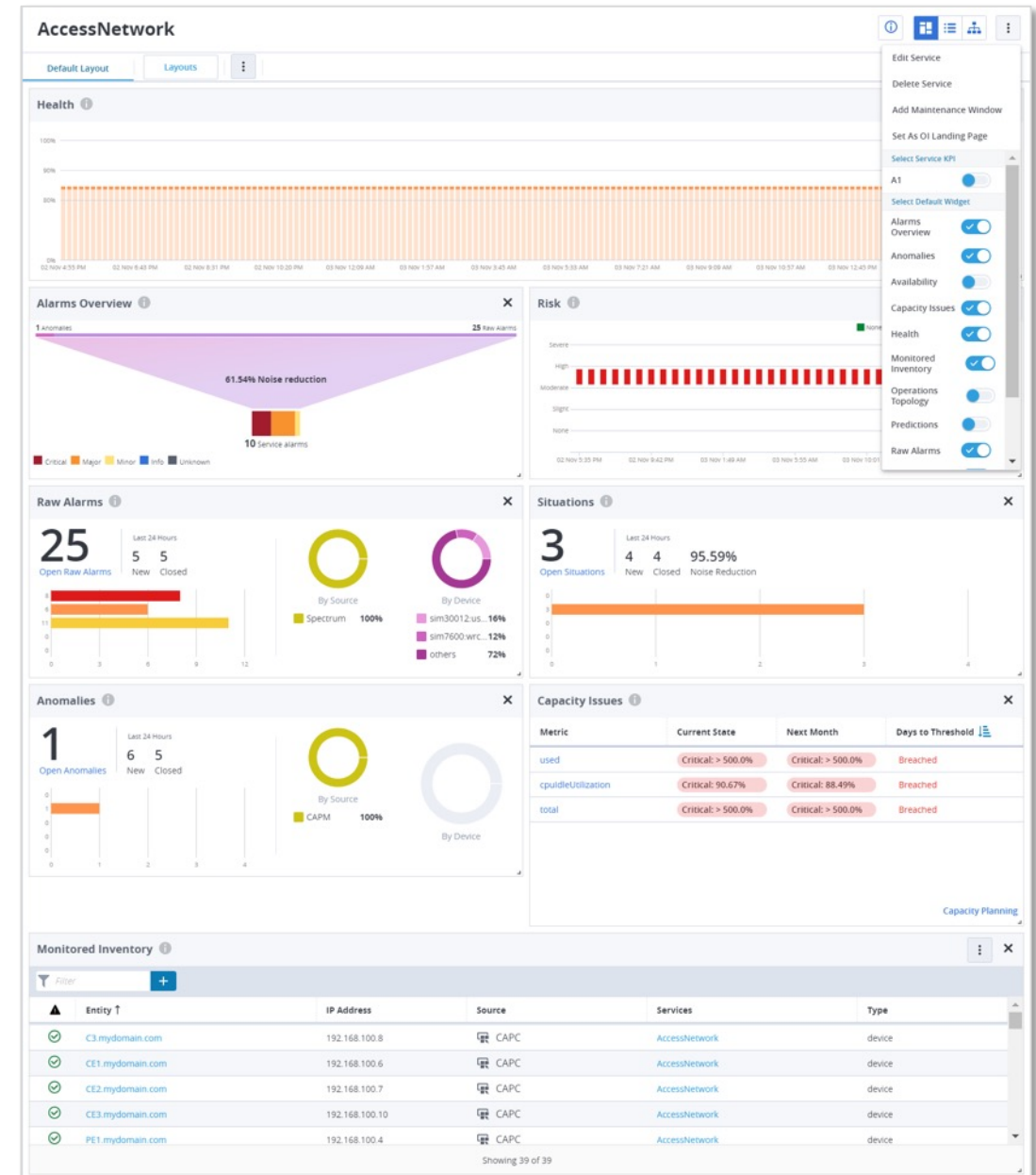


Services / Sub-Services (# Subs) ⌵	ⓘ ⓘ	Last 24 Hr Availability	Location ⓘ	Tags ⓘ	Health ⓘ	Situations (Subs) ⓘ	⚠ Alarms ⓘ	Risk ⓘ
AccessNetwork ⓘ					100%	0	0	None
AE_NetOpsInfra ⓘ					76%	6	14	High
Ashburn-ASH ⓘ					100%	0	0	None
> CDN-Service (2) ⓘ		Boston		CDN Business	100%	0 (12)	1	Slight
> Colussus (2) ⓘ				Colussus	100%	0 (0)	0	None
Colussus ⓘ					100%	0	0	None
Colussus ⓘ					100%	5	8	Slight
> DigitalBanking (6) ⓘ				newtag	97%	0 (40)	126	High

# Empower Hybrid Teams with Service-Driven Operations

# 360 Degree Context for Service Owners/SREs

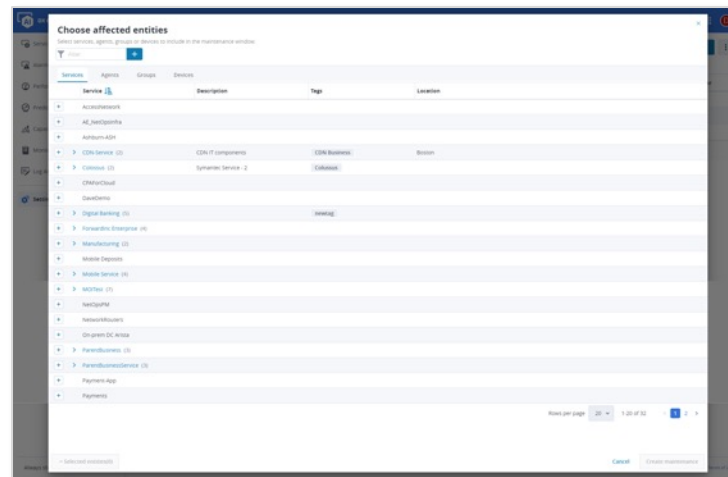
- Contextual information and navigation entry points for:
  - Health, availability and other KPIs with custom service KPI configuration
  - Monitored inventory that are a part of the service
  - Raw alarms and Situations trend over time to identify the health degrading components
  - Capacity projections at the service level to optimize resources in time
- Personalize the service details view for contextual widgets
- 1-minute service KPIs intervals to have the latest IT to Business view



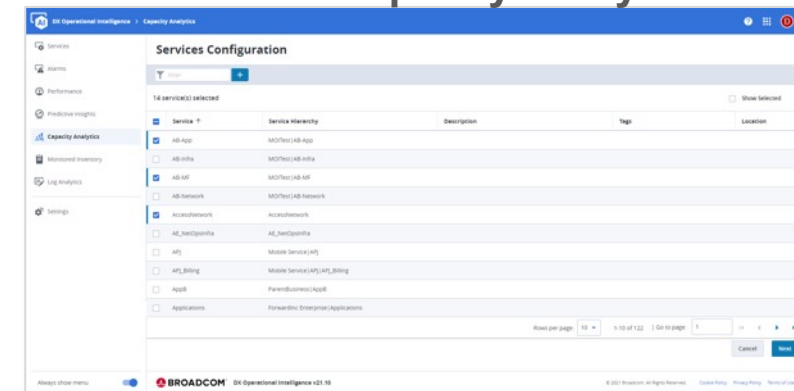
# Service Driven Configurations for Consistent Anchor

- Maintenance windows can be configured for the entire service(s) to ease management and suppress alarms and tickets
- Predictive capacity insights can be enabled for services and leverage service KPIs for what-if analysis
- Filters across the product based on services and service tags providing an easy and consistent way as users navigate through their workflows
- Out of the box dashboards for service driven monitoring

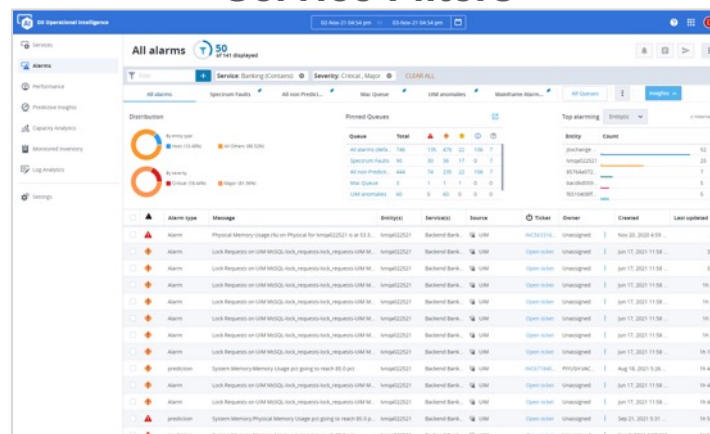
## Maintenance Windows



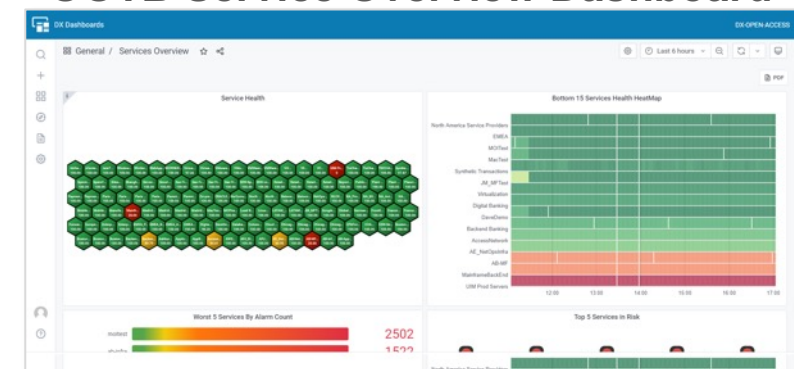
## Predictive Capacity Analytics



## Service Filters



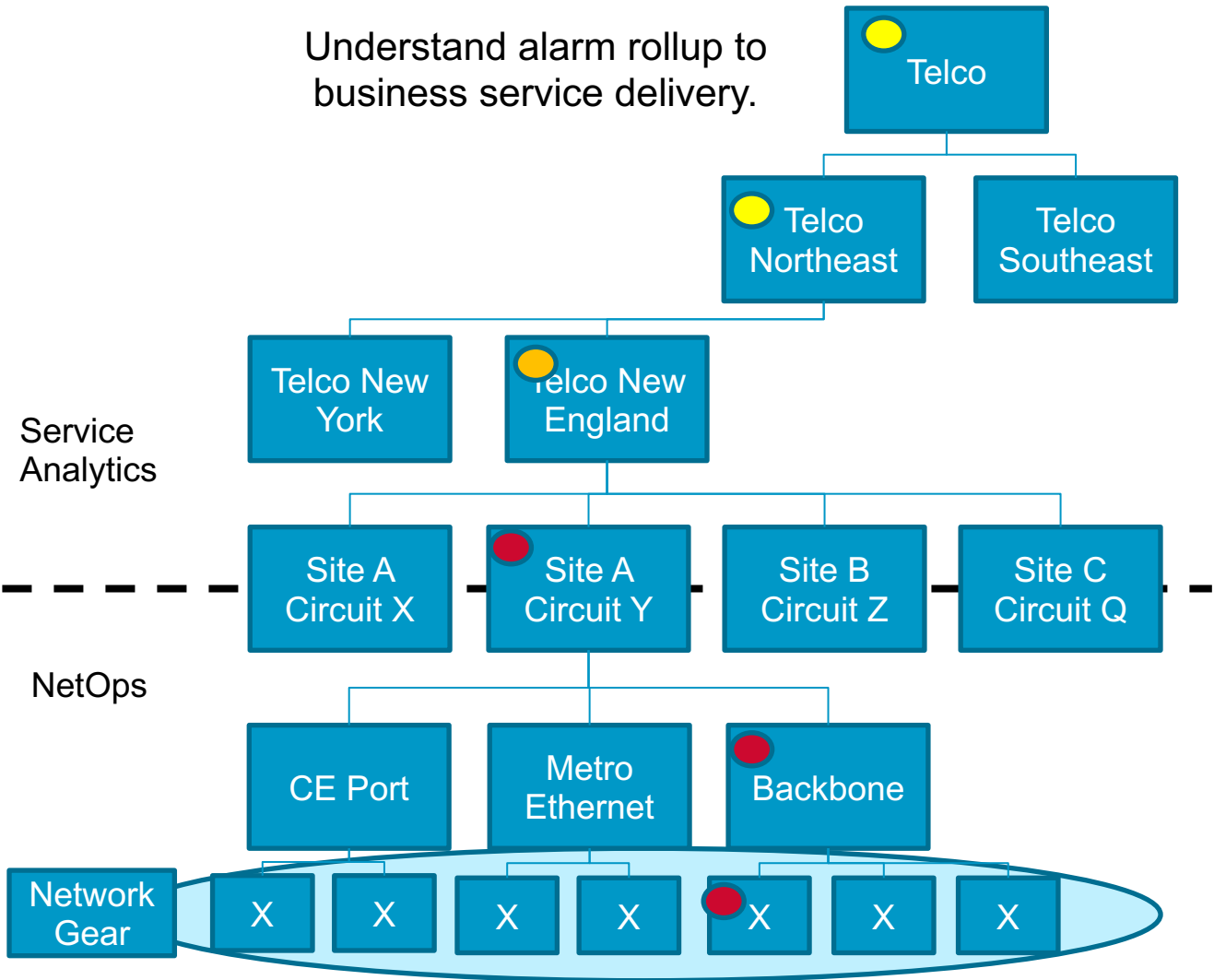
## OOTB Service Overview Dashboard





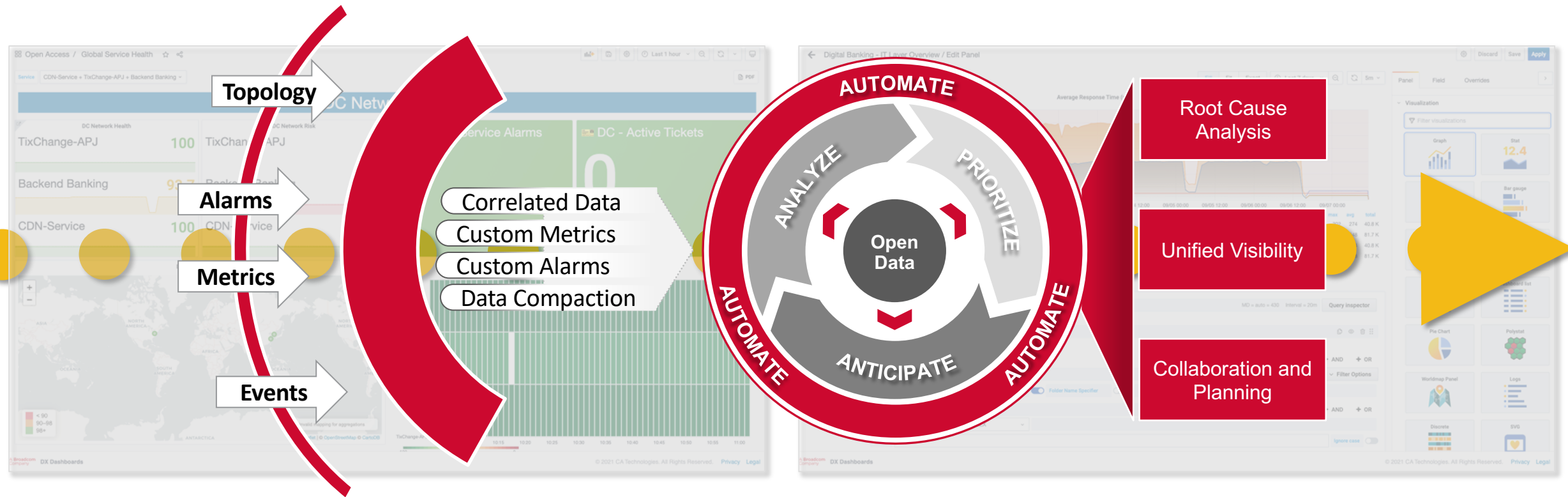
# Network Services within DX Operational Intelligence

- DX NetOps (Spectrum) services can be leveraged within DX Operational Intelligence to view network services as part of cross-domain services
- Identify the impact of network services on business or IT services through this integration
- Easy configuration via Spectrum – OI connector (Spectrum Data Publisher)



# Manage Services at Scale

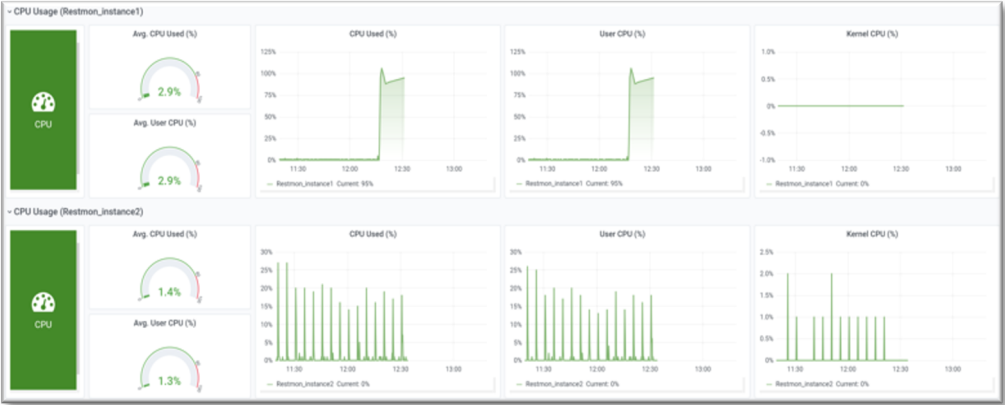
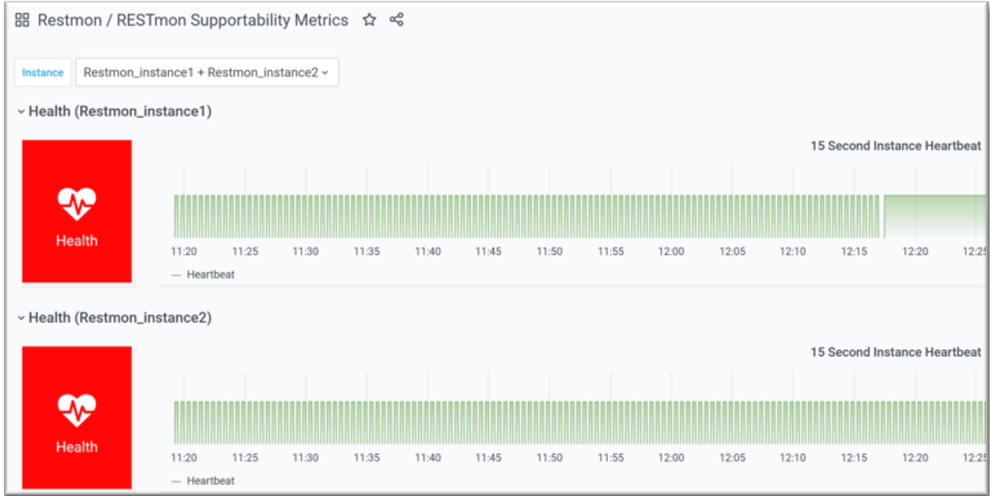
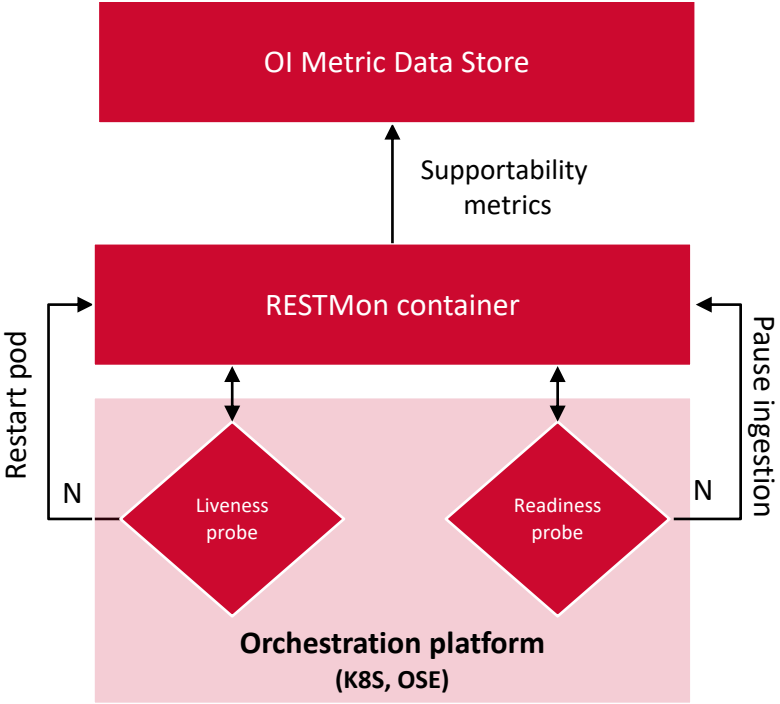
- Service Analytics supports up to 20k services across the service drive workflows
- Manage services programmatically via [CRUD APIs](#)
- Control and limit service management via out of the Power User role



# Integrations

# RESTMon 2.1 for 3rd Party Integrations

- Monitor RESTMon performance & health via OTB DX Dashboard
- Improve availability with Liveness & Readiness probes; Works OTB on orchestration platforms such as Kubernetes & OSE
- 7 New Reference Integrations available to get started
- Improved performance of the overall RESTMon framework





# Enhanced Ticketing and Webhook Integrations

- New bi-directional integration added for BMC Remedy ticketing
- Additional filters based on service tags, alarm state, etc. for channel policy definitions
- Intuitive Webhook integration via UI with the ability to select the payload attributes and test/validate the Webhook connection before saving to ensure the integration was successful

The screenshot shows the 'Create Generic Webhook' form in the AIOps interface. The form includes the following fields and options:

- Enable the channel:** A checkbox.
- Channel Name:** A required text input field.
- Webhook URL:** A required text input field with a note: 'Enter URL with http:// or https://'.
- Authentication Type:** A dropdown menu currently set to 'No Authentication'.
- Webhook Headers:** A section with a table for adding headers. The table has columns for 'Key' (with a dropdown 'Enter or select key') and 'Value' (with a text input 'Enter value').
- Webhook Payload:** A large text area with a note: 'You can either copy and paste or select the payload data file from "Add Keys" button.' There is an 'Add Keys' button and a 'Required' label.
- Linked Policies:** A dropdown menu.
- Buttons:** 'Delete', 'Cancel', 'Test', and 'Create'.

The footer of the interface shows the Broadcom AIOps logo and copyright information: '© 2021 Broadcom. All Rights Reserved. Cookie Policy Privacy Policy Terms of Use'.

The screenshot shows a dropdown menu titled 'Select filter attribute...'. It lists various attributes that can be used for filtering, each with a dropdown arrow:

- Acknowledged
- Age (In min)
- Alarms Count
- Annotation
- Closed Products
- Closure Ts
- Cluster Previous Name
- Hosts
- Initial Impacted Host
- Initial Impacted Services
- Initial Impacted Template
- Is Closed
- Is Force Closed
- Is Orphan
- Is Stable
- Maintenance
- Message
- Most Impacted Host
- Most Impacted Service
- Most Impacted Template
- Noisy
- Primary Root Cause Host
- Primary Root Cause Service
- Primary Root Cause Source
- Root Cause Message
- Root Cause Relative Confidence
- Root Cause Score
- Root Cause Severity
- Root Cause SubCluster Id
- RootCause Count
- Service
- Severity
- Situation Id
- Situation Source
- Source
- Stable Time
- Start Time
- Status
- SubClusters Count
- Timestamp



## Settings



Data Sources

### Setup Data Sources

Download the DX Gateway to ingest a wide variety of data: metrics, events, alarms, logs, inventory groups, etc.

[Setup](#)

Connector Parameters

### Connector Parameters

Find the unique keys required to integrate on-premise deployments

[View](#)

11 Monitoring Groups

### Configure Monitoring

Set what is monitored and how (anomaly detection, prediction, capacity planning, etc.)

[Configure](#)

17 Predictive Definitions

### Enable Predictive Definitions

Enable and customize predictive data definitions for metrics

[Enable](#)

25 Policies

### Create Policies

Define policy rules (including alarms) in order to detect and respond to events



1 ITSM

### Connect Ticketing System

Connect with a ticketing system (e.g. Jira, ServiceNow) to manage incidents and create tickets



15 Notification Channels

### Connect Notification Channels

Integrate with email, slack and other Webhook-based channels



7 Message Templates

### Create Message Templates

Create custom messages, with system variables, to be reused across notification channels

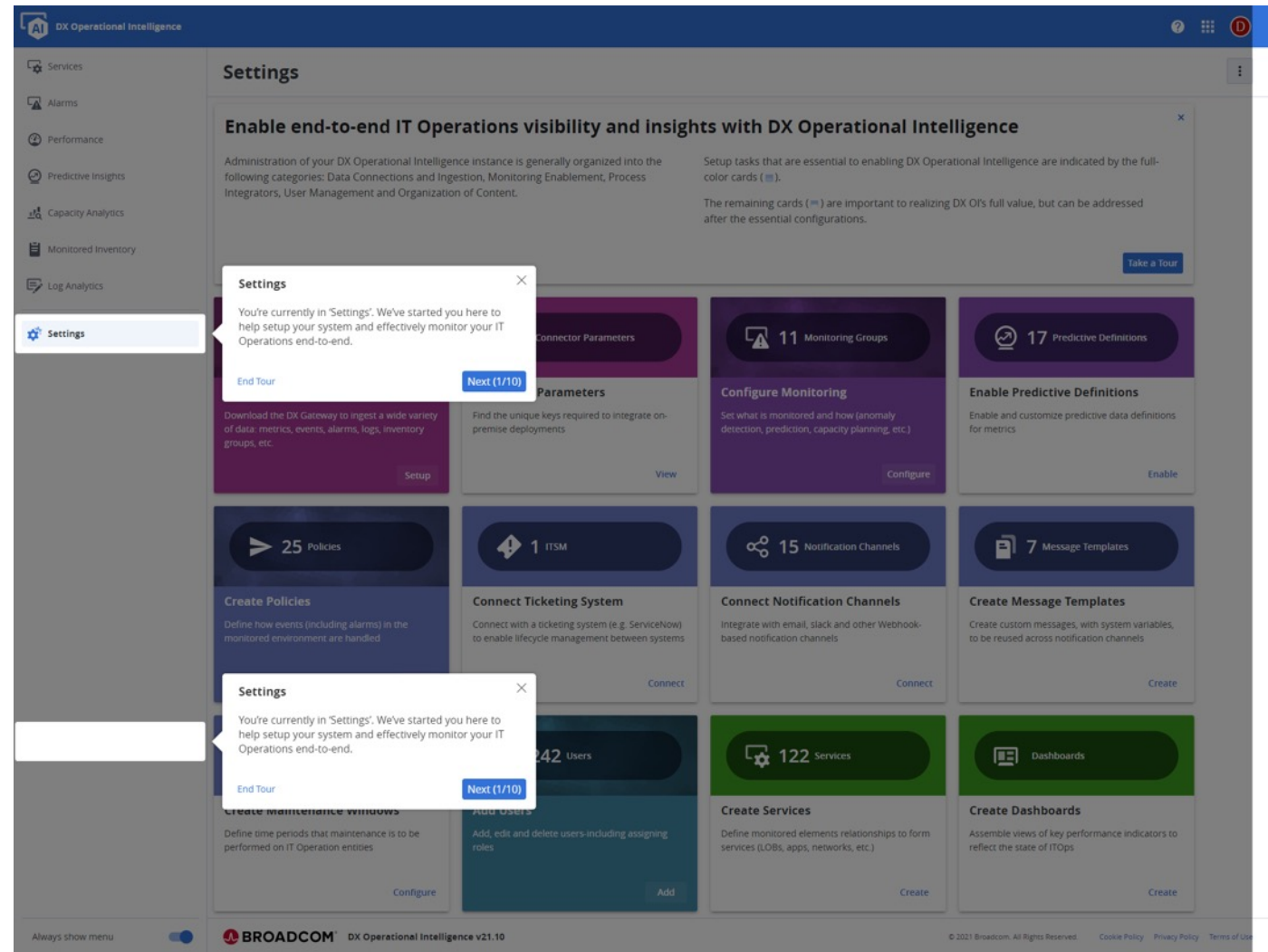
# Deploy and Manage with Ease

# Improved Seamless Installation Lifecycle

- IOPS evaluation pre-requisite for the installer
- Minimized footprint and Export by product for ease of downloads
- Download tokens to control authorized downloads
- Improved Uninstall script
- Path to upgrade from 20.2
- Role-based administration for
  - Cluster administrator
    - Define namespace
    - Define persistent volumes (PVs)
    - Define high-level directories
  - Application administrator
    - Install application using non-privileged ID
- Supported on OCP 4.7 and K8s 1.21

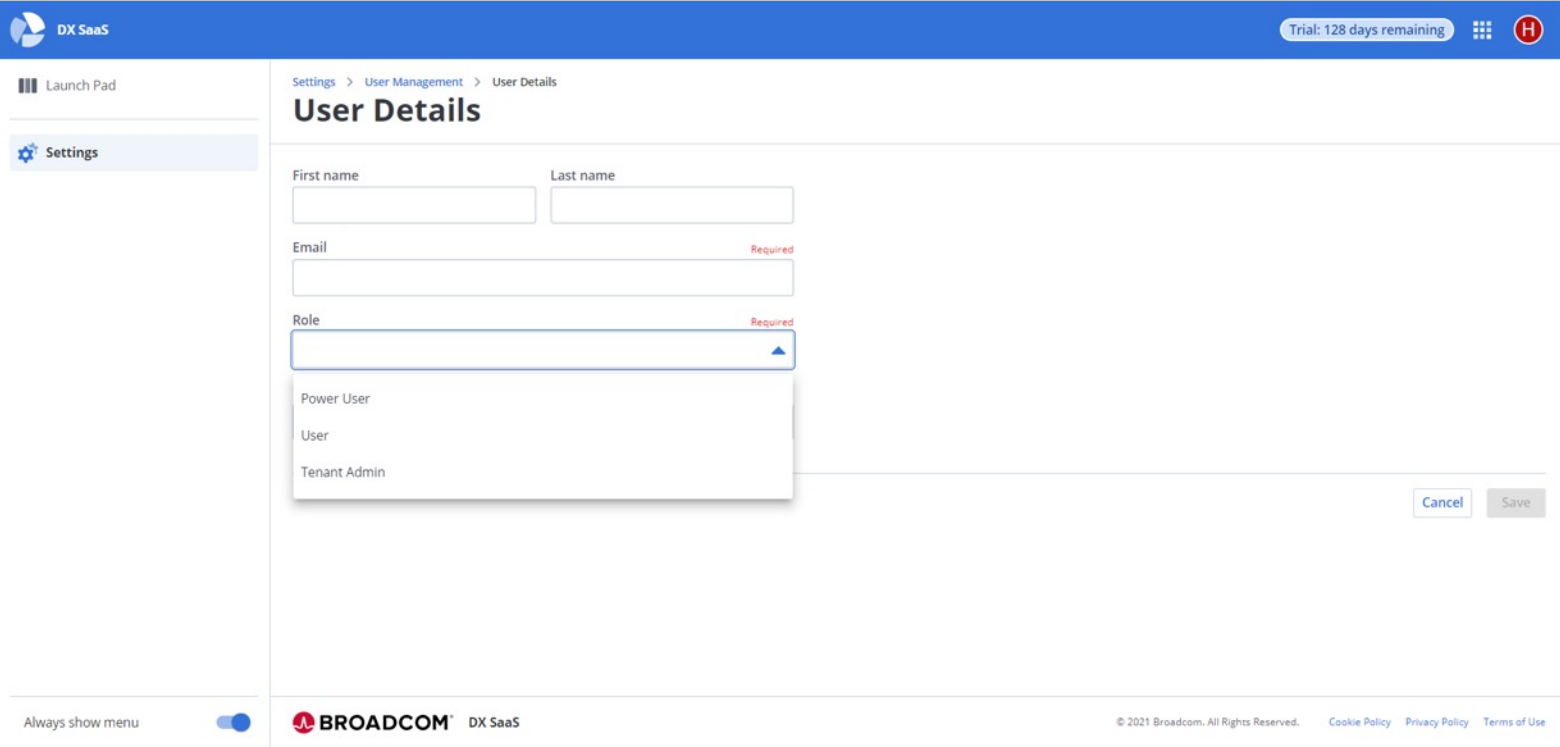
# One Stop Settings Page for Easy Tenant Onboarding

- Default landing page for 1<sup>st</sup> time login of Tenant Administrator
- Provides a virtual tour to familiarize the Tenant Administrator with the Settings page
- Provides all the configurations required for tenant administration in a single view along with the high level summary of the existing configurations



# Out of the Box Roles to Control Access and Privileges

- Out of the box roles across the platform to assign pre-defined privileges for :
  - Tenant Administrators: Everything
  - Power Users: Everything except tenant onboarding and user management
  - Users: Primarily read only access
- Provides mapping with SAML groups



The screenshot displays the 'User Details' form within the DX SaaS interface. The form is located under the 'Settings > User Management > User Details' breadcrumb. It includes input fields for 'First name', 'Last name', and 'Email'. The 'Email' field is marked as 'Required'. Below these is a 'Role' dropdown menu, also marked as 'Required', which is currently open, showing three options: 'Power User', 'User', and 'Tenant Admin'. The 'Power User' option is highlighted. At the bottom right of the form are 'Cancel' and 'Save' buttons. The interface also features a 'Launch Pad' menu on the left, a 'Settings' gear icon, and a 'Trial: 128 days remaining' notification in the top right. The footer includes the 'Always show menu' toggle, the 'BROADCOM DX SaaS' logo, and copyright information: '© 2021 Broadcom. All Rights Reserved. Cookie Policy Privacy Policy Terms of Use'.





**BROADCOM<sup>®</sup>**  
SOFTWARE

**Solving the Complex.**