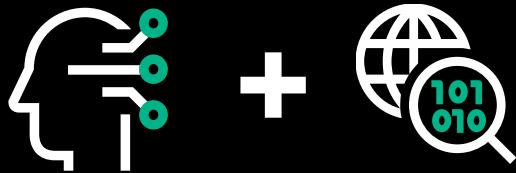




HPE INTELLIGENT ASSURANCE SUITE



The HPE Intelligent Assurance Suite is a Big Data and Artificial Intelligence based platform that provides a powerful way to transform vast amounts of network data into actionable insight that paves the way toward zero-touch operations and self-driven networks. The HPE Intelligent Assurance Suite provides Machine-Learning driven correlation and automation to dramatically reduce the number of alarms, both identify and operationalize unknown problems, helping operations prevent major outages and facilitate automatic control loops, from edge to cloud.



HPE INTELLIGENT ASSURANCE

connects the dots to let you focus on business

CHALLENGES

Today, communications service providers (CSPs) and digital service providers (DSPs) are striving to increase customer satisfaction and lower operational costs, while at the same time developing competitive differentiation. In this climate, it is essential that the underlying network infrastructure operates at peak effectiveness and efficiently. To reach this goal, the service assurance process has to evolve toward “zero-touch” operations, which implies that automation growingly needs to be derived from the knowledge hidden in the vast amounts of network data.

Today's two main challenges in the service assurance process for network operations are:

- Lack of availability of network domain experts to facilitate knowledge acquisition.
- Event and alarm management in the new networks (virtual or software-defined networks). Indeed, network operation domains cannot wait for knowledge to be accumulated over the coming years, while operating the network inefficiently. The level of complexity to operate these cloudified, virtualized networks is much higher than in traditional networks, since the number of elements involved is much larger and dynamic in nature. There is no other way to acquire and apply knowledge on how to operate new networks than doing it automatically.

HPE SOLUTION

The HPE Intelligent Assurance Suite helps CSPs to extract the hidden knowledge from the network. It leverages information stored in a data lake to automatically identify groups of events (alarms, tickets or configuration logs) that occur on a regular basis, that is, patterns helping operations to operationalize rules in HPE Unified Correlation Analyzer (UCA) that will, in turn, automate the actions to handle them whenever they occur. Those automated actions can be:

- Removal of non-significant alarms and duplicated alarms
- Reduction in symptomatic alarm information, focusing attention on root cause, with or without automated resolution
- Creation of predictive alarms
- Execution of actions to remediate or prevent a network issue

The HPE Intelligent Assurance Suite addresses specific use cases that are of interest to operations in different situations, bringing to market solutions that provide tangible value to CSPs and DSPs in the OSS domain:

- Increasing efficiency of the operations for problem detection and resolution
- Leveraging Machine-Learning techniques to find relevant patterns in historical data, helping operations identify unknown problems and reduce flows of alarms, reusing available Big Data/AI open sources
- Processing existing data sources and delivering end-to-end use cases that manage network events

The HPE Intelligent Assurance Suite addresses those various use cases; thanks to two main blocks in its architecture: The **Foundation** and **Intelligence layers**. Within the first, **Fault Archival and Statistics** provides insights of a descriptive nature, constitutes the foundation for the intelligent use cases and measures their benefits. Within the second, **Pattern Discovery and Operationalization** provide insights that can be used to trigger automatic correlations or preventive actions, leading to the automatic resolution of incidents before they become serious problems that impact the customers.

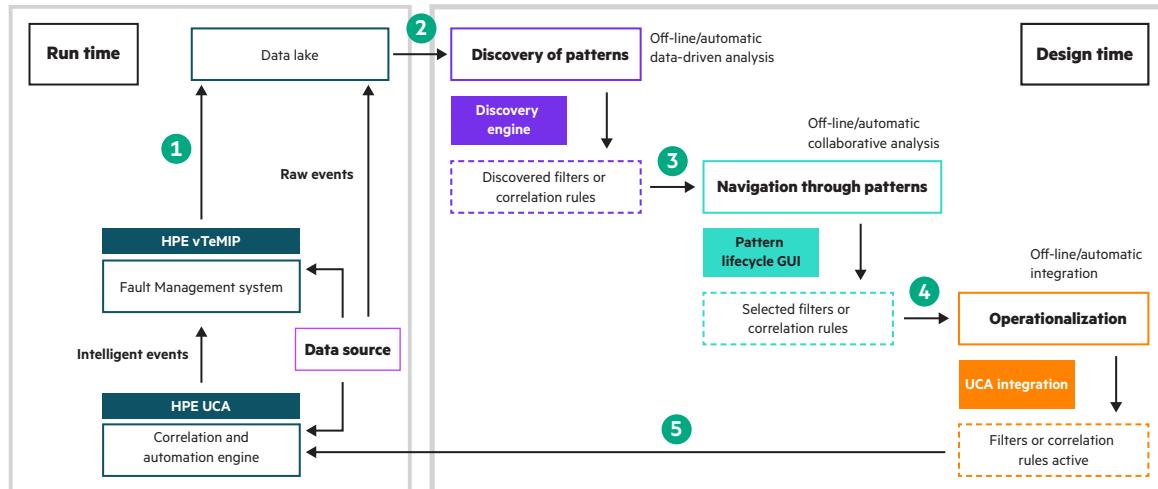


FIGURE 1. HPE Intelligent Assurance automating the Fault Management process

Hewlett Packard Enterprise delivers a product whose ultimate goal is not to provide Machine-Learning capabilities, but to use them to automate the end-to-end Fault Management process with much more effectiveness than ever before.

OUT-OF-THE-BOX FEATURES

Fault Archival and Statistics

HPE Fault Archival and Statistics augments the traditional Fault Management OSS with powerful alarm reporting and analysis functions achieved by exporting in real time all the incoming alarms into a Big Data platform, making all alarms available irrespective of their current state. With an optimized dimensional model, you can quickly access large amounts of fault information for analysis and reporting, thereby extracting knowledge and insight from Fault Management data.

By generating detailed statistical analysis and reports about all the faults from this warehouse, HPE Fault Archival and Statistics allows you to better understand network behavior and how it is managed.

A set of off-the-shelf notice boards allows monitoring of both overall network health and network management activity. A number of charts are made available to provide information on network entities, operation contexts and domains directly accessible from HPE Unified OSS Console.

The HPE Fault Archival and Statistics KPIs can be split into several dimensions:

- Improvement in Fault Management effectiveness:** Percentage of filtering and correlation reducing the number of actionable alarms, percentage of automation reducing the need for ticket creation by operator intervention and increasing automated problem resolution
- Improvement in responsiveness:** Percentage reduction in the diagnostic time, percentage reduction in time needed for trouble ticket creation
- Improvement in customer satisfaction:** Percentage reduction in resolution time of problems
- Improvement in NOC staff effectiveness:** Percentage increase in number of problems resolved by NOC FTE per shift/day/week/quarter/year

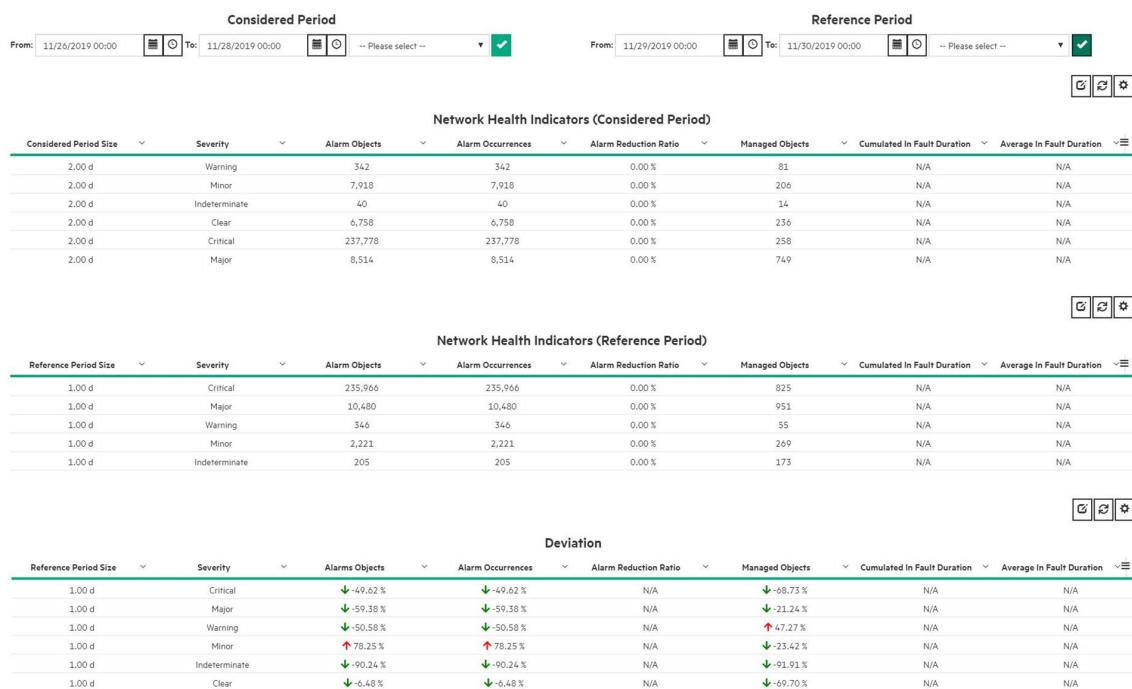


FIGURE 2. Fault Archival and Statistics: Comparison of Network Health with a reference period

A Frequency tool allows to understand the frequency and the distribution of events, in terms of dimensions related to symptoms or topological values, and time slices (e.g., 30 minutes).



FIGURE 3. Frequency tool: Distribution of symptoms with drilldown to the regions of a given symptom

Pattern Discovery and Operationalization

The primary objective of the application of Pattern Discovery is to find automatically:

- Groups of events with similar attributes or properties into sets. This results, as an example, in reducing the volume of alarms that need to be processed by operations teams and allows them to work with higher quality and richer information.
- Correlations emerging from the application of statistical techniques, leveraging Machine Learning.

Pattern Discovery also provides a GUI to help discover new patterns. This GUI has a wide set of attributes to easily adjust and fine-tune the results. Most important attributes are: Support of the pattern, time window, and confidence.

Once a Pattern-Discovery run has finished, the end user is able to easily navigate among the patterns that have been discovered, understand the benefits of a certain pattern versus other related patterns, and ultimately decide which patterns should be operationalized.

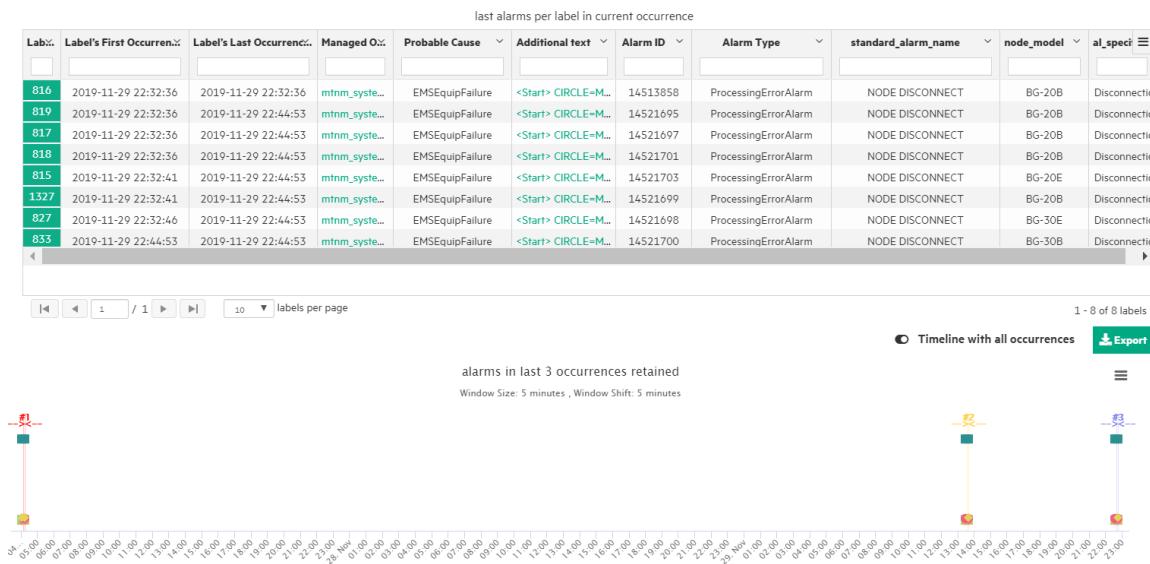


FIGURE 4. Details of a pattern: Group of alarms that make up the pattern and timeline with last occurrences

The results emerging from the application of the Pattern Discovery are operationalized within a production correlation solution: Automatic integration with HPE UCA is part of the feature set of the HPE Intelligent Assurance Suite.

Scenarios of patterns that can be operationalized in HPE UCA are:

- Suppression: One given element is producing low priority alarms every minute and the field called operator note is empty. The outcome is the suppression of these repetitive events.
- Compression: A given system is generating several different alarms also within the minute or a very short time window: Operating System alarm, Database alarm, and Network node alarm. In this case, the compression maintains only one of the occurrences of the repetitive event.
- Problem-alarm: It is known that the outcome of a certain pattern is an incident (for example: network outage) that needs to be prevented. Here the outcome is raising a ticket in the ticketing system in order to prevent the network outage when the pattern is detected. In the release 2, it is also possible to link the problem detection with the problem remediation, by selecting one of the decision-trees deployed in the Automation engine.
- Predictions: Some patterns detected automatically show a predictive behavior. For those predictive patterns, Operationalization creates a correlation rule on the events leading to the issue to be predicted, that will create a predictive alarm and could also execute a remediation action to prevent the issue to happen.

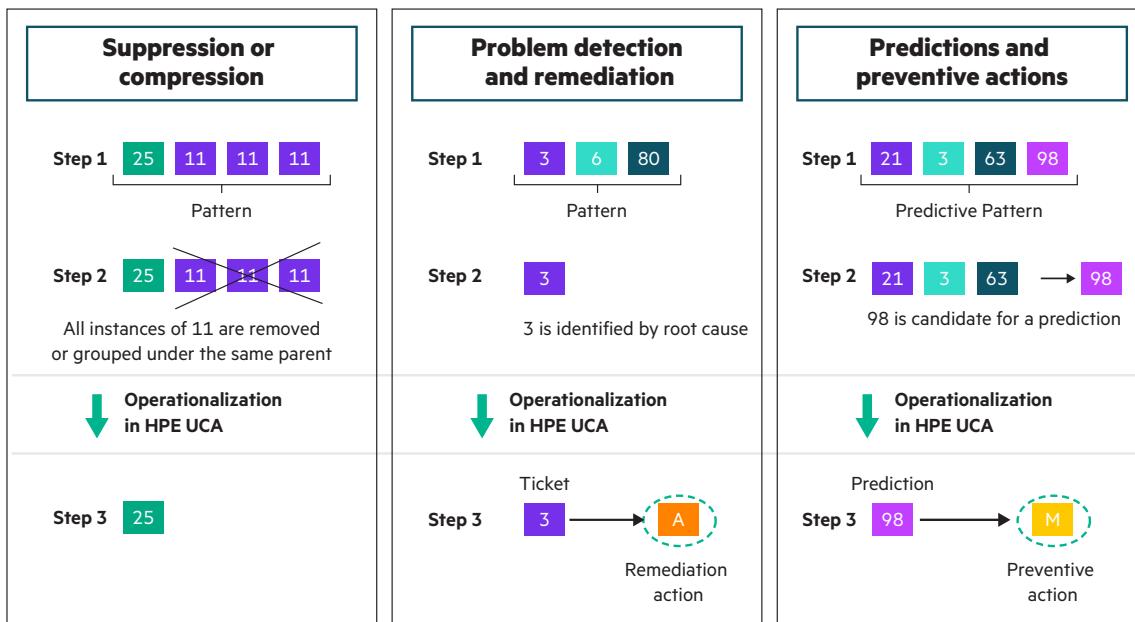


FIGURE 5. Pattern Operationalization scenarios

In certain scenarios, events can be enriched with information coming from other data sources, which allows to increase the level of automation, provided that the different data sources are preprocessed to fit the format expected by the Pattern-Discovery engine. As an example: If events are enriched with information related to trouble tickets, the number of patterns eligible to be operationalized can be reduced (as interesting patterns are only those ending up in an alarm related to a ticket), leading to lot of time saved by the operators.

By reviewing the results provided by out-of-the-box reports in Fault Archival and Statistics, users can quantify the improvement in the volume of alarms managed before and after operationalizing a certain pattern (or a set of patterns).

For those patterns that have been operationalized, there is also an Audit tool that allows to:

- Understand if the patterns are triggered as expected: if not, new discoveries should be launched to address the new situations happening in the network
- Identify those events that are not correlated by any rule, so that specific discoveries can be launched on them to reach a better level of correlation
- Visualize the future alarms, individually and aggregated (e.g., per region)
- Analyze the accuracy of the predictions generated by the predictive patterns

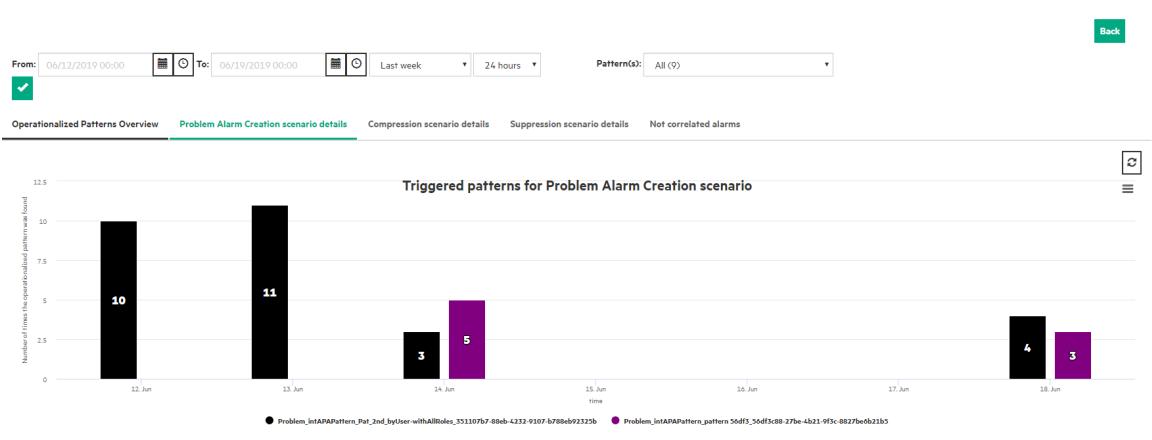


FIGURE 6. Audit report to understand patterns triggered in the selected period

There are cases where the most important information of the network event is reported in free-text (non-structured information) fields: For discovering patterns on that type of events, an initial step of free-text processing is required. Pattern Discovery allows to execute free-text processing, analyze the results (clusters) and iterate on it, before launching the discovery to get patterns.

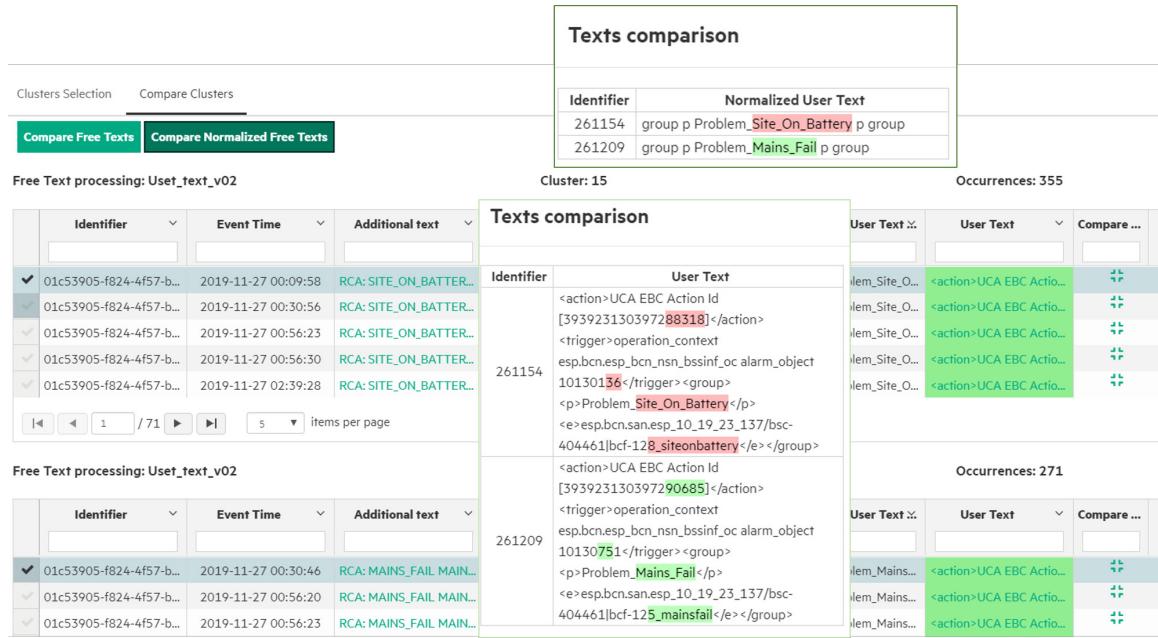


FIGURE 7. Analysis of the clusters generated by the free-text processing



HPE INTELLIGENT ASSURANCE SUITE TECHNICAL SPECIFICATIONS

Solution based on proven technologies

The unique technology of the HPE Intelligent Assurance solution relies on best-in-class and proven technologies, such as:

- High-performance report generation with the best-in-class visualization capabilities: **HPE Unified OSS Console**
- Highly scalable and flexible data management architecture that allows to store and analyze huge amounts and types of data, all in a single open source platform: **Apache Hadoop** and **Apache Spark**
- A solution fully integrated within **HPE vTeMIP** or other Fault Management systems, through a high-speed and reliable mediation bus based on **Apache Kafka**
- A solution fully integrated with **HPE UCA**, for automatic correlation in Pattern-Discovery scenarios

System requirements

Hardware and software

For the HPE Intelligent Assurance Suite

Linux®: Any Intel® Xeon® x86-64 Server (see supported platforms/operating system support)

For the HPE Unified OSS Console web client applications

Supported web browsers: IE, Firefox, Google™ Chrome

Please contact your sales representative for up-to-date information on supported versions.

For memory, disk, and CPU dimensioning, an analysis of hardware requirements is strongly recommended.

Please contact your sales representative for a sizing study request.

Third-party software

Apache Hadoop (Cloudera), through HPE specific part numbers for Cloudera (HPE and Cloudera have an established OEM resell relationship)

Supported platforms for the HPE Intelligent Assurance Suite

Operating system support

Red Hat® Enterprise Linux 7

Please contact your sales representative for up-to-date information on support for newer versions.

Hadoop support

Cloudera CDH 6.3

Considerations

Growth

The minimum hardware/software requirements for any future version of this product may be different from the current version requirements.

HPE OSS ASSURANCE SOLUTIONS

HPE Intelligent Assurance is part of a comprehensive integrated portfolio of assurance solutions and services that help DSPs meet business and customer expectations while providing sophisticated features that improve service and network operations efficiency. These integrated solutions provide visibility of the actual customer experience and its relation to the health of telecom, IT, and IP network and services, and automatically trigger incident and problem management processes to handle any customer, service, or network issues.

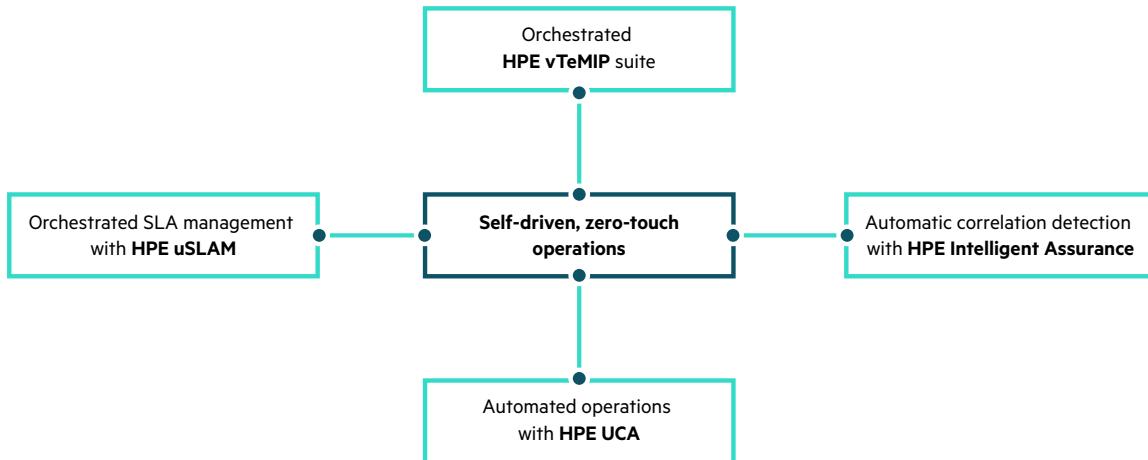


FIGURE 8. HPE OSS Assurance—self-driven, zero-touch operations

HPE OSS Assurance solutions is a rich set of software and services:

- A software portfolio that fits customer's innovative technology requirements
- A consulting-led approach, delivered by HPE Business Transformation Services, to help translate your strategic drivers to measurable business outcomes
- Design, implementation, and support services, delivered by HPE Pointnext Services professionals all over the world

HPE OSS Assurance portfolio is proposing a set of applications to address automation and zero-touch Network Operations Center (NOC) operations at several levels—resource, service, and customer.

COMMUNICATIONS AND MEDIA SOLUTIONS, HEWLETT PACKARD ENTERPRISE

HPE Communications and Media Solutions is dedicated to creating vertical solutions for the communications and media industry. With over 30 years of experience in the industry, we have over 50 solutions, over 1500 active contracts, and more than 300 telco customers in 160 countries, we provide software and services that enable your digital transformation, automate your operations, and help you grow your business with innovative cloud-native network solutions and digital, 5G-ready services.



ABOUT HEWLETT PACKARD ENTERPRISE

Hewlett Packard Enterprise is the global edge-to-cloud platform-as-a-service company that helps organizations accelerate outcomes by unlocking value from all of their data, everywhere. Built on decades of reimagining the future and innovating to advance the way people live and work. HPE delivers unique, open and intelligent technology solutions, with a consistent experience across all clouds and edges, to help customers develop new business models, engage in new ways, and increase operational performance.

LEARN MORE AT

hpe.com/dsp/transform

Make the right purchase decision.
Contact our presales specialists.



Chat



Email



Call



Get updates

© Copyright 2018, 2020 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Google is a trademark of Google LLC. Intel Xeon is a trademark of Intel Corporation in the U.S. and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries. All third-party marks are property of their respective owners.

a00045920ENW, March 2020, Rev. 1