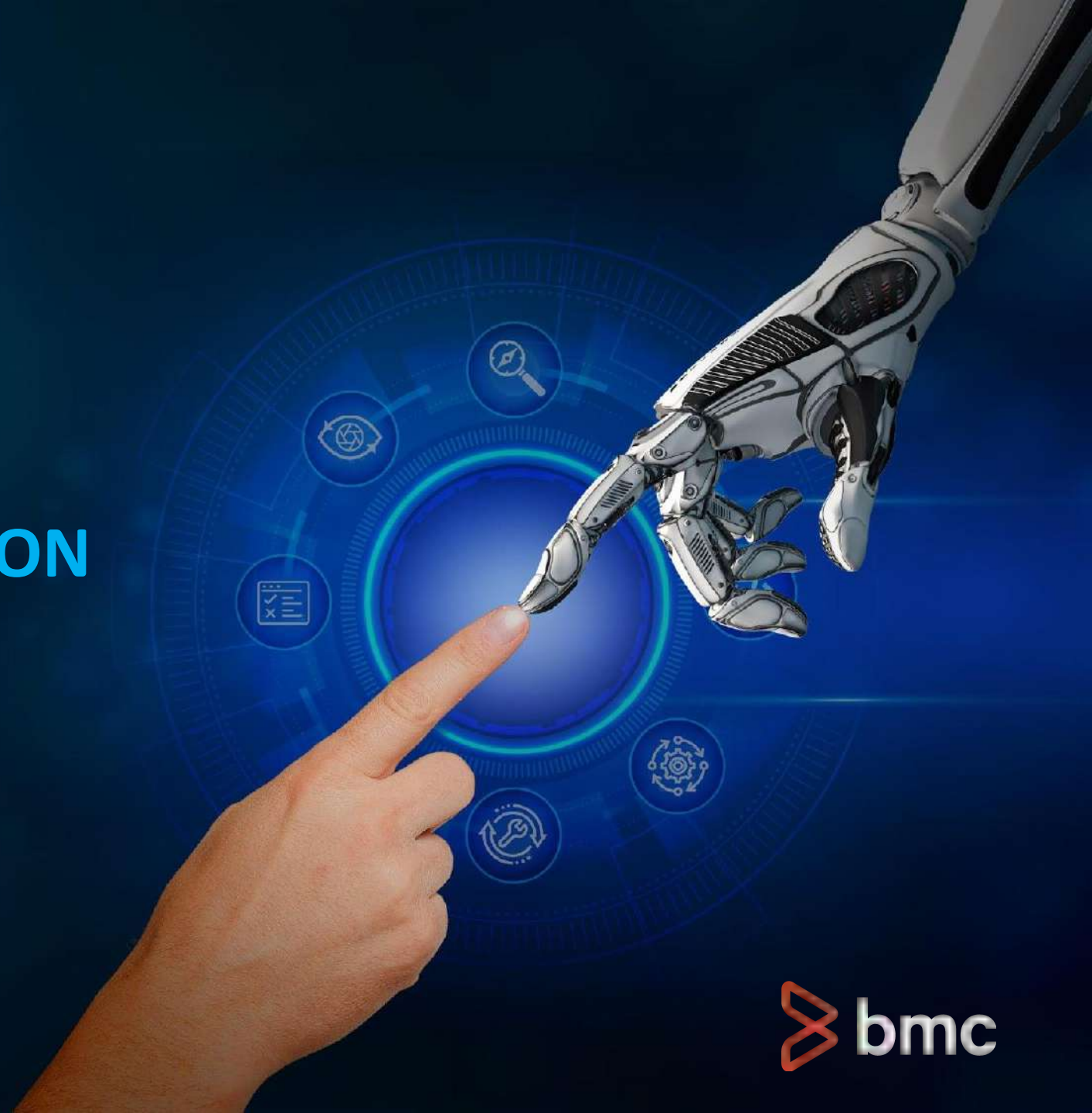
bmc helix

BMC HELIX REMEDIATE
CUSTOMER PRESENTATION



August 2020

bmc

LEGAL NOTICE

The information contained in this presentation is the confidential information of BMC Software, Inc. and is being provided to you with the express understanding that without the prior written consent of BMC, you may not discuss or otherwise disclose this information to any third party or otherwise make use of this information for any purpose other than for which BMC intended.

All of the future product plans and releases described herein relate to BMC's current product development considerations, which are at the sole discretion of BMC and are subject to change and/or cancellation at any time. BMC cannot and does not provide any assurance as to whether these plans will result in any future releases of the nature described. These future product plans should not be viewed as commitments on BMC's part and thus should not be relied upon in customer purchase decisions.

Taming the Tech Tsunami

Multi-Cloud

Multi-Cloud becomes a reality

Multi-Device (IoT)

IoT gets down to business

Multi-Channel

Omni-Channel Experience takes center stage

DevOps

DevOps is the new norm

Big Data

Data is the new oil

Cognitive Automation Key To Address This Complexity

Turn Your Unknowns to Knowns

Unknown Assets Cloud & On-Prem	Know your Assets Cloud & On-Prem
Unknown Events & Alerts	Know all Events & Alerts
Unknown Vulnerabilities	Know Your Vulnerabilities
Unknown Spend	Know Your Spend
Unknown Usage	Know Your Usage
Unknown Issues	Know Issues Before the Customer

Re-imagine Service Experience

TODAY

Human Driven

Manual | **Inaccurate** | **Expensive**

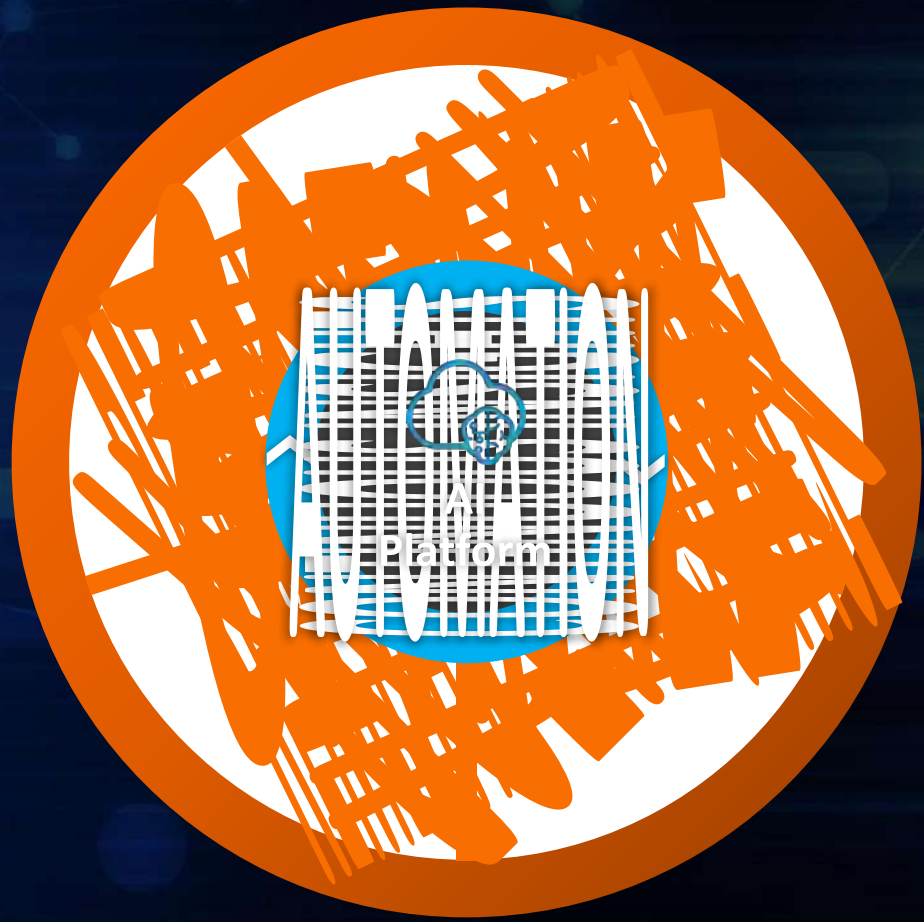
TOMORROW

Augmented Intelligence

AI/ML | **Chatbots** | **RPA Bots**

Convergence of "Service and Operations" Experience

"Industry First Integrated ITSM + ITOM Platform Powered by AI/ML"



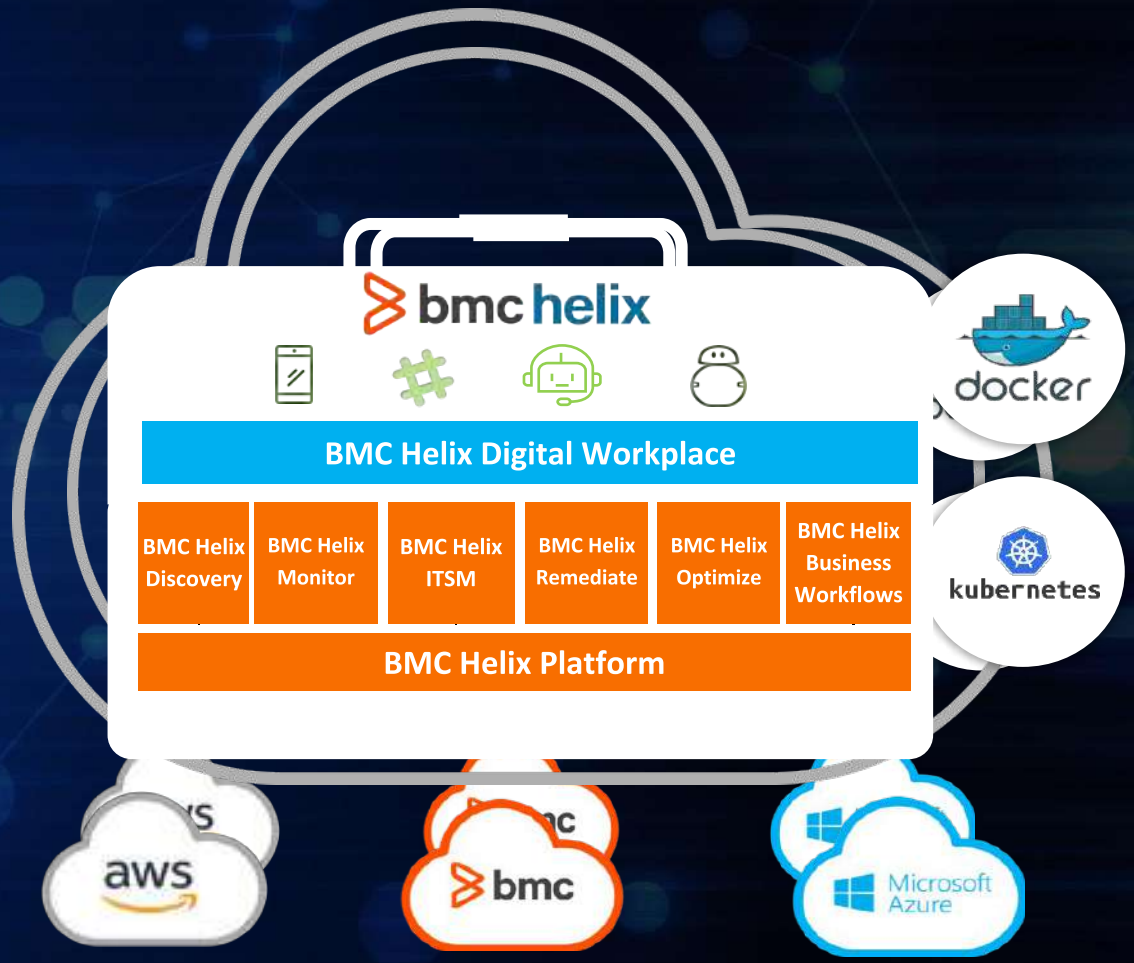
BMC's Journey to Helix

Industry First End-to-End Platform for "Service and Operations" Experience

Remedy Service Management Suite

TrueSight Suite

ITSM & ITOM



Service and Operations Experience

Trends Impacting IT Operations

By 2025, 80% of enterprises will move entirely to cloud

Infrastructure and operations is now a broker of services

Risk is now linked to business outcomes

Focus on threat detection and response

Investment in security skills and governance tools

Source: Gartner: Top 7 Security and Risk Management Trends 2019;
Gartner: Top 10 Trends Impacting Infrastructure and Operations in 2018

Challenges of Current State

Patching Takes Too Long

- 84 days to patch, on avg
- 30 days to exploit
- 54 day window of vulnerability

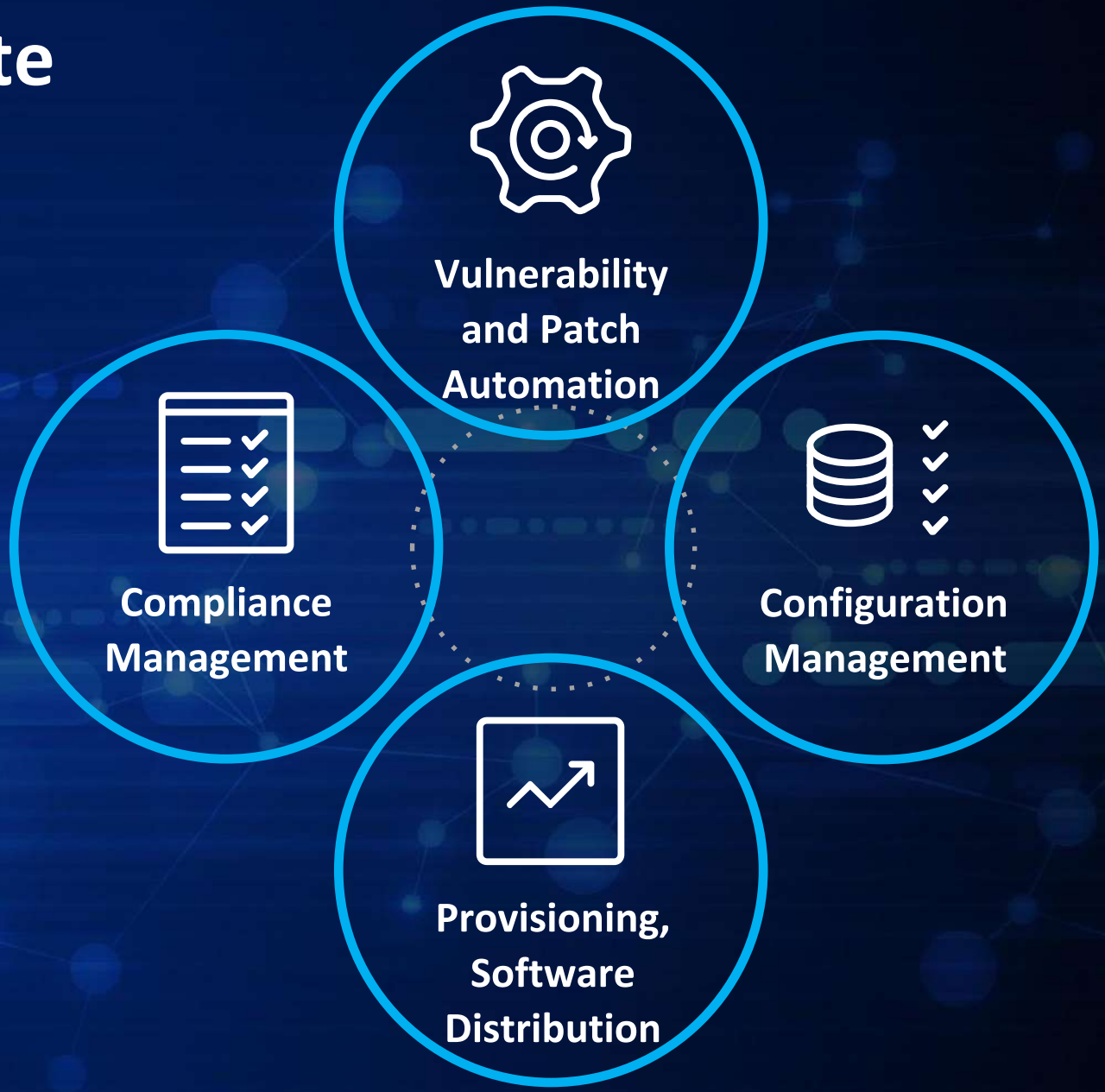
Crushing Volume of Vulnerabilities

- Over 18K new vulnerabilities in 2019
- 99% of exploited vulns known > 1 yr
- SecOps gap
- Manually intensive
- Talent shortage

Concerns over Public Cloud Security

- 93% very worried
- 91% use public cloud
- 1 billion records exposed
- #1 cause of cloud security failures = misconfiguration

Desired State



HOW BMC HELIX REMEDIATE CAN HELP

BMC Helix Remediate

BMC Helix Remediate is a set of solutions which automate the security and compliance of your entire hybrid IT footprint, including on-prem servers, networks, and public cloud IaaS and PaaS resources, to remove bottlenecks, increase productivity, and improve security.

BMC Helix Remediate – Vulnerability Management

VALUE DIFFERENTIATOR

Integration with Vulnerability Scanners

Analysis and Mapping to Assets and Patches

Set Automated Remediation Based on Priorities

What BMC Impacts:

- Integration with leading vulnerability scanners (Tenable, Rapid 7, Qualys) with auto import of scan files
- Use of advanced analytics to map vulnerabilities to assets, determine patches or configuration changes needed,
- Prioritizes remediation based on severity, services exposed, risk scoring
- Integration with ITSM change management
- Ease of use features including vulnerability noise reduction, actionable dashboards with drill down and remediation capability, visibility to vulnerabilities on unmapped assets , exception management, vulnerability tagging

Why This Matters :

- 58% of organizations suffered a breach in the past year, and over 41% exploited a software vulnerability
- Average cost of data breach $3.9 M
- Vulnerabilities grow in number (16K+ new ones in 2018) and automated analysis and remediation is needed
- Ease of use features allow more vulnerabilities to be closed in less time with less labor

BMC Helix Remediate – Simplified Patching

VALUE DIFFERENTIATOR

Greater Speed and Ease-of-use

Visibility to Patch Status and Missing Patches

Automated Remediation

What BMC Impacts:

- Simplified patching for extreme ease-of-use and rapid deployment of patches to become more secure in less time
- Patch based on policies you set for greater speed and reduced manual effort

Why This Matters :

- Visibility to overall security patch status, missing patches, vulnerabilities to be remediated
- One BMC customer (major Canadian bank) used automation to reduce patch deployment time from 2 weeks to less than one day

BMC Helix Remediate – Cloud Security

VALUE DIFFERENTIATOR

Regulatory Compliance

Automated Remediation

Application-Centric Security

What BMC Impacts:

- Automatically identify insecure configurations of cloud IaaS/PaaS resources
- Extensive OOTB policy library (CIS, PCI DSS, GDPR, and more) and support for custom policies
- Take automated corrective action and document the process in ITSM

Why This Matters :

- Cloud service providers are not responsible for security of the content clients place in the public cloud – BMC Helix Cloud Security can help
- Automated corrective action saves labor, automates compliance with regulations and policies, replicates best practices for higher quality, increases productivity

BMC Helix Remediate – Discovery Integration

VALUE DIFFERENTIATOR

Blind Spot Detection

Expanded Visibility to Vulnerabilities Requiring Remediation

Automated Remediation

What BMC Impacts:

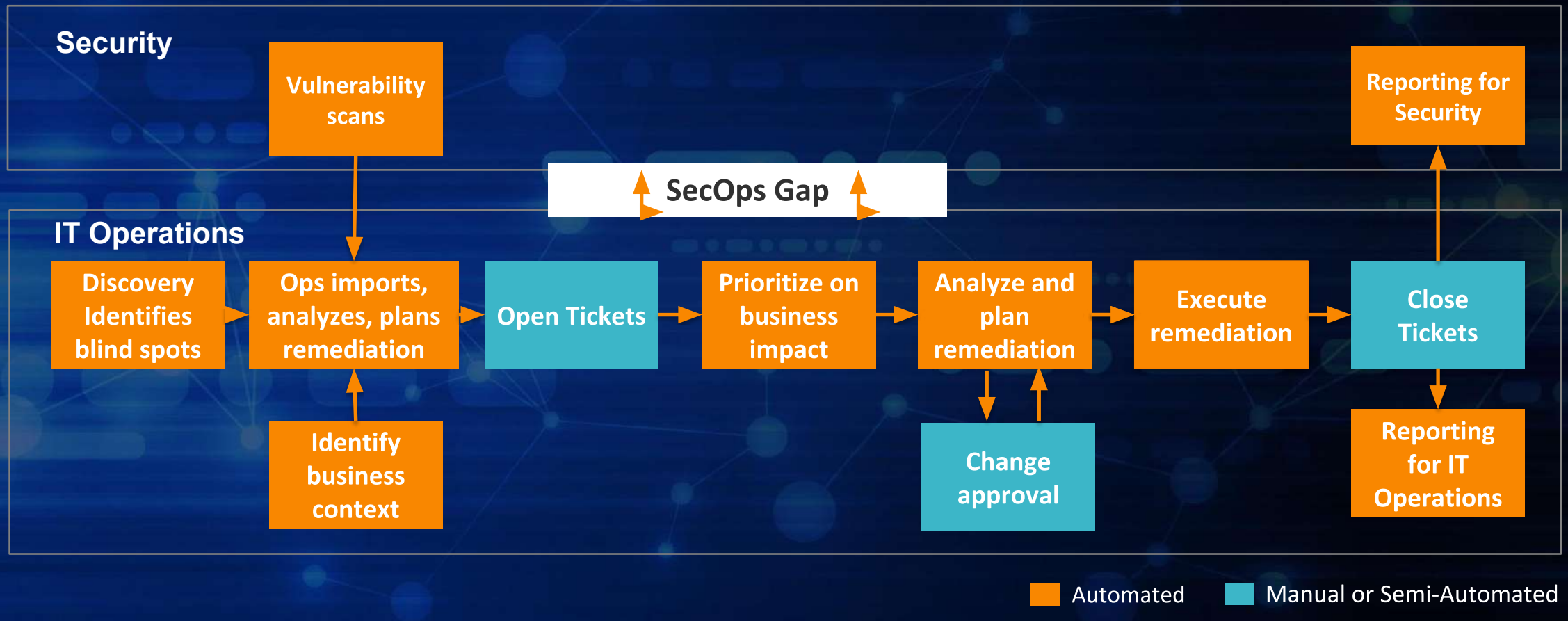
- Visibility to assets missed by vulnerability scanners (blind spots)
- Scan of additional assets detected expanded view of vulnerabilities to be remediated

Why This Matters :

- Typically 10-15% of servers are missed by vulnerability scanners (lack of permissions, dev environments, other)
- Scans of assets in blind spots can be implemented to expand list of vulnerabilities requiring remediation

BMC Helix Remediate – Discovery and ITSM Integration

Vulnerability Management with Automated End-to-end Change Management



BMC HELIX REMEDIATE CAPABILITIES

BMC Helix Remediate

BMC Helix Vulnerability Management

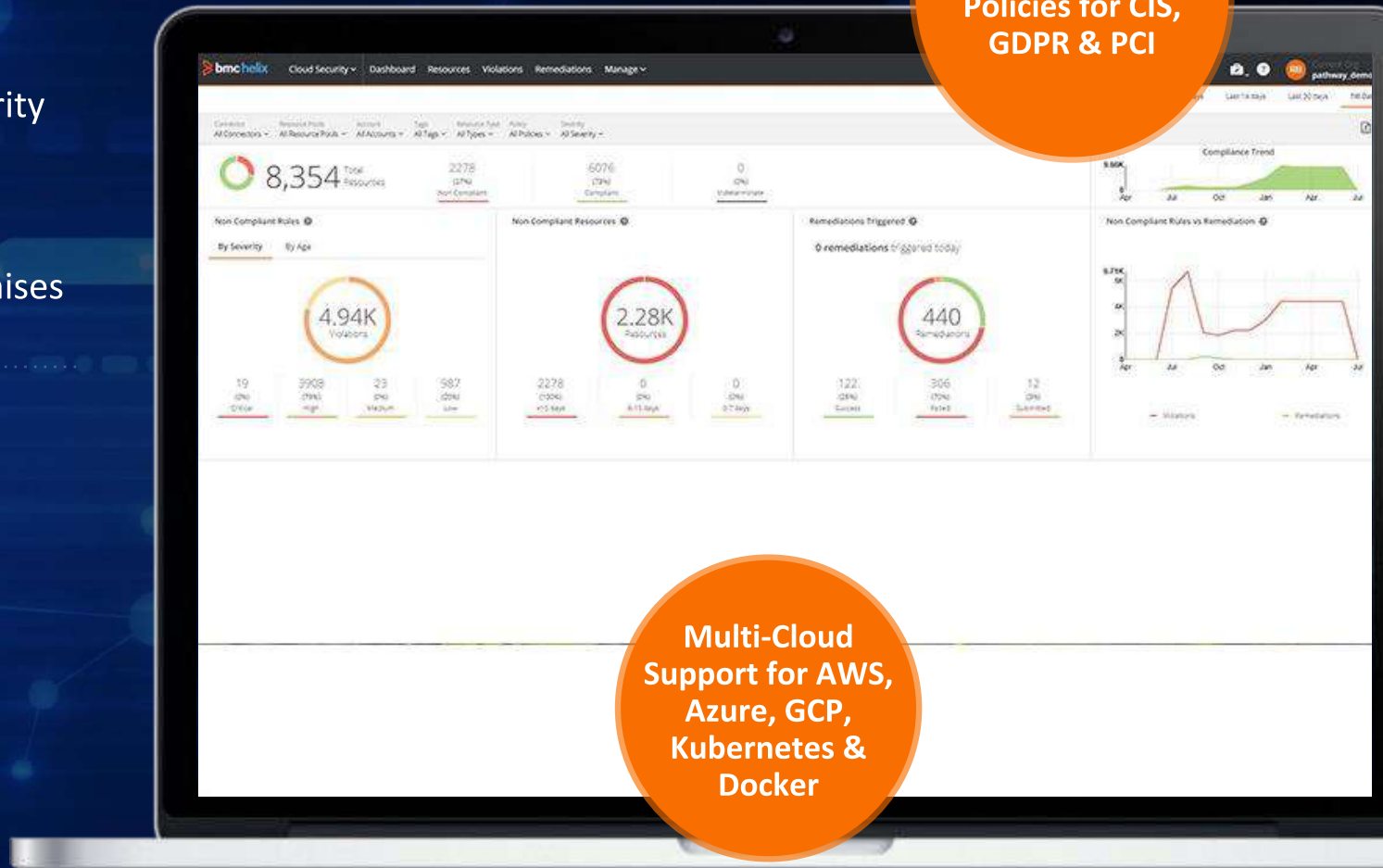
Analytics and automation to rapidly remediate security vulnerabilities.

Simplified patching for ease-of-use and quick remediation of security vulnerabilities both on-premises and in the cloud.

BMC Helix Cloud Security

Automated security testing and remediation of misconfigured cloud resources

Fix with automated actions while orchestrating the process in ITSM (Change and Incident Management)



BMC Helix Vulnerability Management

Vulnerability Management

Ingest security scans data, view severity, understand business context, and plan remediation of identified vulnerabilities.

Simplified Patching

Policy-based patching and specialized dashboards for real-time visibility to patch compliance by server and policy.

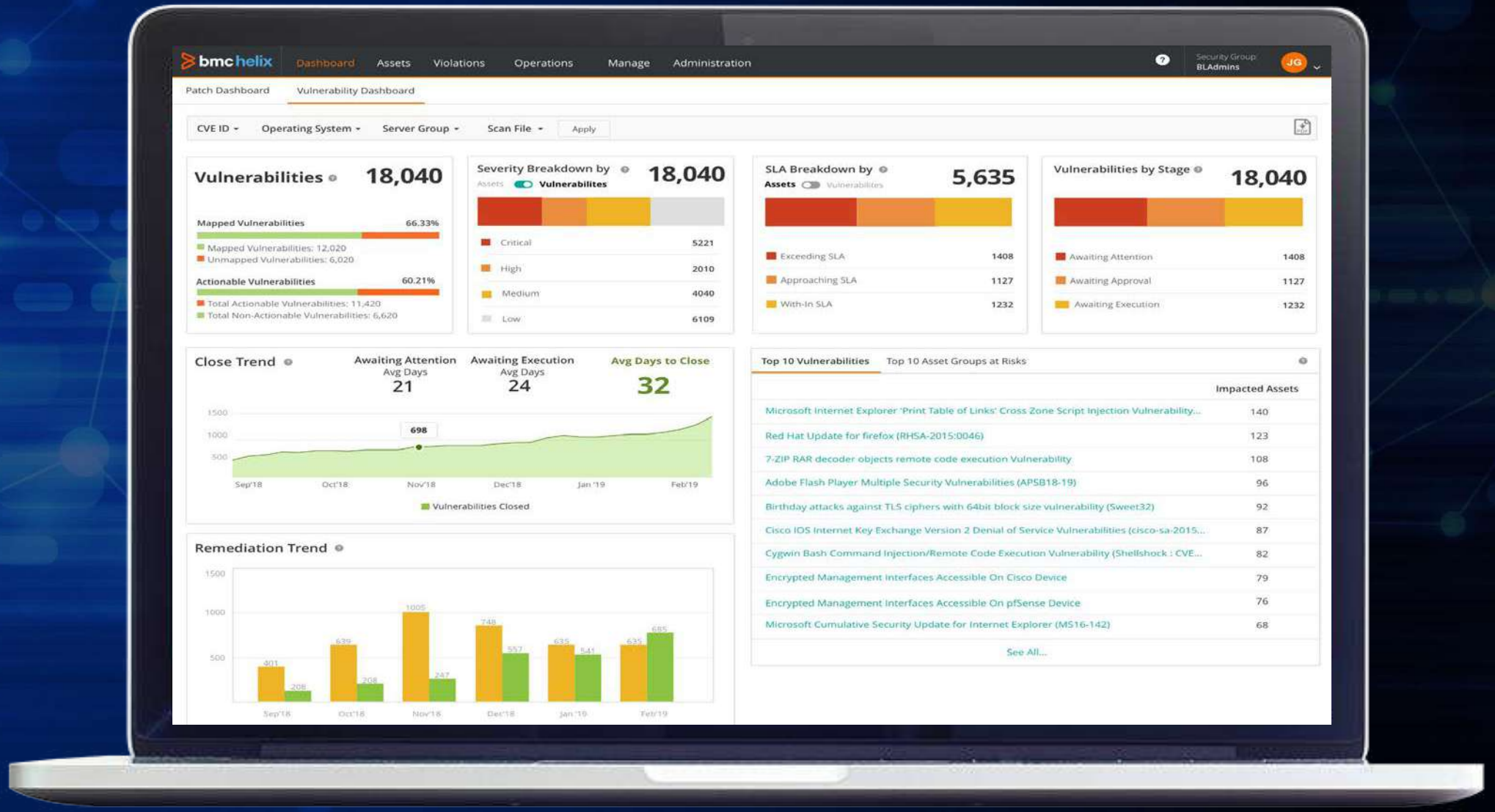
Dashboard Views

Provide views of both security and operational data to help improve communication between teams (close SecOps gap).

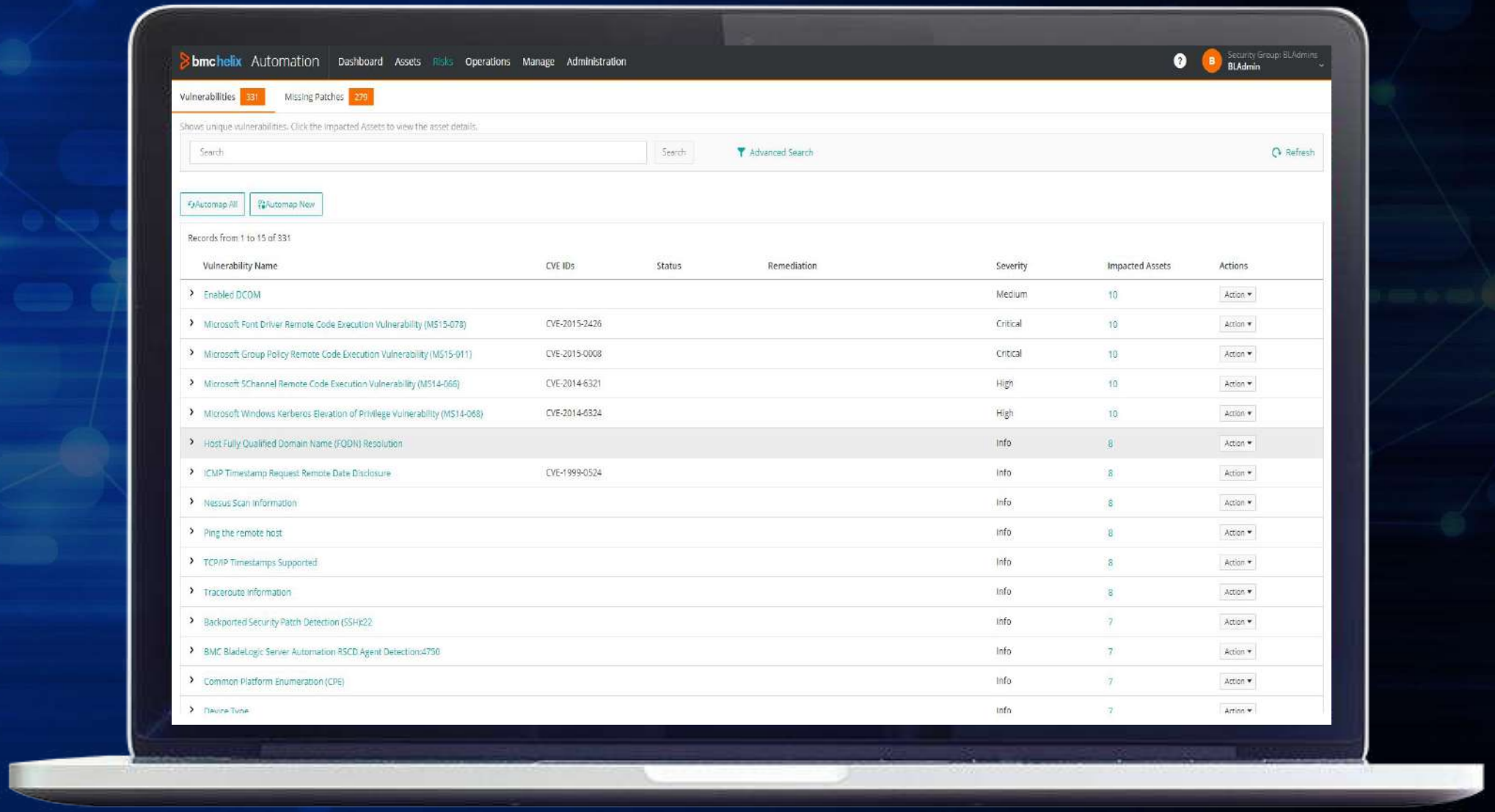
Blindspot Detection

Correlate security scan / discovery information with systems that are being managed. Identify unscanned systems that could pose increased risk to your organization.

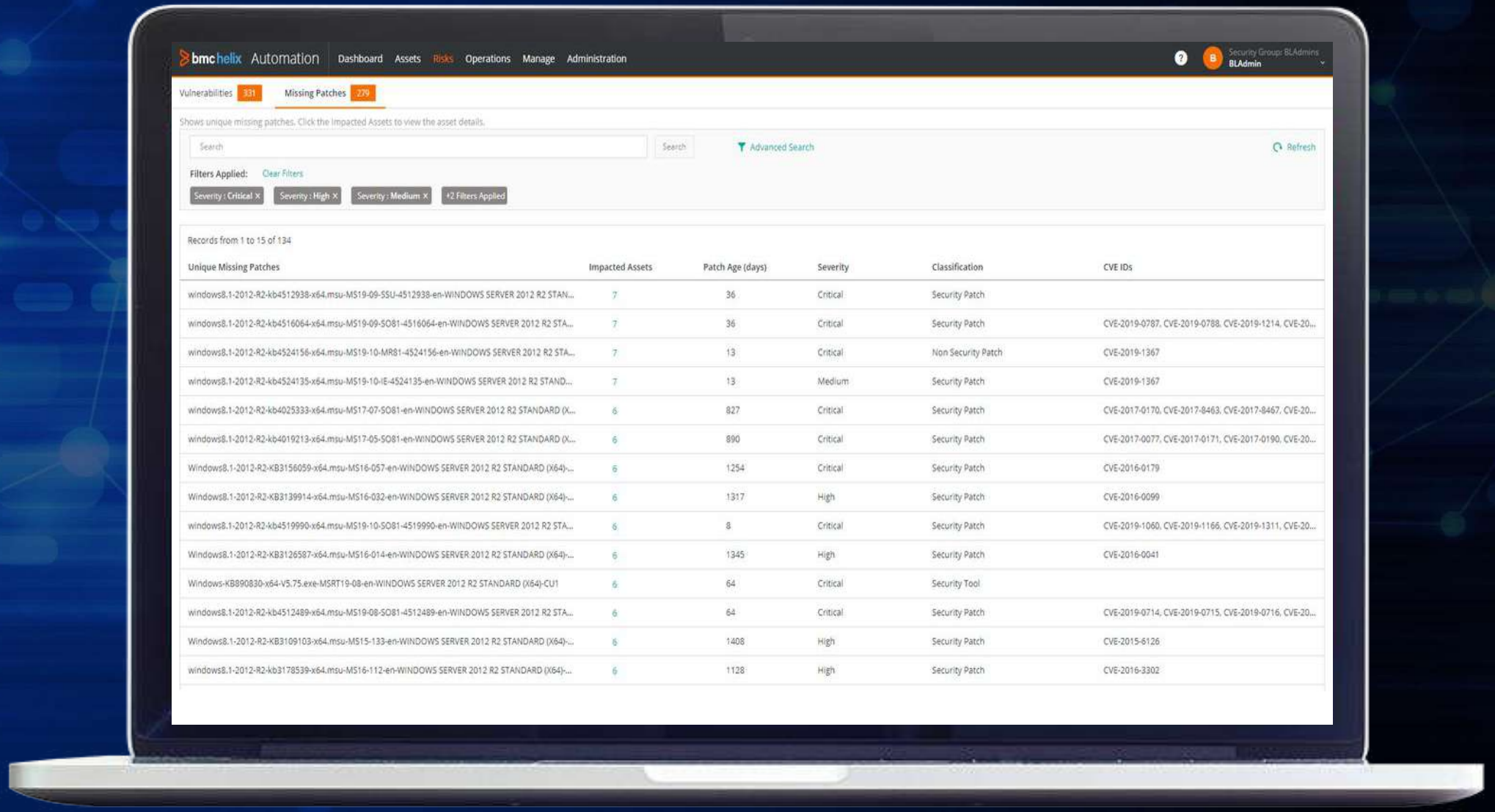
Vulnerability Management Dashboard



Vulnerability Details

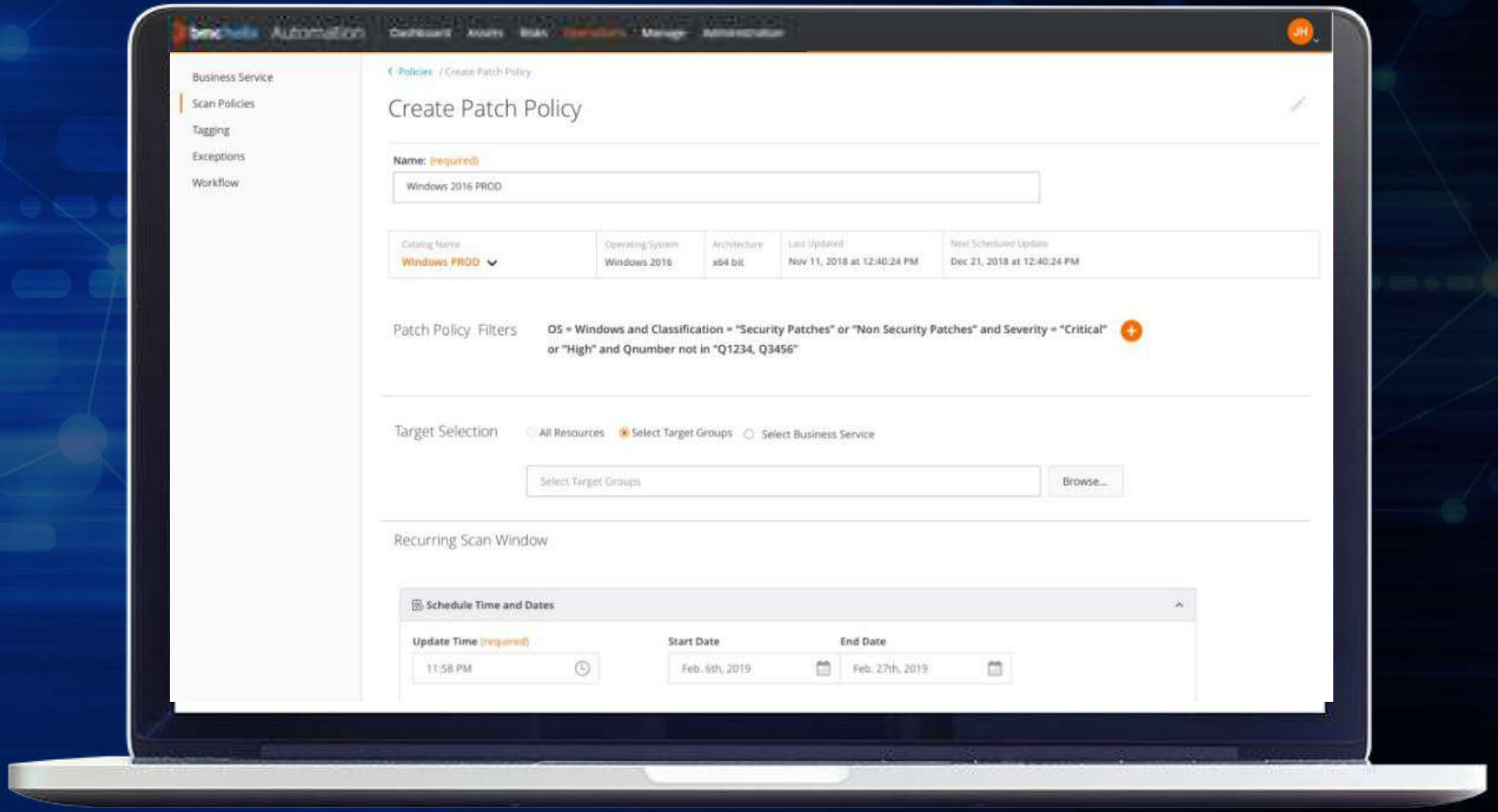


Missing Patches

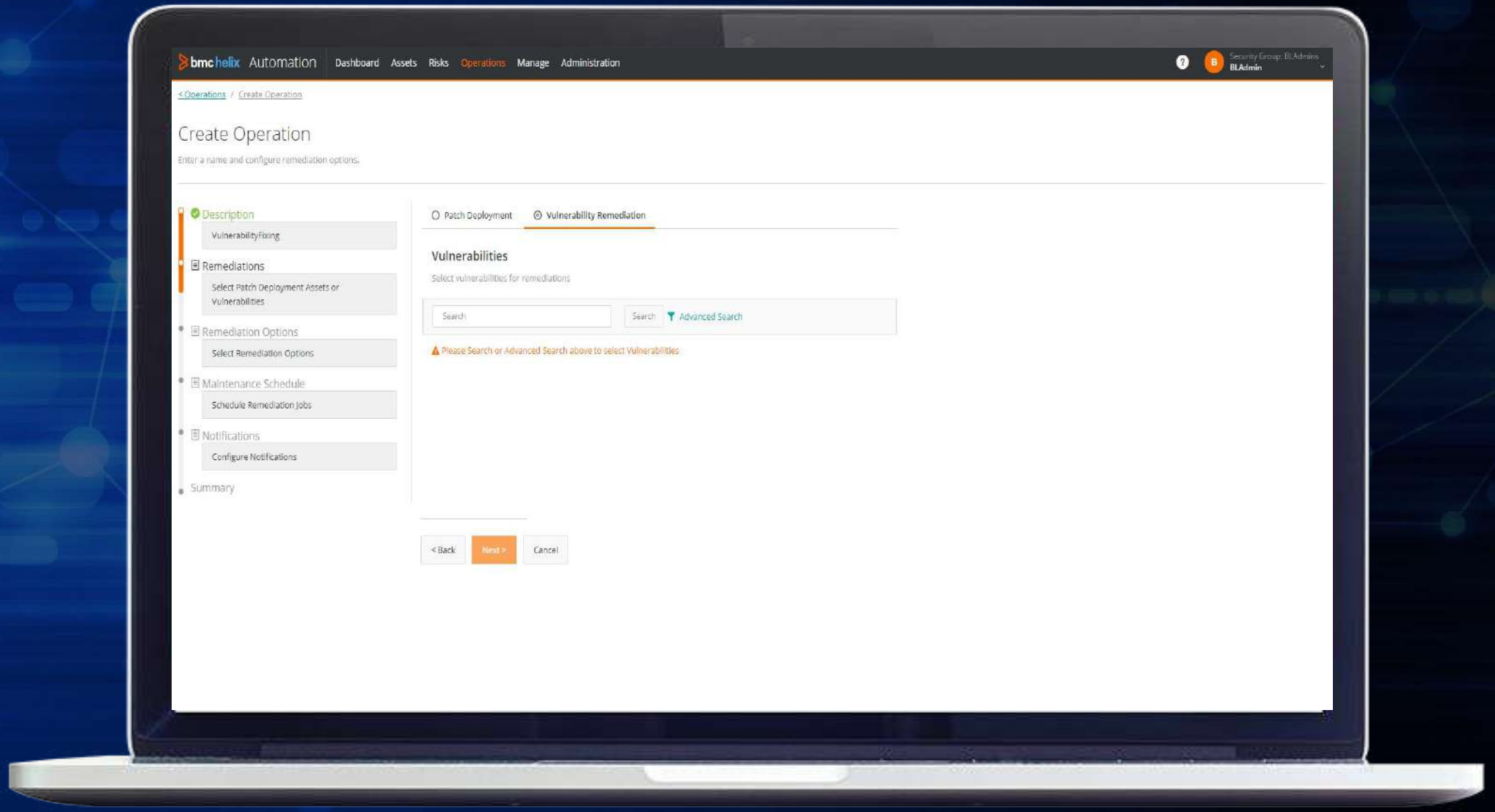


Unique Missing Patches	Impacted Assets	Patch Age (days)	Severity	Classification	CVE IDs
windows8.1-2012-R2-kb4512938-x64.msu-MS19-09-SSU-4512938-en-WINDOWS SERVER 2012 R2 STAN...	7	36	Critical	Security Patch	
windows8.1-2012-R2-kb4516064-x64.msu-MS19-09-SO81-4516064-en-WINDOWS SERVER 2012 R2 STA...	7	36	Critical	Security Patch	CVE-2019-0787, CVE-2019-0788, CVE-2019-1214, CVE-20...
windows8.1-2012-R2-kb4524156-x64.msu-MS19-10-MR81-4524156-en-WINDOWS SERVER 2012 R2 STA...	7	13	Critical	Non Security Patch	CVE-2019-1367
windows8.1-2012-R2-kb4524135-x64.msu-MS19-10-IE-4524135-en-WINDOWS SERVER 2012 R2 STAND...	7	13	Medium	Security Patch	CVE-2019-1367
windows8.1-2012-R2-kb4025333-x64.msu-MS17-07-SO81-en-WINDOWS SERVER 2012 R2 STANDARD (X...	6	827	Critical	Security Patch	CVE-2017-0170, CVE-2017-8463, CVE-2017-8467, CVE-20...
windows8.1-2012-R2-kb4019213-x64.msu-MS17-05-SO81-en-WINDOWS SERVER 2012 R2 STANDARD (X...	6	890	Critical	Security Patch	CVE-2017-0077, CVE-2017-0171, CVE-2017-0190, CVE-20...
Windows8.1-2012-R2-KB3156059-x64.msu-MS16-057-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-...	6	1254	Critical	Security Patch	CVE-2016-0179
Windows8.1-2012-R2-KB3139914-x64.msu-MS16-032-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-...	6	1317	High	Security Patch	CVE-2016-0099
windows8.1-2012-R2-kb4519990-x64.msu-MS19-10-SO81-4519990-en-WINDOWS SERVER 2012 R2 STA...	6	8	Critical	Security Patch	CVE-2019-1060, CVE-2019-1166, CVE-2019-1311, CVE-20...
Windows8.1-2012-R2-KB3126587-x64.msu-MS16-014-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-...	6	1345	High	Security Patch	CVE-2016-0041
Windows-KB890830-x64-V5.75.exe-MSRT19-08-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-CU1	6	64	Critical	Security Tool	
windows8.1-2012-R2-kb4512489-x64.msu-MS19-08-SO81-4512489-en-WINDOWS SERVER 2012 R2 STA...	6	64	Critical	Security Patch	CVE-2019-0714, CVE-2019-0715, CVE-2019-0716, CVE-20...
Windows8.1-2012-R2-KB3109103-x64.msu-MS15-133-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-...	6	1408	High	Security Patch	CVE-2015-6126
windows8.1-2012-R2-kb3178539-x64.msu-MS16-112-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-...	6	1128	High	Security Patch	CVE-2016-3302

Create Patch Policy



Create Remediation Operations



BMC Helix Cloud Security

Regulatory Compliance

Prove regulatory compliance and identify insecure public cloud IaaS/PaaS and container configurations.

Operational Governance

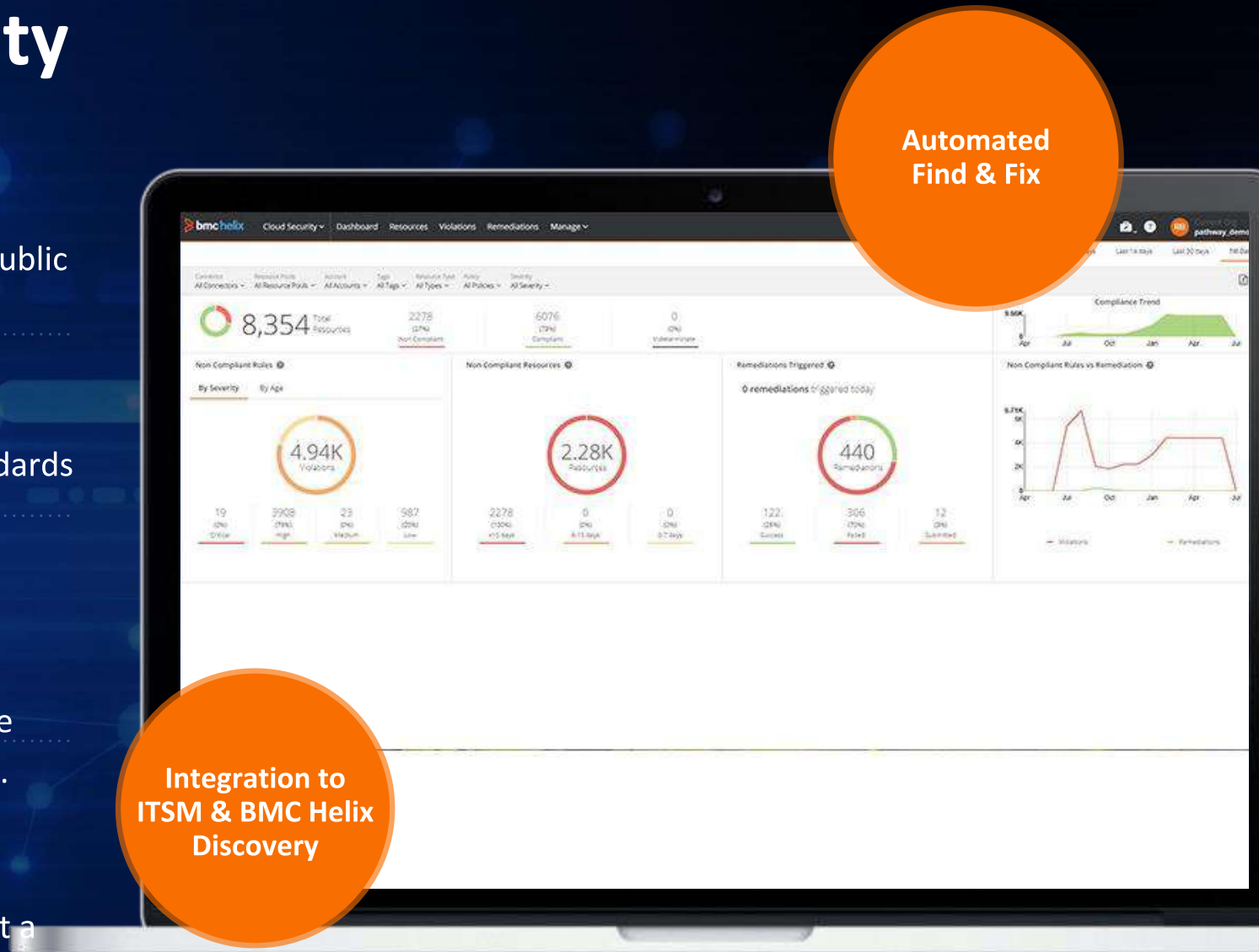
Ensure cloud usage remains within operational standards and best practices.

Automated Remediation

Fix resources with automated actions – no coding required! – while documenting and orchestrating the process in ITSM (Change and Incident Management).

App-Centric Security

With integration to BMC Helix Discovery, you can get a complete picture of resource dependencies within your business services, to manage cloud security by application.



BMC Helix Cloud Security

Regulatory Compliance

- Automatically identify insecure configurations of cloud IaaS/PaaS resources.
- Extensive OOTB policy library (CIS, PCI DSS, GDPR, and more) and support for custom policies.
- Real-time multi-cloud security & compliance mgmt. Intuitive point-and-click UI, to narrow the focus and drill into details.

★★★★½

A well-oiled machine

The stability has been really good...no limits to scalability. More

Managing Director.
IT Consulting

IT Central Station

BMC Helix Cloud Security

Automated Remediation

- Fix IaaS/PaaS resource configurations with automated action – no coding required
- Remediation action is ready-to-use, included with the OOTB policies, as well as support for customization.
- Automated remediation via either UI button click, or by fully automatic self-driving remediation.
- Closed-Loop Security Incident and Change Mgmt.

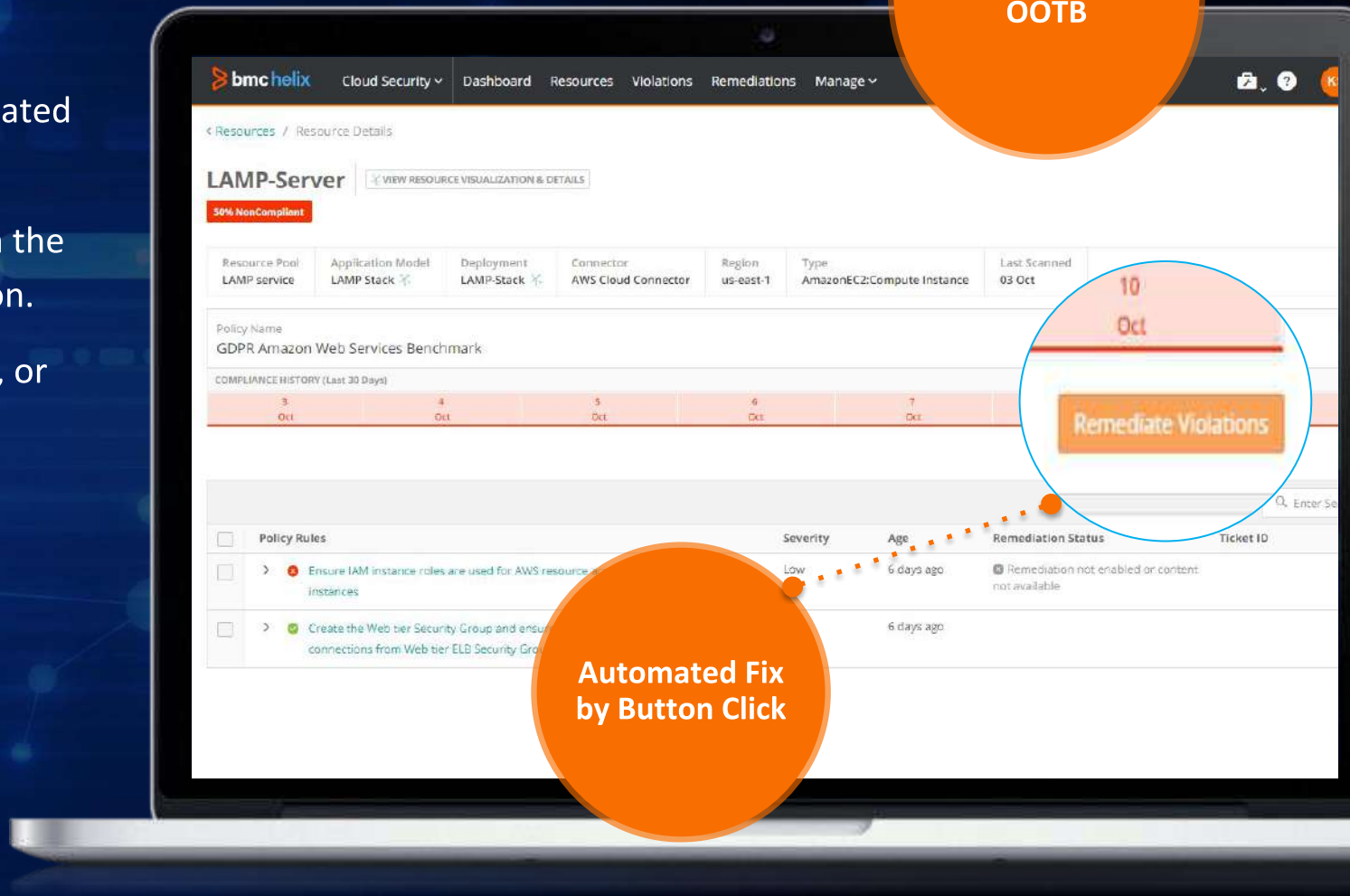
★★★★½

Easy, automated, multi-cloud

A huge time saver...catches things you might have missed...remediate with a click. More

VP of Cloud Operations.
IT Consulting

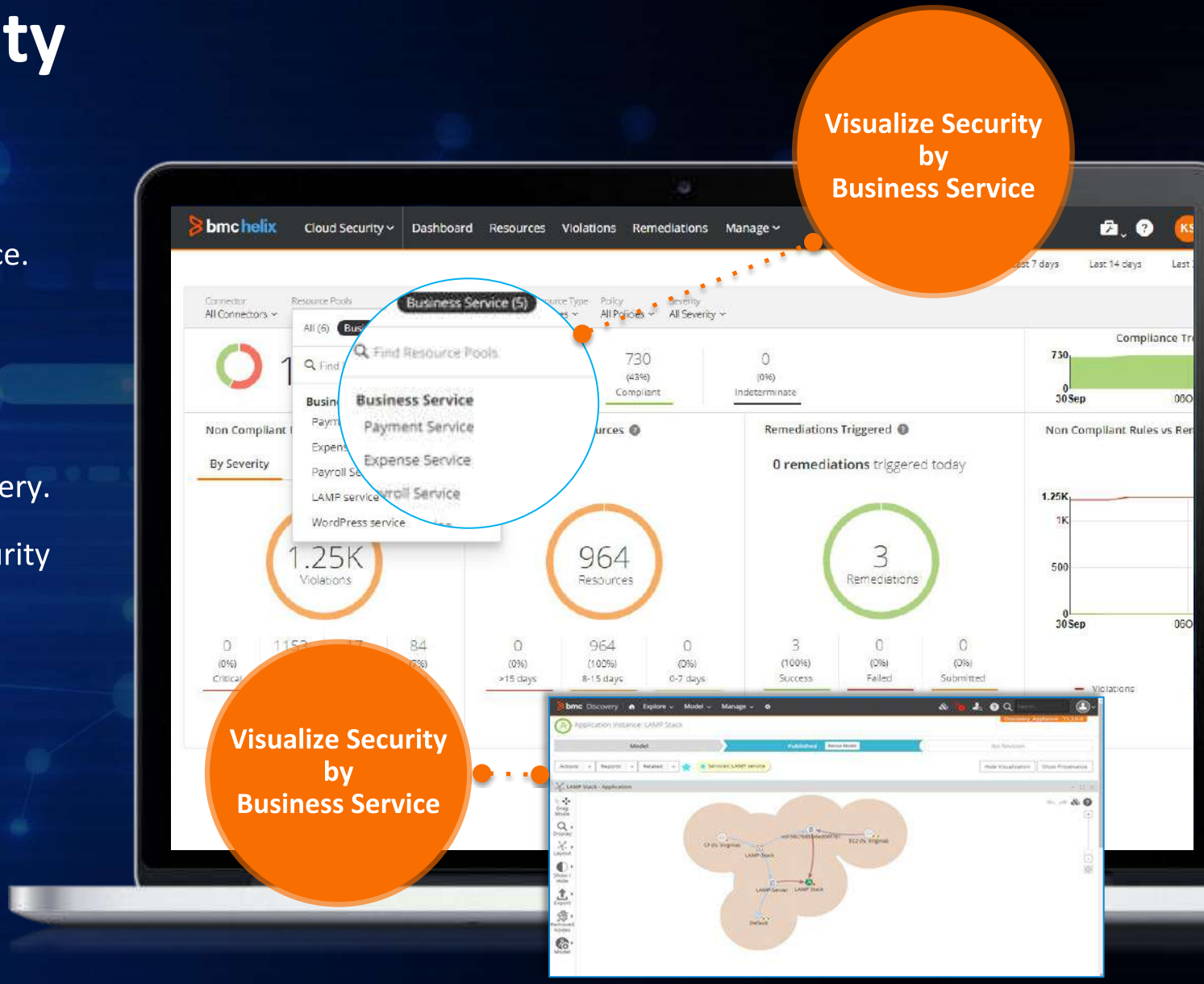
IT Central Station



BMC Helix Cloud Security

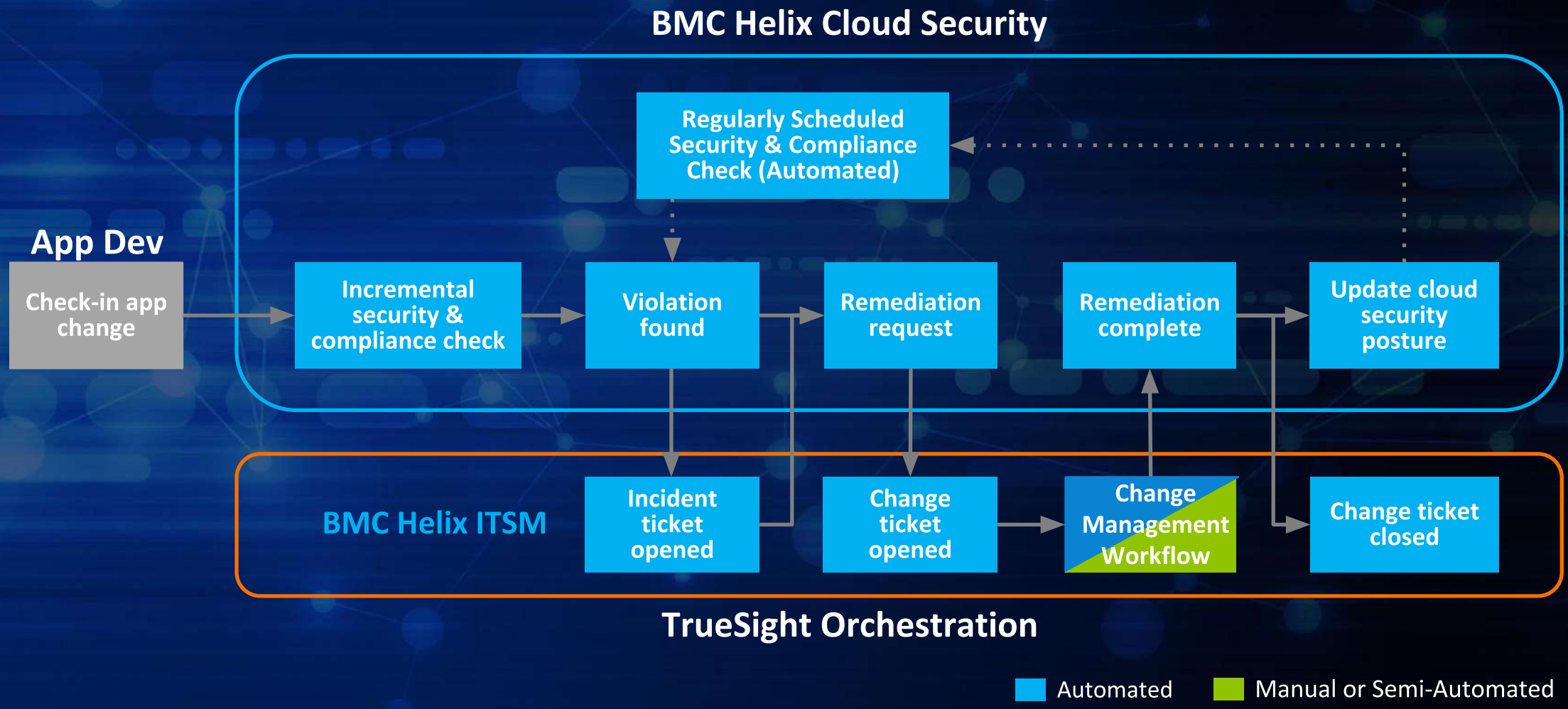
App-Centric Security

- Visualize security posture by app / business service.
- Help developers own and manage the security posture of their apps, while Security maintains centralized governance (e.g., policies).
- Ingest “Business Services” from BMC Helix Discovery.
- Switch seamlessly between BMC Helix Cloud Security and Discovery with single sign-on.



Closed-Loop Security & Compliance Management

BMC Helix Cloud Security Integration with ITSM



Event-Driven Compliance

Event-Driven Compliance is a feature which uses automated policy checks so that customer's AWS cloud accounts achieve nearly continuous, real-time cloud security and compliance posture mgmt. for many of the most popular services

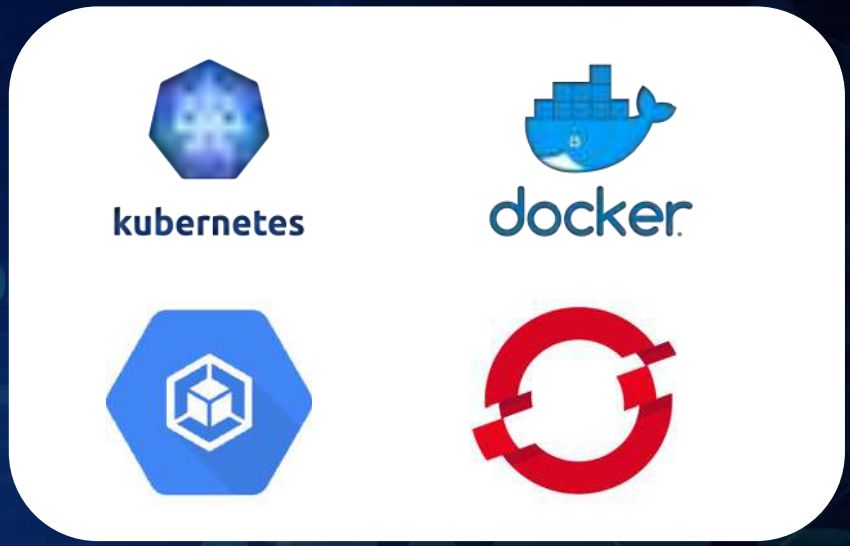
The moment a change is made – add a new resource or modify an existing one – BMC Helix Cloud Security runs an incremental compliance check of that change

EDC can be selected when configuring an AWS connector

Admins can enable auto remediation to further strengthen the benefit of EDC

Container Configuration Security

CIS Docker Benchmark
CIS Kubernetes Benchmark – Master
CIS Kubernetes Benchmark – Worker
Google Kubernetes Engine
RedHat® OpenShift



Full-stack container configuration security

- Cluster, host, daemon, image, container

★★★★½

A well-oiled machine

The stability has been really good...no limits to scalability. More

Managing Director,
IT Consulting

IT Central Station

★★★½☆

Strong container security

A good tool to make sure your containers are safe and sound. More

User,
Manufacturing Company

IT Central Station

★★★★½

Easy, automated, multi-cloud

A huge time saver...catches things you might have missed...remediate with a click. More

VP of Cloud Operations,
IT Consulting

IT Central Station

Cloud Server Security and Compliance

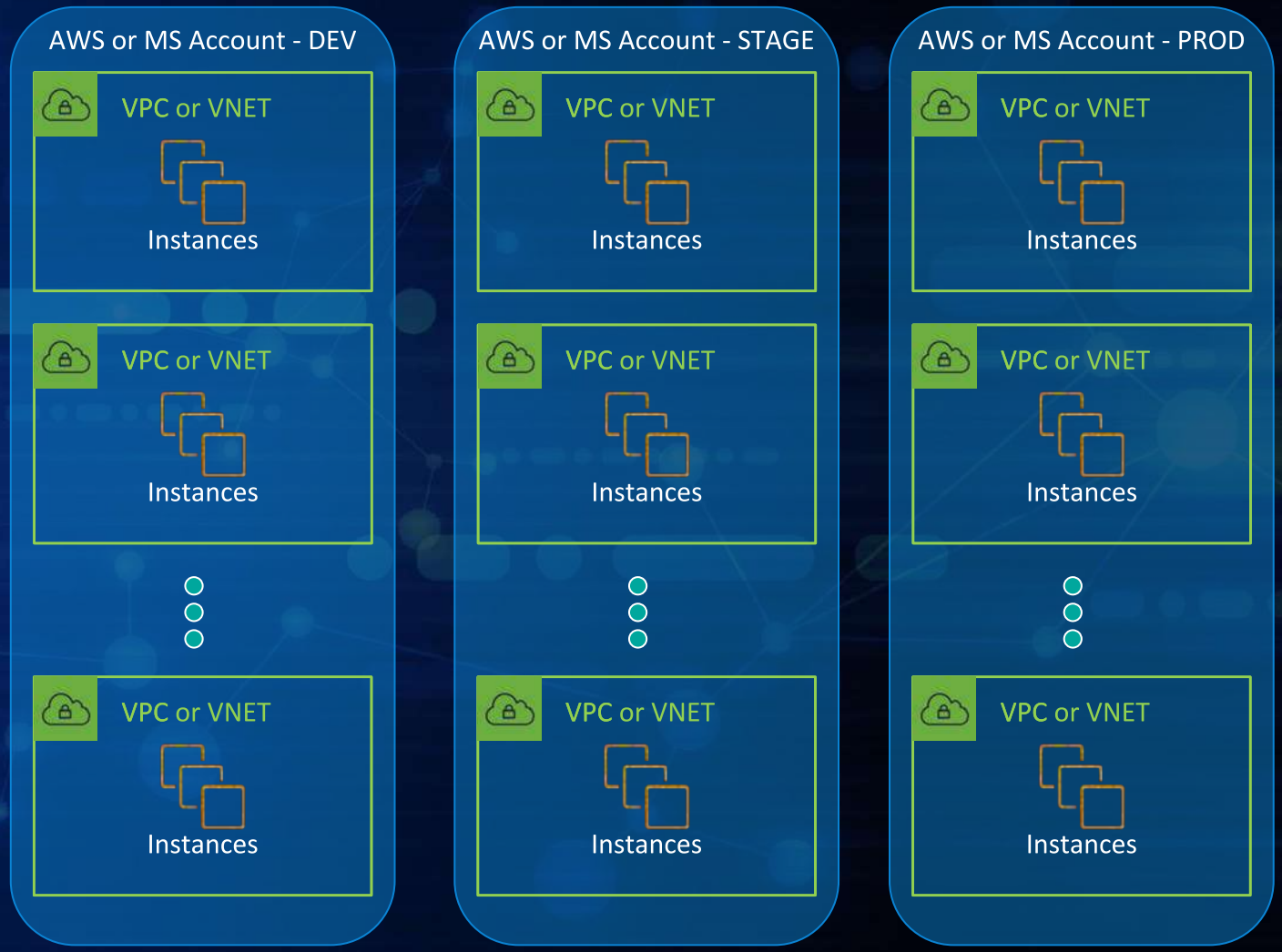
Problem

Manual security and compliance management of AWS EC2 or MS Azure VM instances impedes agility and presents risk

- Manually find every instance
- Manually install a Smart Agent
- Manually enroll into an endpoint mgmt. solution

Solution

- Automated find and enroll every instance into server security mgmt.
- Automated, simplified OS patching
- Automated configuration security
- Common solution for server patching and compliance mgmt., on-prem and in the cloud



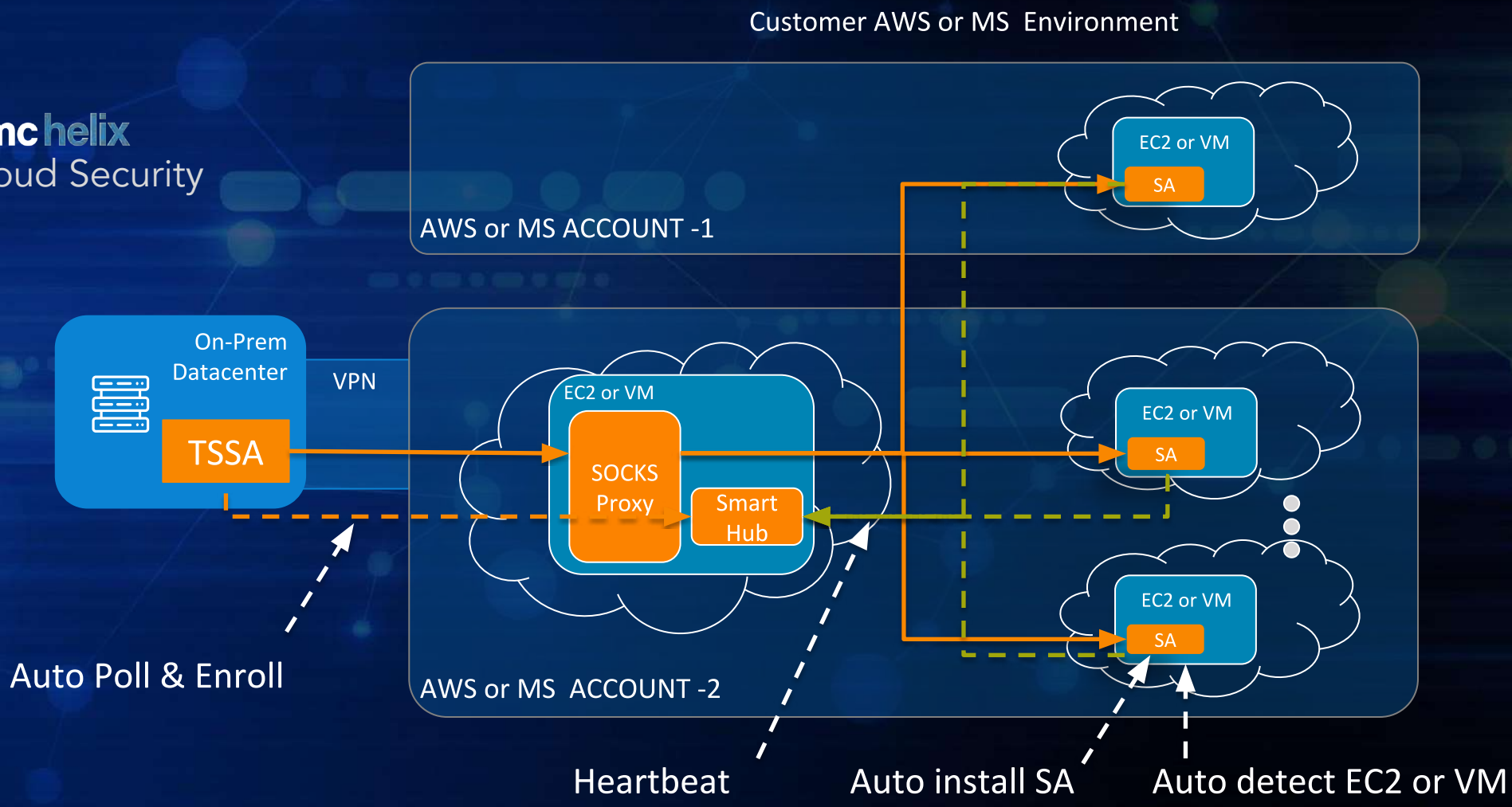
HOW IT WORKS

BMC Helix Cloud Security + TrueSight Server Automation

AUTO

- **DETECT**
- **INSTALL**
- **POLL**
- **ENROLL**

bmc helix Cloud Security



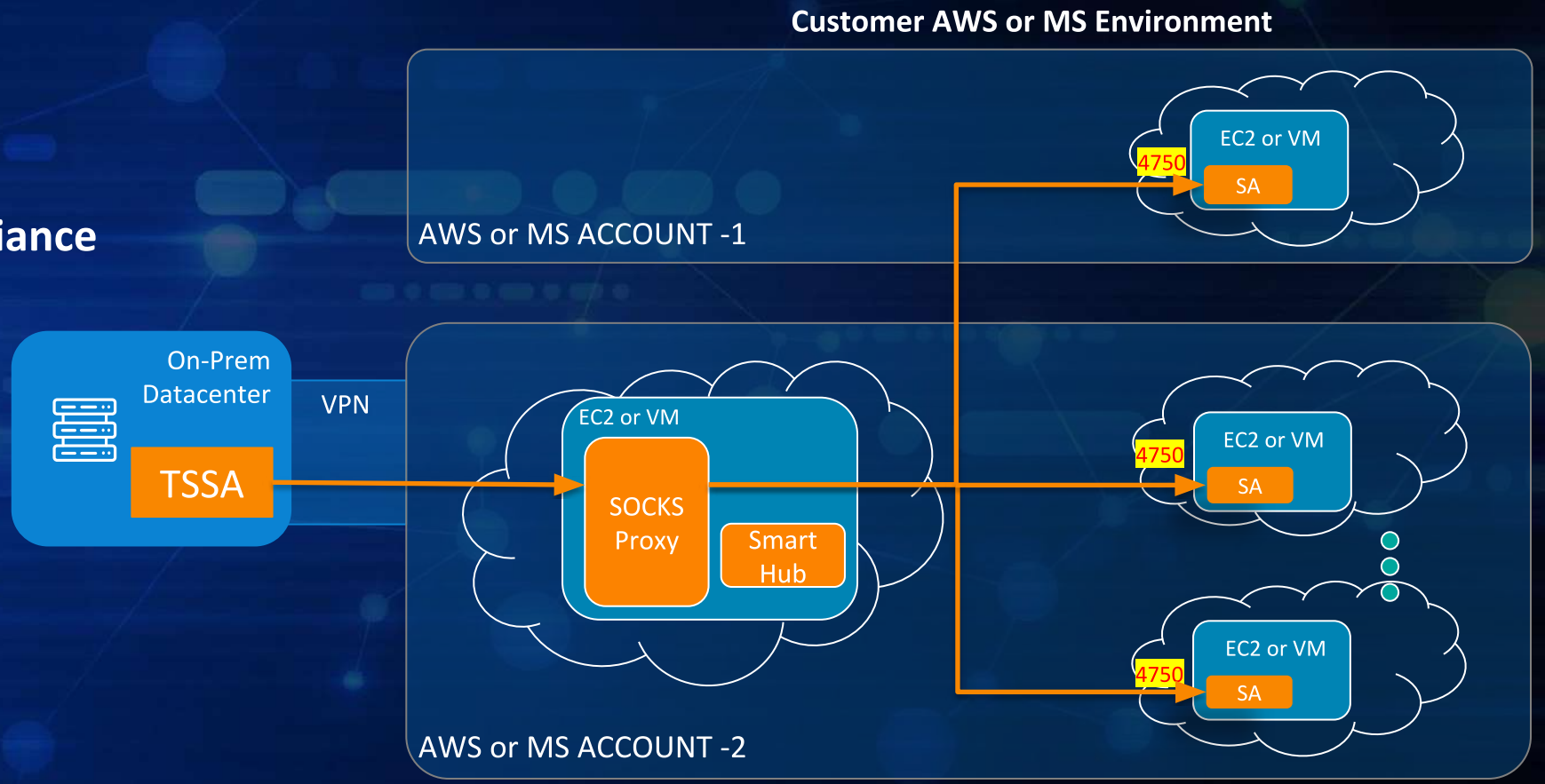
Supported Capabilities

1. Patching
2. OS Compliance
3. Configuration Compliance
4. Vulnerability Management
5. Live Browsing
6. Audit & Drift Detection
7. Software Deployment

AUTOMATED CLOUD SERVER MANAGEMENT - BENEFITS

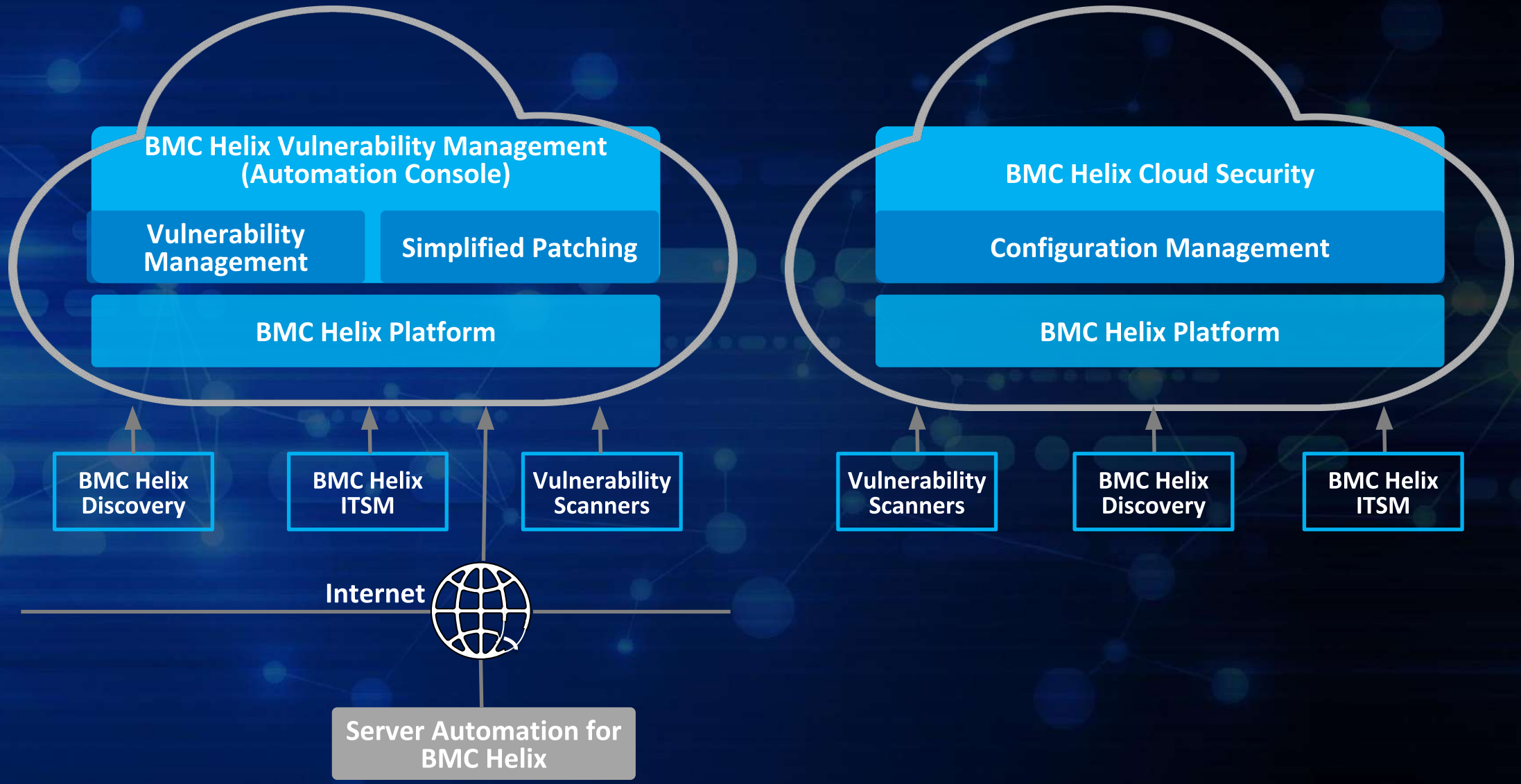
CAPABILITIES

- Patching
- OS Compliance
- Configuration compliance
- Vulnerability mgmt.
- Live browsing
- Snapshot
- Deploy jobs

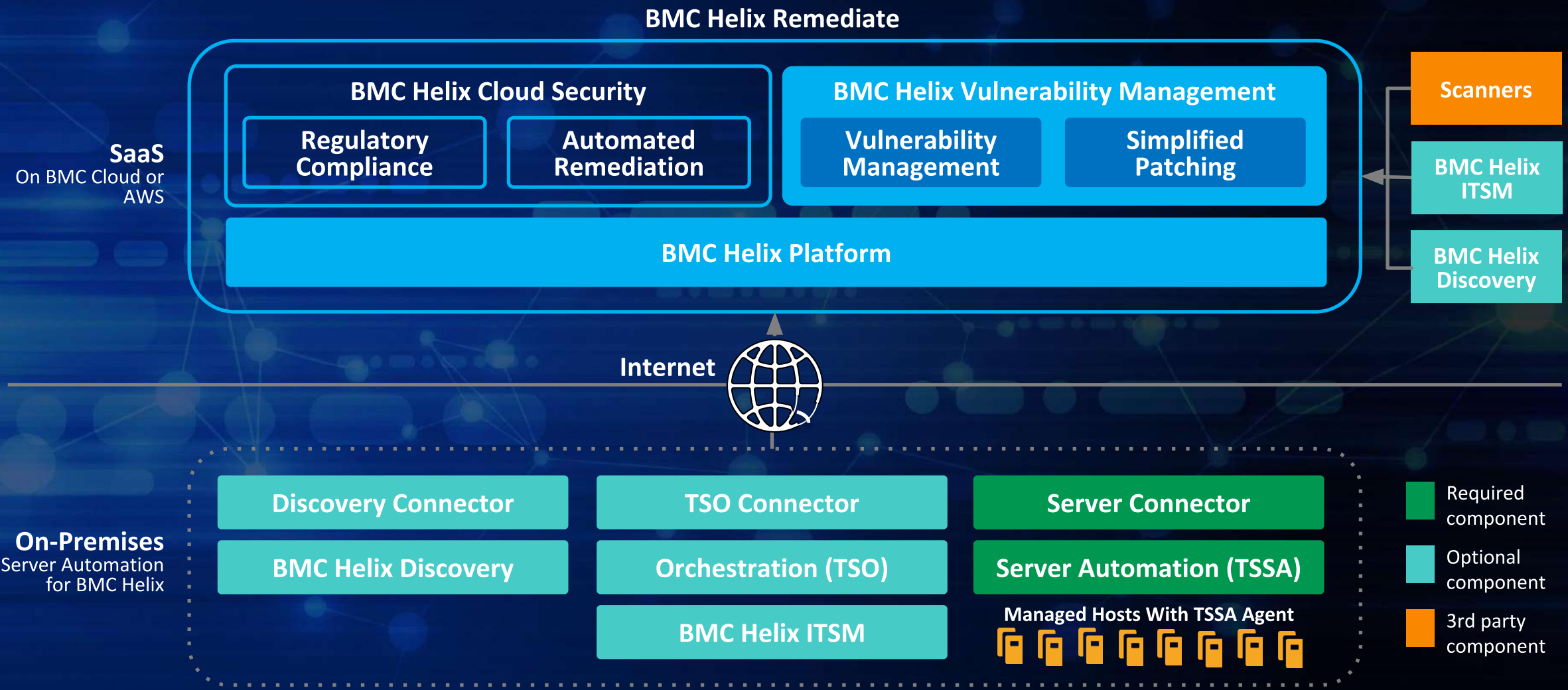


BMC HELIX REMEDIATE DEPLOYMENT CHOICES

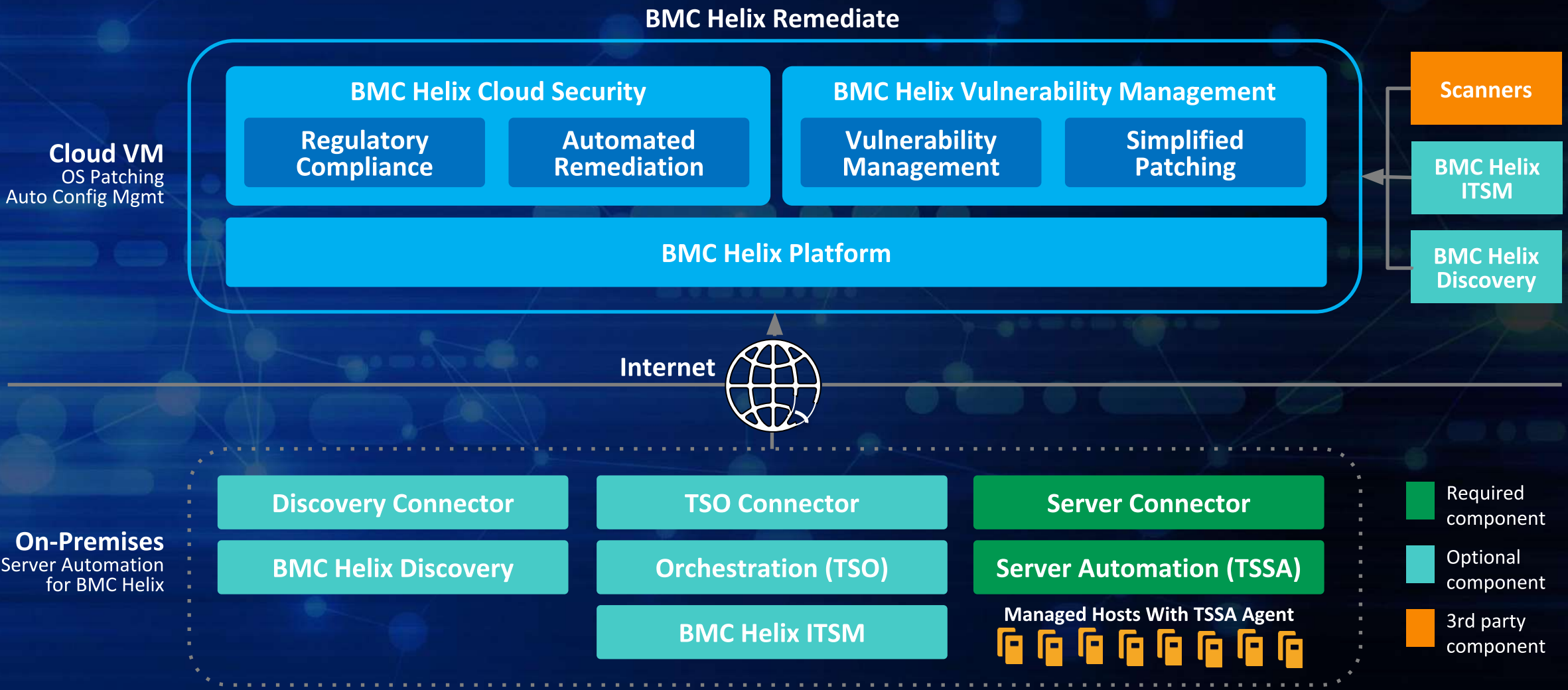
BMC Helix Remediate



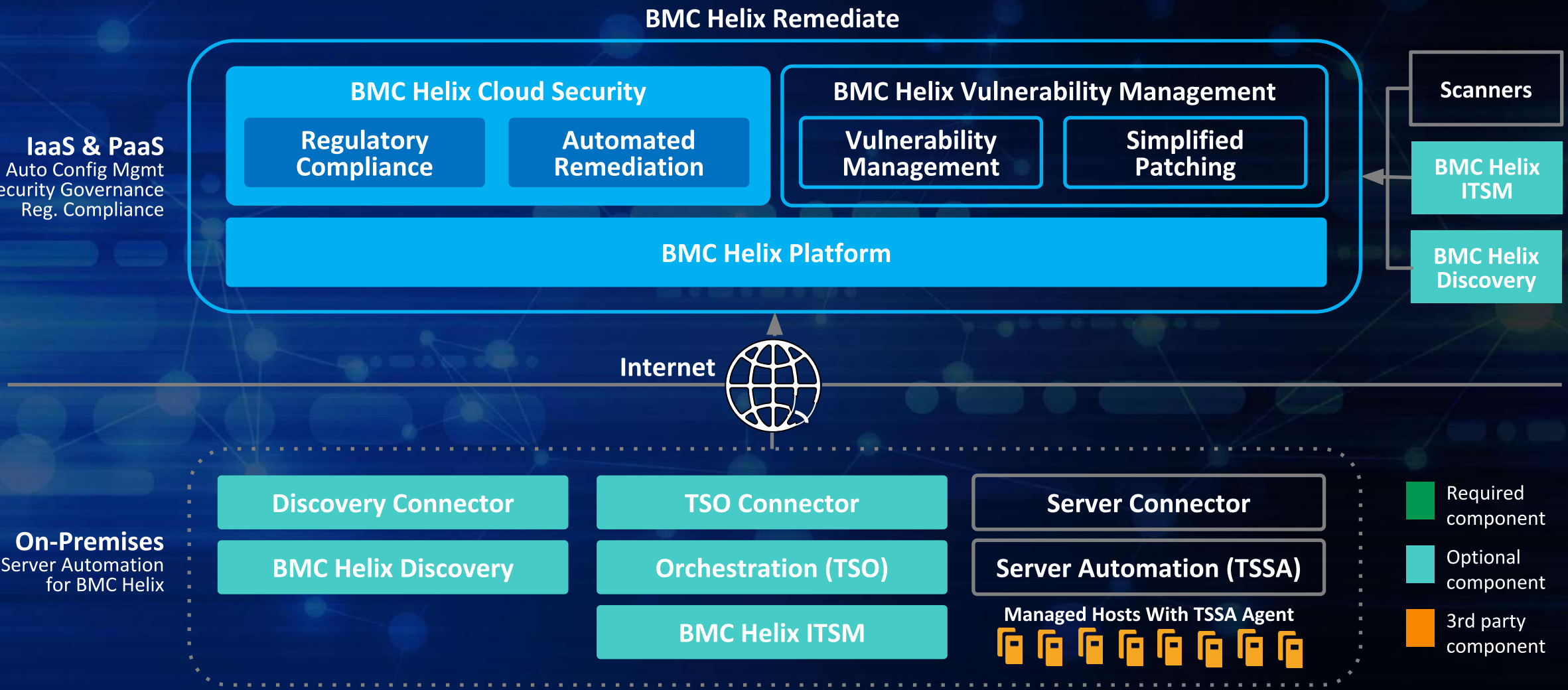
BMC Helix Remediate | On-prem Server Management



BMC Helix Remediate | Cloud Server Management



BMC Helix Remediate | Cloud Configuration Security



CUSTOMER USING BMC HELIX REMEDIATE

Large Canadian Bank

One of Canada's leading integrated financial groups. With more than 23,000 employees they have been recognized as a top employer and innovator.

We have been using BMC automation solutions to manage our servers and security vulnerabilities for several years now, and they've made a huge difference in our organization. These solutions make everyone's life easier, and enable us to better focus on the efforts and activities that bring value to the bank and to customers.

— Leader of Infrastructure Services Integration and VP of IT Operations

About BMC

BMC is a global leader in innovative software solutions that enable businesses to transform into digital for the ultimate competitive advantage. Our Digital Enterprise Management solutions are designed to fast track digital business from mainframe to mobile to cloud and beyond.