Hybrid Cloud Server Management and Compliance

With BMC Helix Remediate

Table of Contents

Summary

Businesses of all sizes use cloud servers to augment their on-prem IT capabilities. Whether on-prem or in the cloud, organizations need a single console from which they can manage security and compliance of their servers. BMC Helix Remediate provides that ability. This whitepaper explains how the solutions which comprise BMC Helix Remediate come together to simplify the job of server security and compliance.

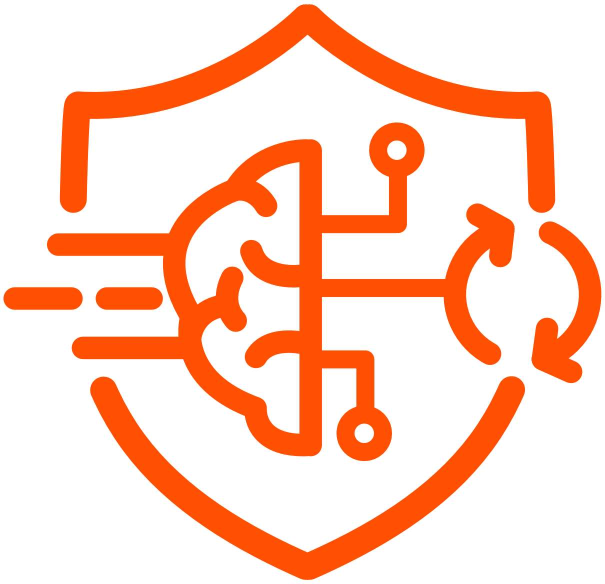
Business Problem

Over 91% of organizations use public cloud, including server instances such as EC2 from Amazon Web Services (AWS). AWS dominates the global IaaS public cloud market, with $15.5 billion in 2018 revenue[1]. But it is not just AWS cloud servers to be managed; businesses also have on-prem servers. To simplify the already Herculean task of managing server security and compliance across their hybrid cloud enterprise, organizations need a single context from which to do so, because simplifying security and compliance enables business agility.

Explanation

Consider an organization running EC2 instances in their AWS accounts. There may be any number of Virtual Private Clouds (VPCs) running, in any number of accounts. Under the Shared Responsibilities Model[2], the customer is solely responsible for patch, vulnerability, and compliance management (OS and EC2 configuration) of their EC2 virtual machines. An enterprise could easily spin up hundreds, if not thousands, of EC2s spanning DEV, QA, and PROD environments, every instance of which must be appropriately configured and maintained if it is to be both secure and compliant.

Someone might be tempted to do this manually. Trouble is, the cloud changes too quickly. Limitations of visibility and shadow cloud usage notwithstanding, even if one could locate all of the EC2s running in the enterprise's public cloud estate, and then manually enroll them in an endpoint management solution, the list would be outdated the moment the tedious effort is completed, if not before. Developers are continuously innovating, and their CI/CD pipelines wait for no one.



[1] Gartner, July 2019 press release, 2019-07-29, Nag et. al.
[2] https://aws.amazon.com/compliance/shared-responsibility-model/

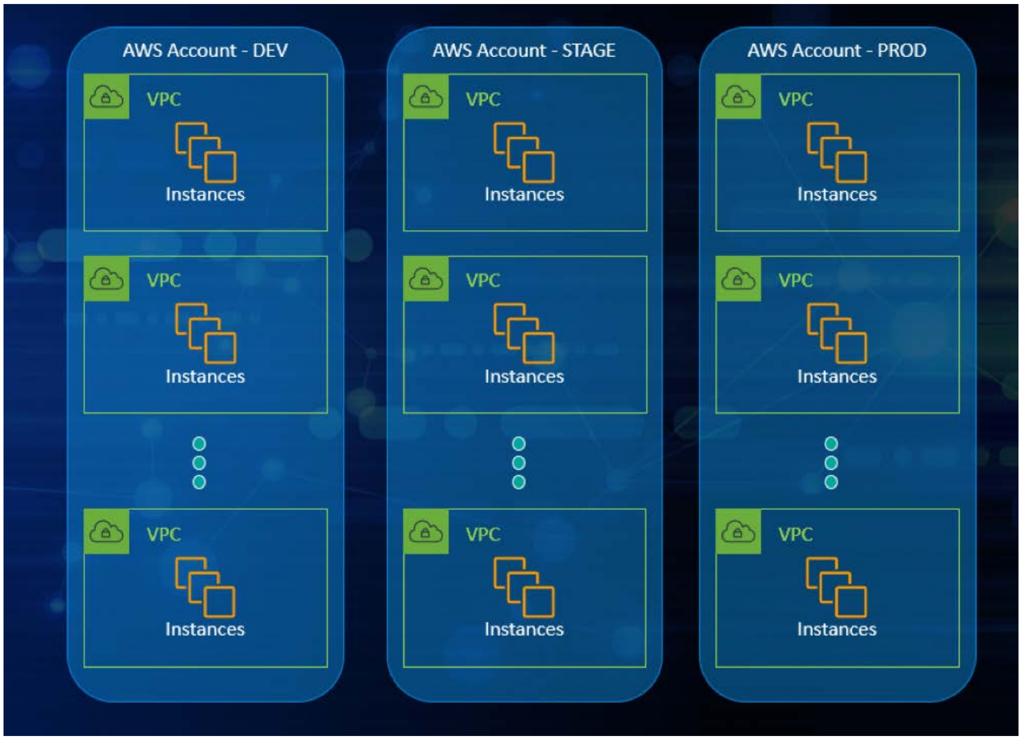
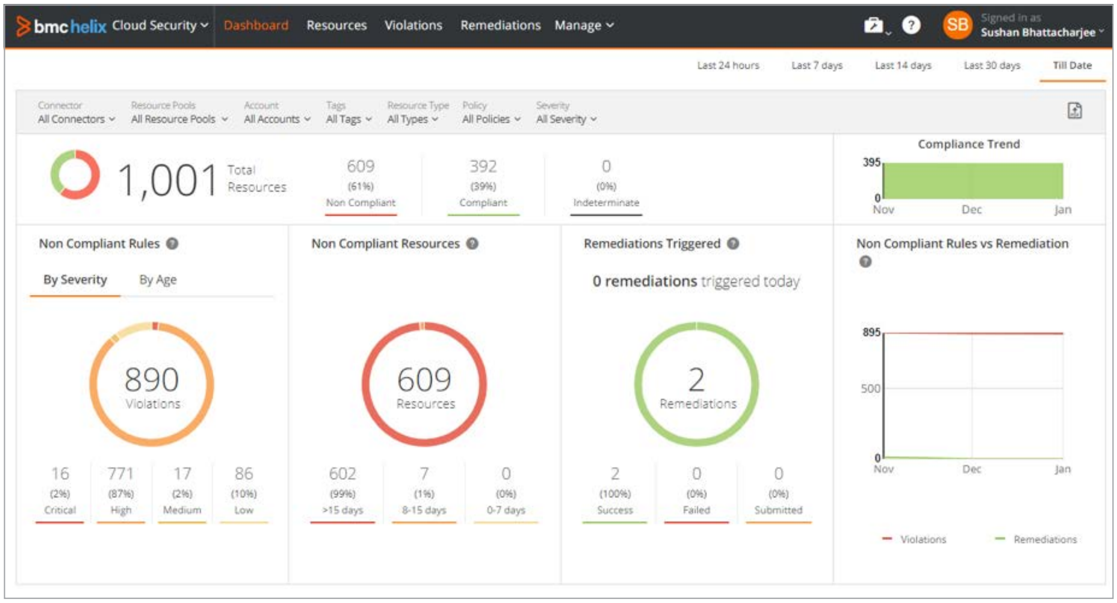


Figure 1: AWS EC2 Instances Spread Across A Vast and Dynamic Cloud Footprint

Fortunately, policy-based, automated “find and fix” is a forte of BMC Helix Cloud Security (Figure 2), which can **programmatically locate EC2 instances and automatically enroll** them in BMC’s TrueSight Server Automation, whose strength is patch, vulnerability, and compliance management of servers.



Connector: All Connectors
Resource Pools: All Resource Pools
Account: All Accounts
Tags: All Tags
Resource Type: All Types
Policy: All Policies
Severity: All Severity

1,001 Total Resources

609 (61%) Non Compliant
392 (39%) Compliant
0 (0%) Indeterminate

Non Compliant Rules
By Severity
By Age
890 Violations
16 (2%) Critical
771 (87%) High
17 (2%) Medium
86 (10%) Low

Non Compliant Resources
609 Resources
602 (99%) >15 days
7 (1%) 8-15 days
0 (0%) 0-7 days

Remediations Triggered
0 remediations triggered today
2 Remediations
2 (100%) Success
0 (0%) Failed
0 (0%) Submitted

Non Compliant Rules vs Remediation

Figure 2: Cloud Security and Compliance at a Glance with BMC Helix Cloud Security

Solution

BMC Helix Remediate is a solution set which includes BMC Helix Cloud Security, BMC Helix Automation Console, and TrueSight Server Automation.

- **BMC Helix Cloud Security** (BHCS) automates policy-based security checks and remediation, so that cloud IaaS and PaaS services are securely configured.

- **BMC Helix Automation Console** helps IT Operations identify, prioritize, and remediate vulnerable servers (such as those missing patches), by enriching scan data from popular vulnerability scan tools. It is a single console to manage both on-prem and hybrid cloud servers.

- **TrueSight Server Automation** acts as the execution engine for OS compliance assessment, patch deployment, vulnerability remediation, deployments, and server management.

Our solution to set up cloud server management for any new public cloud server consists of 3 simple, automated steps.

Automated Agent Installation.

First, a BHCS policy searches your AWS environment for any EC2 instances which do not include a lightweight Smart Agent. This Smart Agent is part of the TrueSight Server Automation (TSSA) solution. Upon finding such an EC2 instance, BHCS flags it as a violation and uses its inherent automated remediation capabilities, in cooperation with SSM, to install the TSSA Smart Agent. This automated installation can happen with a simple mouse click ("on-demand"), or with fully automated Self-Driving Remediation. It can also happen consistent with your incident and change management process. The choice and control are yours.

EC(2) Phone Home.

Next, after having been installed on each of the flagged EC2 instances, each Smart Agent begins sending a heartbeat signal back to the Smart Hub, installed in a Management VPC within your AWS environment, as shown in Figure 3. This heartbeat requires no manual intervention to setup.

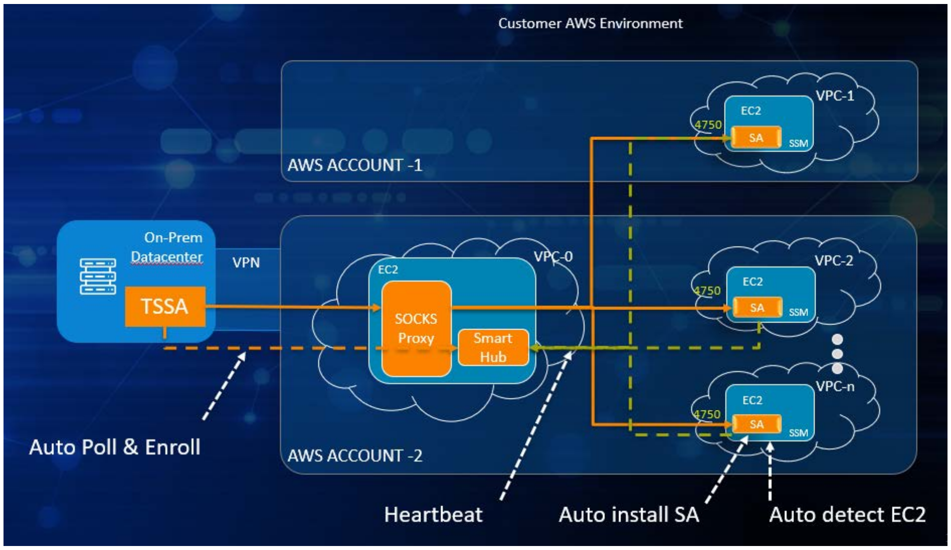


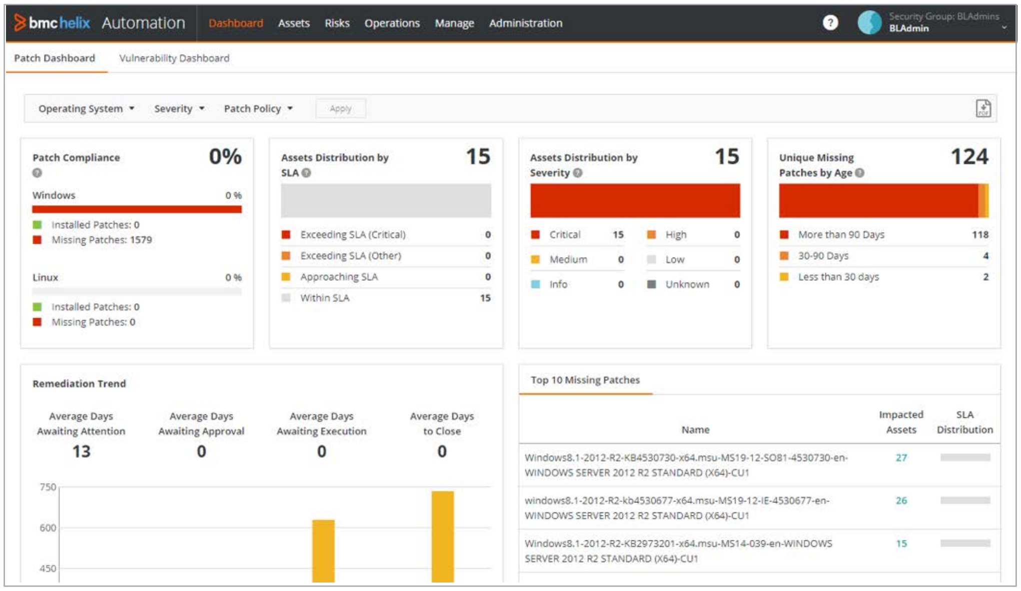
Figure 3: Hybrid Cloud Server Mgmt. with BMC Helix Remediate

Poll and Enroll.

TrueSight Server Automation (TSSA) polls the Smart Hub, recognizes the new heartbeat, and enrolls the newly identified EC2 instances with the Smart Agent in the TSSA managed service.

All 3 steps happened automatically, with no manual intervention. The security and compliance of each EC2 in the organization's AWS environment(s) is now being managed by TSSA, in cooperation with BMC Helix Cloud Security.

Similarly, TSSA also manages the security and compliance of on-prem servers, installing Smart Agents, polling heartbeats, and so on. This is the power and simplicity which BMC Helix Remediate provides its customers: a single context from which to manage security and compliance of servers, whether they reside on-prem or in the cloud. This user experience, shown in Figures 4 and 5, together with automation, simplifies the complex job of server management.



Patch Compliance 0%

Windows 0 %
- 🟩 Installed Patches: 0
- 🟥 Missing Patches: 1579

Linux 0 %
- 🟩 Installed Patches: 0
- 🟥 Missing Patches: 0

Assets Distribution by SLA 15

🟥 Exceeding SLA (Critical)	0
🟧 Exceeding SLA (Other)	0
🟨 Approaching SLA	0
⬜ Within SLA	15

Assets Distribution by Severity 15

🟥 Critical	15	🟧 High	0
🟨 Medium	0	⬜ Low	0
🟦 Info	0	⬛ Unknown	0

Unique Missing Patches by Age 124

🟥 More than 90 Days	118
🟧 30-90 Days	4
🟨 Less than 30 days	2

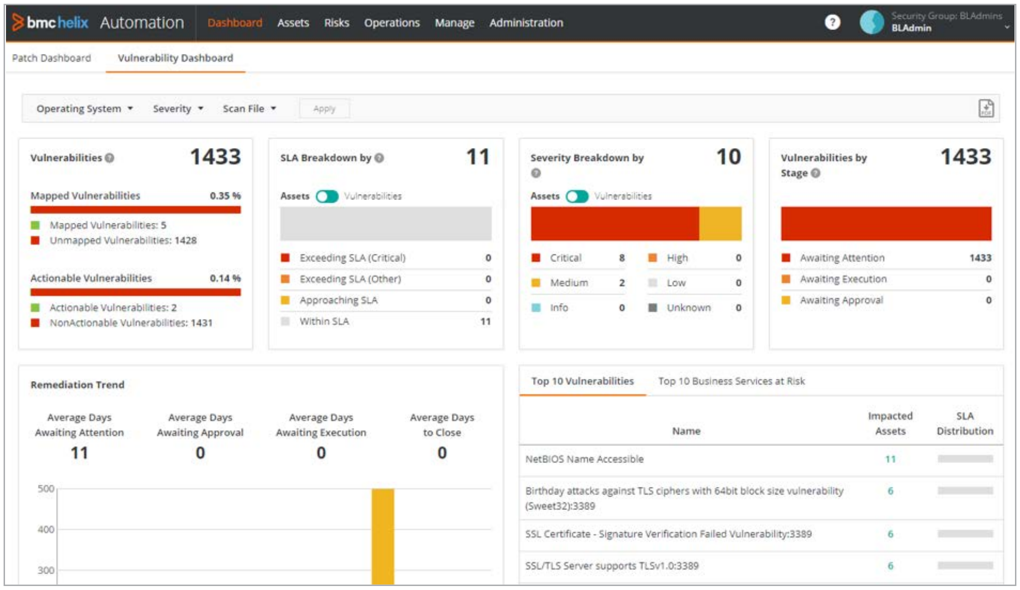
Remediation Trend

Average Days Awaiting Attention	Average Days Awaiting Approval	Average Days Awaiting Execution	Average Days to Close
13	0	0	0

Top 10 Missing Patches

Name	Impacted Assets	SLA Distribution
Windows8.1-2012-R2-KB4530730-x64.msu-MS19-12-SO81-4530730-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-CU1	27	
windows8.1-2012-R2-kb4530677-x64.msu-MS19-12-IE-4530677-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-CU1	26	
Windows8.1-2012-R2-KB2973201-x64.msu-MS14-039-en-WINDOWS SERVER 2012 R2 STANDARD (X64)-CU1	15	

Figure 4: BMC Helix Automation Console's Patch Dashboard



Vulnerabilities 1433

Mapped Vulnerabilities 0.35 %
- 🟩 Mapped Vulnerabilities: 5
- 🟥 Unmapped Vulnerabilities: 1428

Actionable Vulnerabilities 0.14 %
- 🟩 Actionable Vulnerabilities: 2
- 🟥 NonActionable Vulnerabilities: 1431

SLA Breakdown by 11

Assets ● Vulnerabilities

🟥 Exceeding SLA (Critical)	0
🟧 Exceeding SLA (Other)	0
🟨 Approaching SLA	0
⬜ Within SLA	11

Severity Breakdown by 10

Assets ● Vulnerabilities

🟥 Critical	8	🟧 High	0
🟨 Medium	2	⬜ Low	0
🟦 Info	0	⬛ Unknown	0

Vulnerabilities by Stage 1433

🟥 Awaiting Attention	1433
🟧 Awaiting Execution	0
🟨 Awaiting Approval	0

Remediation Trend

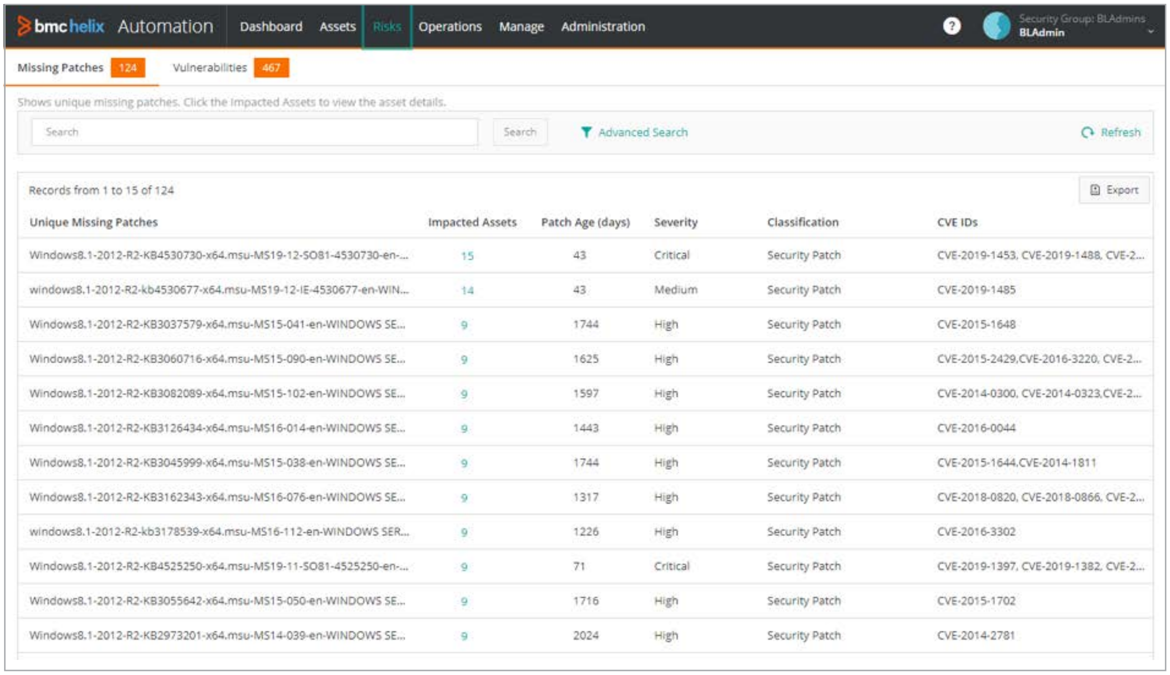
Average Days Awaiting Attention	Average Days Awaiting Approval	Average Days Awaiting Execution	Average Days to Close
11	0	0	0

Top 10 Vulnerabilities | Top 10 Business Services at Risk

Name	Impacted Assets	SLA Distribution
NetBIOS Name Accessible	11	
Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32):3389	6	
SSL Certificate - Signature Verification Failed Vulnerability:3389	6	
SSL/TLS Server supports TLSv1.0:3389	6	

Figure 5: Vulnerability Dashboard on BMC Helix Automation Console

The jobs, patch orchestration, and vulnerability management for all servers, physical or virtual, on-prem or in the cloud, are facilitated via the BMC Helix Automation Console and by using the battle-hardened capabilities of TrueSight Server Automation to execute tasks behind the scenes.

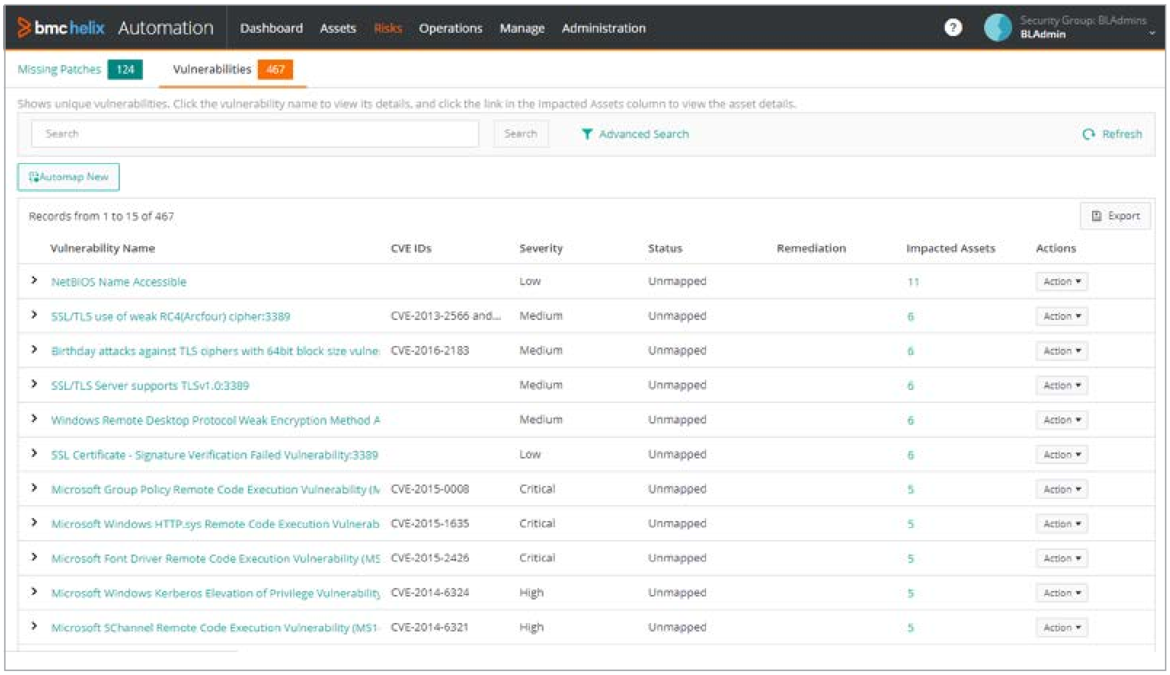


Shows unique missing patches. Click the Impacted Assets to view the asset details.

Records from 1 to 15 of 124

Unique Missing Patches	Impacted Assets	Patch Age (days)	Severity	Classification	CVE IDs
Windows8.1-2012-R2-KB4530730-x64.msu-MS19-12-SO81-4530730-en-...	15	43	Critical	Security Patch	CVE-2019-1453, CVE-2019-1488, CVE-2...
windows8.1-2012-R2-kb4530677-x64.msu-MS19-12-IE-4530677-en-WIN...	14	43	Medium	Security Patch	CVE-2019-1485
Windows8.1-2012-R2-KB3037579-x64.msu-MS15-041-en-WINDOWS SE...	9	1744	High	Security Patch	CVE-2015-1648
Windows8.1-2012-R2-KB3060716-x64.msu-MS15-090-en-WINDOWS SE...	9	1625	High	Security Patch	CVE-2015-2429,CVE-2016-3220, CVE-2...
Windows8.1-2012-R2-KB3082089-x64.msu-MS15-102-en-WINDOWS SE...	9	1597	High	Security Patch	CVE-2014-0300, CVE-2014-0323,CVE-2...
Windows8.1-2012-R2-KB3126434-x64.msu-MS16-014-en-WINDOWS SE...	9	1443	High	Security Patch	CVE-2016-0044
Windows8.1-2012-R2-KB3045999-x64.msu-MS15-038-en-WINDOWS SE...	9	1744	High	Security Patch	CVE-2015-1644,CVE-2014-1811
Windows8.1-2012-R2-KB3162343-x64.msu-MS16-076-en-WINDOWS SE...	9	1317	High	Security Patch	CVE-2018-0820, CVE-2018-0866, CVE-2...
windows8.1-2012-R2-kb3178539-x64.msu-MS16-112-en-WINDOWS SER...	9	1226	High	Security Patch	CVE-2016-3302
Windows8.1-2012-R2-KB4525250-x64.msu-MS19-11-SO81-4525250-en-...	9	71	Critical	Security Patch	CVE-2019-1397, CVE-2019-1382, CVE-2...
Windows8.1-2012-R2-KB3055642-x64.msu-MS15-050-en-WINDOWS SE...	9	1716	High	Security Patch	CVE-2015-1702
Windows8.1-2012-R2-KB2973201-x64.msu-MS14-039-en-WINDOWS SE...	9	2024	High	Security Patch	CVE-2014-2781

Figure 6: Missing Patches on Servers Under Management



Shows unique vulnerabilities. Click the vulnerability name to view its details, and click the link in the Impacted Assets column to view the asset details.

Records from 1 to 15 of 467

Vulnerability Name	CVE IDs	Severity	Status	Remediation	Impacted Assets	Actions
NetBIOS Name Accessible		Low	Unmapped		11	Action ▾
SSL/TLS use of weak RC4(Arcfour) cipher:3389	CVE-2013-2566 and...	Medium	Unmapped		6	Action ▾
Birthday attacks against TLS ciphers with 64bit block size vulne	CVE-2016-2183	Medium	Unmapped		6	Action ▾
SSL/TLS Server supports TLSv1.0:3389		Medium	Unmapped		6	Action ▾
Windows Remote Desktop Protocol Weak Encryption Method A		Medium	Unmapped		6	Action ▾
SSL Certificate - Signature Verification Failed Vulnerability:3389		Low	Unmapped		6	Action ▾
Microsoft Group Policy Remote Code Execution Vulnerability (M	CVE-2015-0008	Critical	Unmapped		5	Action ▾
Microsoft Windows HTTP.sys Remote Code Execution Vulnerab	CVE-2015-1635	Critical	Unmapped		5	Action ▾
Microsoft Font Driver Remote Code Execution Vulnerability (MS	CVE-2015-2426	Critical	Unmapped		5	Action ▾
Microsoft Windows Kerberos Elevation of Privilege Vulnerability	CVE-2014-6324	High	Unmapped		5	Action ▾
Microsoft SChannel Remote Code Execution Vulnerability (MS1	CVE-2014-6321	High	Unmapped		5	Action ▾

Figure 7: Vulnerabilities Listed Within the BMC Helix Automation Console ng Patches on Servers Under Management

Conclusion

The solutions within BMC Helix Remediate combine to simplify and automate the job of server management, whether those servers reside on-prem, in the cloud, or both. Using policy-based automation and remediation, we find cloud servers not being managed, install a lightweight smart agent, and enroll them in TrueSight Server Automation. OS patching, vulnerability management, and server compliance are all managed from a single GUI.

ⓘ

For more information

To learn more about BMC Helix Remediate, or its constituent solutions, please contact your local BMC Sales office, or visit us online at www.bmc.com/remediate.