Thought Leadership White Paper

How to Effectively Close the SecOps Gap

Increase visibility and eliminate threats with Automated SecOps solutions from BMC

Table of Contents

Executive Summary

The demands of the digital enterprise put pressure on businesses to prevent and stop security threats, meet regulatory compliance requirements, and govern their operations more efficiently. Businesses must defend themselves against the constant barrage of cyber threats aimed at disrupting their systems. Breaches can be expensive, with the average cost now over $3.9 million per breach—and the brand damage is nearly incalculable.[1]

Operations teams are working to keep their systems running and functional for people who depend on them for new and existing services. Security teams must ensure the same systems are secure, up-to-date, and compliant with regulatory standards. Managing the balance between security and system uptime and performance is challenging because the goals of the enterprise may be similar, but both teams have different priorities. These competing priorities and the lack of integration between security and operations teams can create gaps in the security posture that can leave businesses susceptible to increased risk and cyberattacks—commonly known as the SecOps gap.

This white paper examines how companies are closing the SecOps gap with BMC SecOps solutions and are using automation to build security and compliance practices that satisfy the demands of digital business. These solutions align the priorities of the security and operations teams to reduce risk and scale operations—enabling them to work more effectively together.

[1] Ponemon Institute, 2018 Global Cost of a Data Breach Study

A CLOSER LOOK AT THE SECOPS CHALLENGE

Security breaches have potentially catastrophic consequences and must be blocked, and according to the 2018 Verizon Data Breach Investigations Report, 6% of breaches can be attributed to patchable vulnerabilities. But the two primary teams responsible for blocking them have different priorities, timelines, and objectives. Businesses are taking a new management approach to bridge the gap between security and operations teams and ensure that systems stay running and secure. SecOps is an approach to link security and operations teams together with **shared accountability, processes, and tools to ensure that companies do not have to sacrifice security to maintain a commitment to agility**. It enables them to meet new service delivery requirements and move faster with a highly automated, coordinated, and secure approach that facilitates continuous innovation.

> **"Closing the SecOps gap and implementing an integrated approach to automate information security processes greatly improved data security at Morningstar."**[2]
>
> ~Michael Allen, Chief Information Security Officer, Morningstar, Inc.

Let's look at what this model provides and how it differs from traditional approaches. The security team oversees security to prevent hackers and other unauthorized access to enterprise data and systems. This team is also charged with ensuring all IT systems follow company and government-mandated policies and compliance standards. Their job generally stops at the level of identifying the threat, vulnerability, or deficiency. They do not own the operational implementation of the changes necessary to remediate or fix the issues.

Part of the responsibility of the operations team is to carry out corrective actions, such as patching, and ensure that vulnerabilities are mitigated in a timely manner. The operations team is responsible for maintaining uptime, stability, and performance of current systems, and for deploying new services, such as software code and features. For operations personnel, much of their time is focused on keeping systems up and running. They're trying to ensure security and compliance tasks don't interfere with systems operations. However, because the primary mission of operations is to ensure uptime and stability, security updates are frequently delayed or not completed. This situation can create risk (an attack surface) for hackers to exploit vulnerabilities in those systems.

Exacerbating the issue related to vulnerabilities is the fact that **half of all exploitations occur between 10 and 100 days after the vulnerability is published, with the median around 30 days**.[3] However, it takes the average organization 84 days (12 weeks) to deploy a security patch, creating a window of vulnerability of 54 days. One reason for this gap is that interactions between security and operations teams are mostly manual.

When the security team runs automated scans of the IT environment for compliance issues, the results are frequently shared with the operations team via massive spreadsheets that could contain thousands of lines of data. The information isn't prioritized and the data often is provided to the operations team without the context needed. From there, operations must identify what issues need to be addressed and in what priority, which is another manual process. The updates are then scheduled into the production cycle and implemented, which takes time and is a highly manual process.

This process is quite fragmented, manual, and disjointed due to **competing priorities and lack of insight into the other team**. In fact, in a 2018 study by Ponemon Institute and BMC, fifty-six percent of respondents agree that there is tension between IT security and IT operations because of a lack of alignment of their different priorities.

Fortunately, organizations can break down the silos and reduce the burden of manual processes between these two teams with BMC SecOps solutions, and improve security with automation that can scale to the speed and quality demands of the business.

[2] http://newsroom.bmc.com/phoenix.zhtml?c=253321&p=irol-newsArticle_Print&ID=2126044

[3] Verizon 2016 Data Breach Investigations Report

Fifty-six percent of survey respondents agree that there is tension between IT security and IT operations because of a lack of alignment of their different priorities

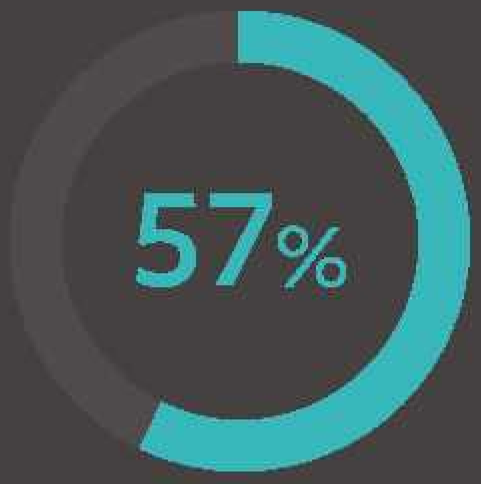
THE SOLUTION: A SECOPS APPROACH

SecOps is a management approach that connects security and operations teams. **It links both teams together to work with shared accountability, processes, and tools to ensure that businesses do not have to sacrifice security to maintain uptime and performance.**

When SecOps methods are embraced, security employees can no longer simply hand off results from a vulnerability scan to operations team members and think their work is done. The goal is to keep both teams engaged in the process and provide visibility into what changes need to be made and the possible impact of those changes to other parts of the business. When these teams don't have an effective way to transfer and consume information, organizations can struggle to quickly remediate vulnerabilities.

BMC SecOps solutions transform disconnected initiatives into a single, unified, secure, and comprehensive process that accelerates vulnerability resolution, controls the cost of remediation, and mitigates risk. This capability enables security and operations teams to become more agile and move to a proactive security position for both cloud and on-premises systems. It also allows the teams to readily embrace key business initiatives related to managing the impact of digital transformation and the continuous delivery of services. These are capabilities vital to the performance of businesses, but create significant security concerns if they are not managed with rigorous and adaptable controls.

BMC SecOps solutions with centralized management can help facilitate coordination and collaboration between security and operations teams. According to the Ponemon study, only 19 percent of respondents rate their organizations' ability to minimize or mitigate IT security risks as very high. One reason is that instead of focusing on prevention, 53 percent of respondents say their organizations' approach to dealing with threats is reactive. Collaboration between these two groups can be improved through the use of tools that bring these two functions closer together and foster teamwork which will benefit the organization as a whole. An integrated, automated solution for vulnerability management is a proactive strategy for preventing and minimizing the risk of a data breach.



Reported their companies had one or more data breaches in the past year, and that they could have occurred because a patch was available for a known vulnerability but not applied.

SecOps empowers companies to take a comprehensive and proactive approach to security issues rather than a reactive one. Organizations can manage by policy and automatically address security issues to protect their businesses. Today, network and systems administrators and IT staff are stretched thin and manual tasks consume key cycles and drive up costs. Automation can help them reduce that burden, and allow these highly skilled resources to be devoted to more strategic tasks.

Professionals who work in security and operations can become proficient in using BMC SecOps solutions within weeks. BMC also provides customizable, user-friendly dashboards for both security and operations teams, and interfaces that make it easier to visualize security issues, and quickly prioritize and address vulnerabilities.

HOW BMC SECOPS BENEFITS BUSINESSES

The following real-life examples explain how BMC SecOps solutions provide better security and compliance while making security and operations teams more effective.

Agile Execution

Integrated Visibility

Rigorous Controls

- **Agile execution to meet business objectives:** Automate the integration of security and operations data to accelerate remediation of vulnerabilities while driving operational excellence.
  - A major insurance and financial services agency reduced 9,000+ staff hours by automatically remediating more than 94,000 events with TrueSight Server Automation.
  - A major U.S. manufacturer reduced the time to fix known vulnerabilities from 880 hours to 30 seconds.
- **Integrated visibility for a holistic view of environments**: Collaboration between security and operations fueled by integrated visibility into risks, impacts, and operational plans.
  - A university and research center used BMC Discovery to automate service mapping for commercial and in-house applications (80 services in all), which helped IT staff assess changes and prioritize incident response.
  - A large manufacturer stated that TrueSight Vulnerability Management enables security and operations teams to see what the other is doing, opening a dialogue to allow the most current issues to be addressed first, while still achieving the operation team's goal of uptime.
- **Rigorous controls to protect customers**: Security and operations work collaboratively to support rigorous and vigilant controls for audits and compliance, while tools absorb some of the complexity, so that organizations can get back to the fundamental services they deliver.
  - A government agency reduced the time to create audit reports from 32 hours to 15 minutes with TrueSight Server Automation.

BMC SecOps solutions provide operations teams with a variety of essential capabilities including:

Providing prescriptive and actionable data to address vulnerabilities based on perceived impact, current operational plans, and policy to enable the expedient remediation of risks.

Enabling more focused activities by the operations teams to reduce the overall attack surface.

Giving the security team a security dashboard to gain views into operational plans to address vulnerabilities and predictive SLAs with burndown details that enable security to assess the current security readiness of their organization.

BMC SECOPS SOLUTION OVERVIEW

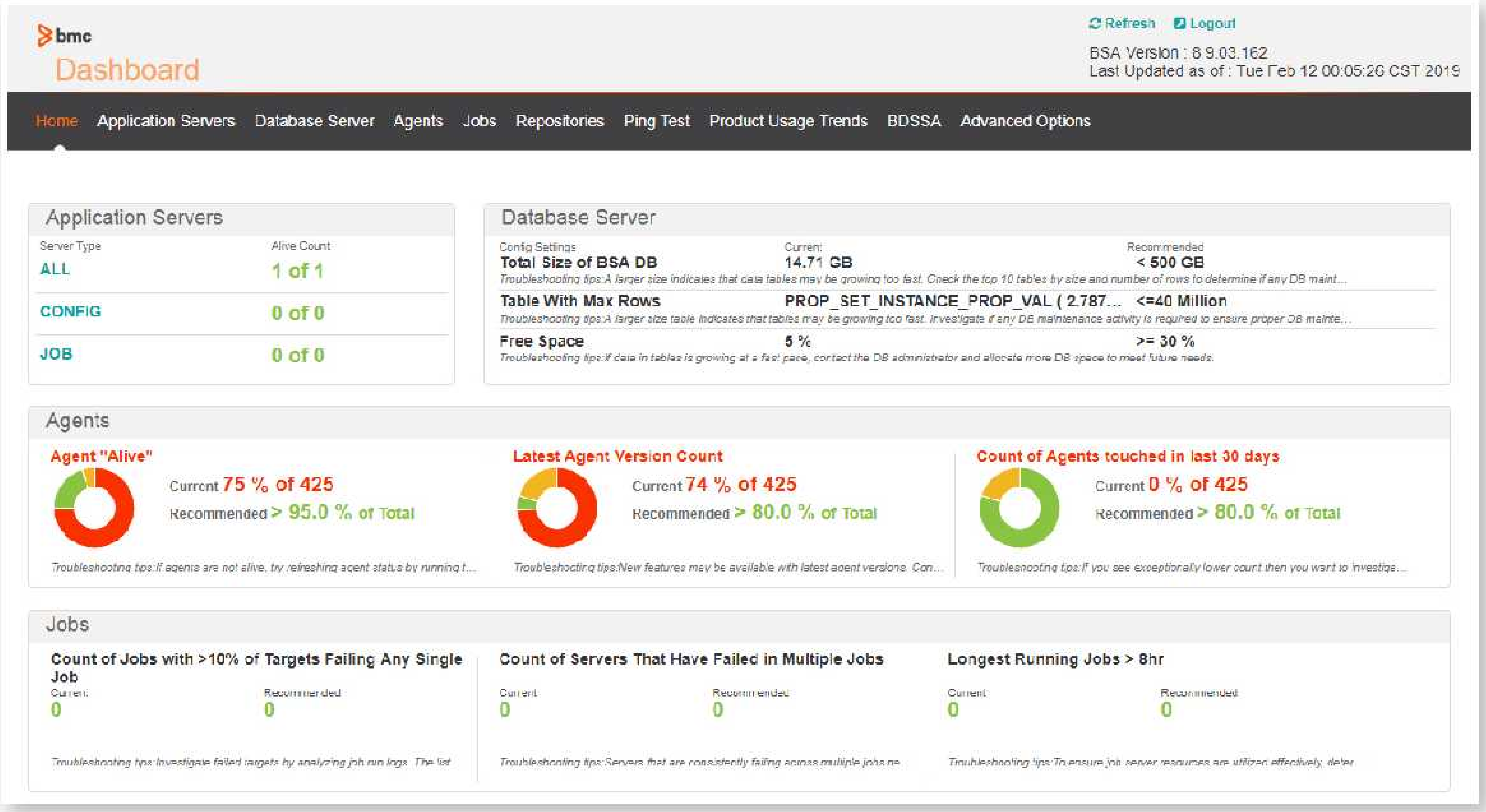
The following products have enabled businesses worldwide to achieve their objectives for maintaining security, improving productivity, and closing the SecOps gap.

These solutions provide teams with the knowledge to take control of their security posture, and the automation needed to scale to the speed and quality demands of the business. Operations teams can access prescriptive and actionable data to prioritize and eliminate potential risks to both servers and networking devices. Security teams provide customizable, real-time views of operational plans for addressing risk and detailed information on potential blind spots.

TrueSight Server Automation provides automated management, control, and enforcement of server configuration changes in the data center and cloud. It enables organizations to escape the high costs and timelines of traditional manual processes.

Capabilities include:

- **Compliance and risk mitigation**: Full cycle of system discovery, monitoring, remediation, and integrated change control, providing continuous compliance with out-of-the-box integration with BMC ITSM suite
- **Full lifecycle management**: Focal point of control for the entire server lifecycle, simplifying compliance, provisioning, configuration, patching, and reporting
- **Advanced built-in security**: Granular role-based access control system that reduces the risk of misconfiguration and improves systems stability
- **Abstracted simplified management**: Enable full-stack layered provisioning for rapid, automated resource allocation



BSA Version : 8 9.03.162
Last Updated as of : Tue Feb 12 00:05:26 CST 2019

Application Servers

Server Type	Alive Count
ALL	1 of 1
CONFIG	0 of 0
JOB	0 of 0

Database Server

Config Settings	Current	Recommended
Total Size of BSA DB	14.71 GB	< 500 GB
Table With Max Rows	PROP_SET_INSTANCE_PROP_VAL (2.787...	<=40 Million
Free Space	5 %	>= 30 %

Troubleshooting tips:A larger size indicates that data tables may be growing too fast. Check the top 10 tables by size and number of rows to determine if any DB maint...

Troubleshooting tips:A larger size table indicates that tables may be growing too fast. Investigate if any DB maintenance activity is required to ensure proper DB mainte...

Troubleshooting tips:If data in tables is growing at a fast pace, contact the DB administrator and allocate more DB space to meet future needs.

Agents

Agent "Alive"
Current 75 % of 425
Recommended > 95.0 % of Total
Troubleshooting tips:If agents are not alive, try refreshing agent status by running t...

Latest Agent Version Count
Current 74 % of 425
Recommended > 80.0 % of Total
Troubleshooting tips:New features may be available with latest agent versions. Con...

Count of Agents touched in last 30 days
Current 0 % of 425
Recommended > 80.0 % of Total
Troubleshooting tips:If you see exceptionally lower count then you want to investiga...

Jobs

Count of Jobs with >10% of Targets Failing Any Single Job
Current 0 Recommended 0
Troubleshooting tips:Investigate failed targets by analyzing job run logs. The list

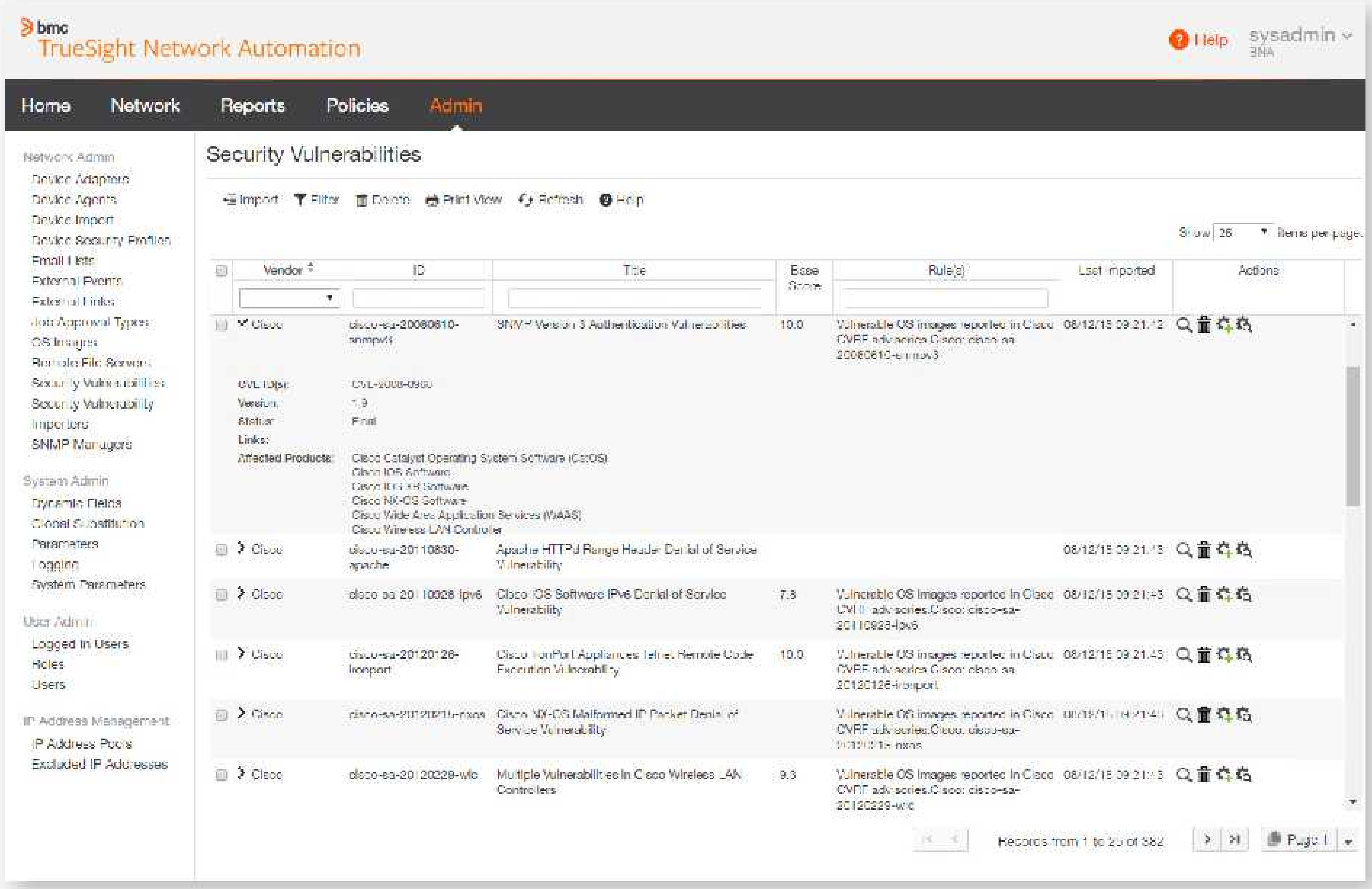
Count of Servers That Have Failed in Multiple Jobs
Current 0 Recommended 0
Troubleshooting tips:Servers that are consistently failing across multiple jobs ne

Longest Running Jobs > 8hr
Current 0 Recommended 0
Troubleshooting tips:To ensure job server resources are utilized effectively, deter

FIGURE 1: TrueSight Server Automation – Fully automate all critical tasks across your data centers

Truesight Network Automation provides automated network management to improve network consistency and reduce risk. It can scan thousands of devices in less than a minute and take action to reduce the risk of breaches and errors. The solution enables organizations to avoid network outages and bad configuration changes, and improves service delivery across the business. IT can free up expensive network administration resources from labor-intensive audits to more strategic tasks.

The solution closes the window of vulnerability with native detection of security risks in real-time, with one-touch rule generation for vulnerabilities and remediation actions. With this single solution, IT staff can manage physical and virtual network devices across most major platforms and ensure compliance while reducing complexity.



Security Vulnerabilities

Show 25 items per page.

Vendor	ID	Title	Base Score	Rule(s)	Last Imported	Actions
Cisco	cisco-sa-20080610-snmpv3	SNMP Version 3 Authentication Vulnerabilities	10.0	Vulnerable OS images reported in Cisco CVRF advisories.Cisco: cisco-sa-20080610-snmpv3	08/12/15 09:21:12	
Cisco	cisco-sa-20110830-apache	Apache HTTPD Range Header Denial of Service Vulnerability			08/12/15 09:21:15	
Cisco	cisco-sa-20110928-ipv6	Cisco IOS Software IPv6 Denial of Service Vulnerability	7.8	Vulnerable OS images reported in Cisco CVRF advisories.Cisco: cisco-sa-20110928-ipv6	08/12/15 09:21:43	
Cisco	cisco-sa-20120126-ironport	Cisco IronPort Appliances Telnet Remote Code Execution Vulnerability	10.0	Vulnerable OS images reported in Cisco CVRF advisories.Cisco: cisco-sa-20120126-ironport	08/12/15 09:21:45	
Cisco	cisco-sa-20121010-nxos	Cisco NX-OS Malformed IP Packet Denial of Service Vulnerability		Vulnerable OS images reported in Cisco CVRF advisories.Cisco: cisco-sa-20121010-nxos	08/12/15 09:21:41	
Cisco	cisco-sa-20120229-wlc	Multiple Vulnerabilities in Cisco Wireless LAN Controllers	9.3	Vulnerable OS images reported in Cisco CVRF advisories.Cisco: cisco-sa-20120229-wlc	08/12/15 09:21:15	

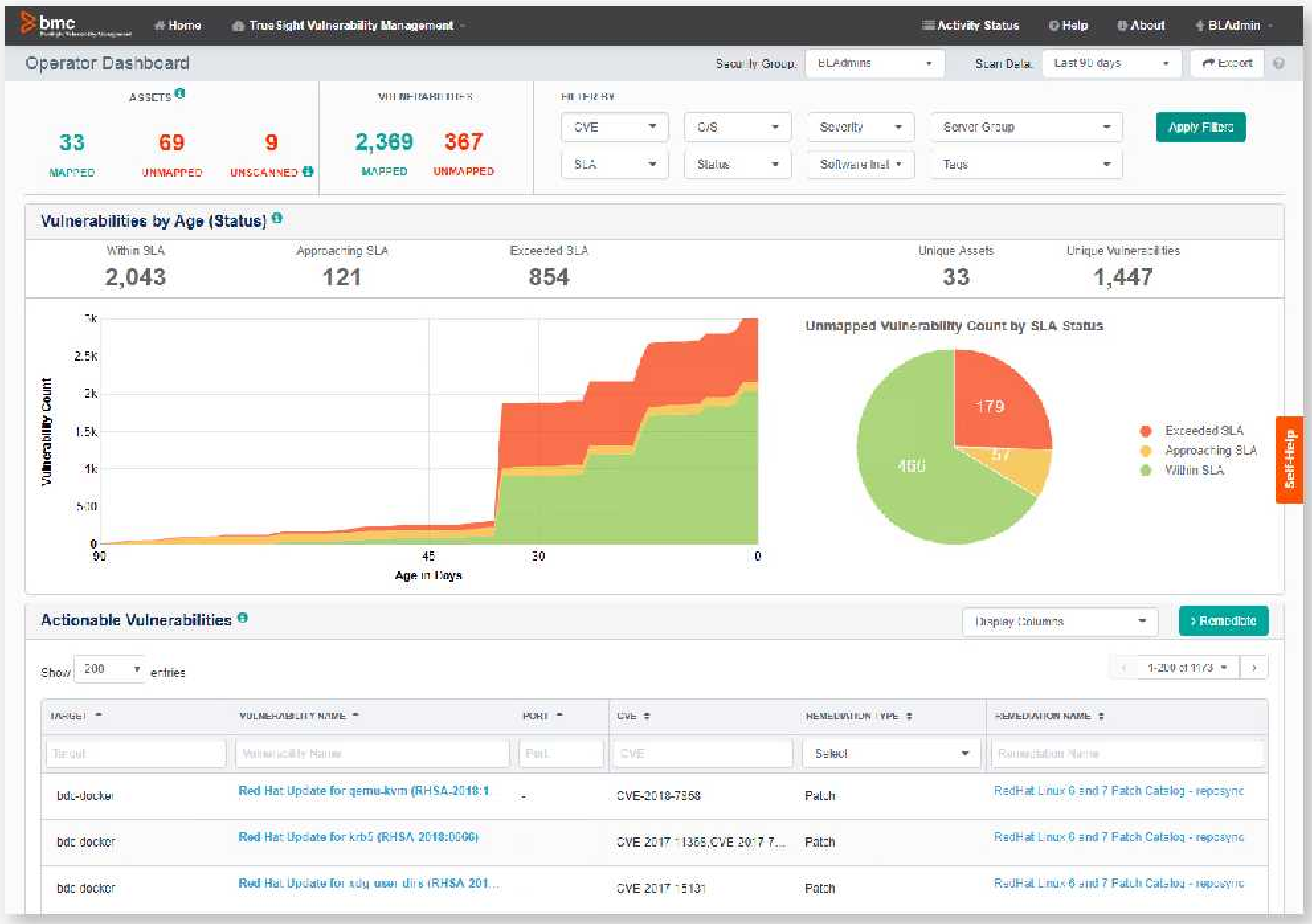
CVE ID(s): CVE-2008-0960
Version: 1.9
Status: Final
Links:
Affected Products: Cisco Catalyst Operating System Software (CatOS)
Cisco IOS Software
Cisco IOS XR Software
Cisco NX-OS Software
Cisco Wide Area Application Services (WAAS)
Cisco Wireless LAN Controller

Records from 1 to 25 of 582

Page 1

FIGURE 2: TrueSight Network Automation – Automate network configuration, change, and compliance processes

TrueSight Vulnerability Management connects to tools like TrueSight Server Automation and TrueSight Network Automation to extend the power of threat remediation. It can also be combined with BMC Discovery to leverage the capability to rapidly discover and map assets and applications, see how many un-scanned assets ("blind spots") are in their environments, and take corrective actions to close windows of opportunity for attackers.



Security Group: BLAdmins

Scan Data: Last 90 days

ASSETS

33	69	9
MAPPED	UNMAPPED	UNSCANNED

VULNERABILITIES

2,369	367
MAPPED	UNMAPPED

Vulnerabilities by Age (Status)

Within SLA	Approaching SLA	Exceeded SLA	Unique Assets	Unique Vulnerabilities
2,043	121	854	33	1,447

Actionable Vulnerabilities

Show 200 entries

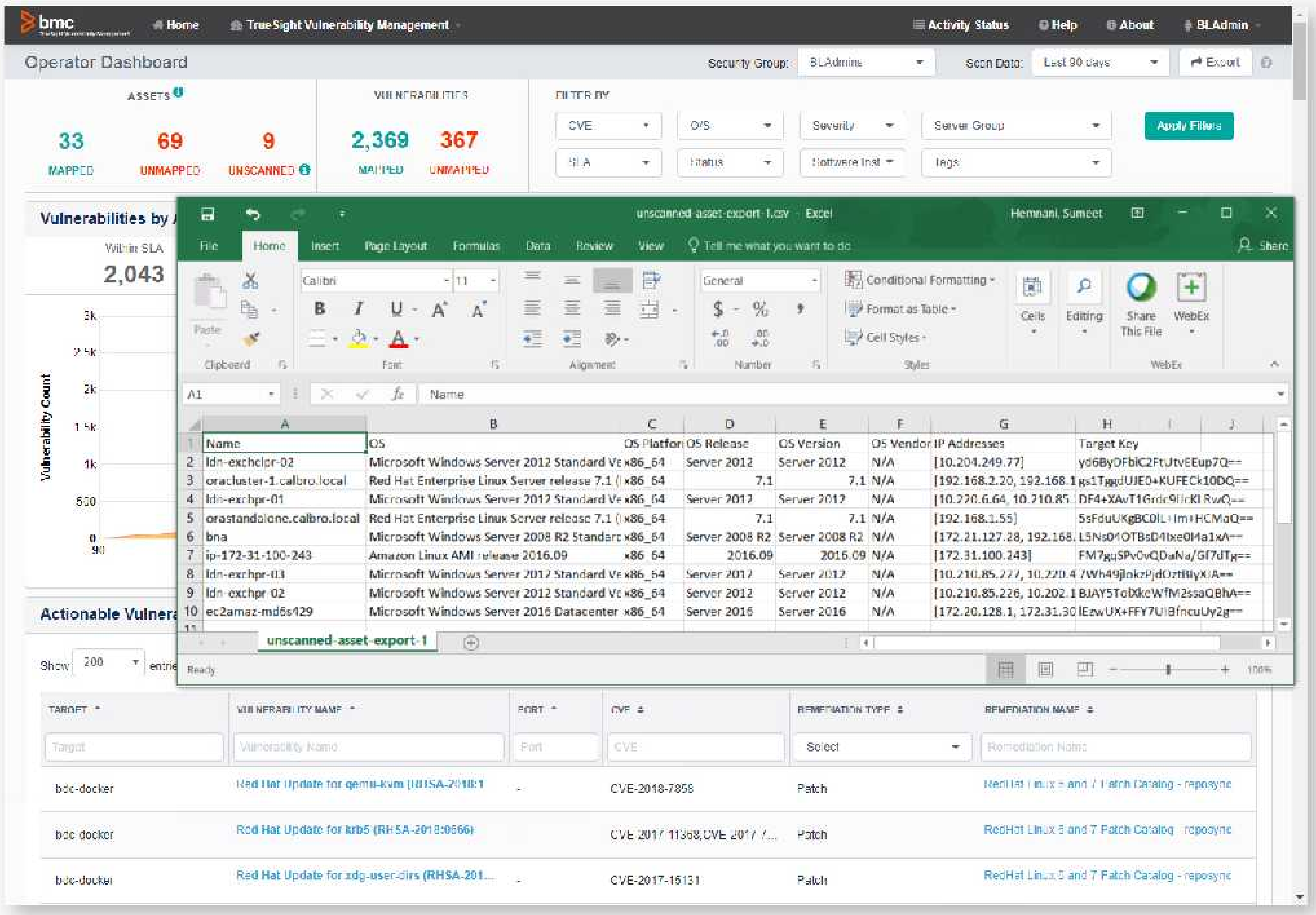
1-200 of 1173

TARGET	VULNERABILITY NAME	PORT	CVE	REMEDIATION TYPE	REMEDIATION NAME
Target	Vulnerability Name	Port	CVE	Select	Remediation Name
bdc-docker	Red Hat Update for qemu-kvm (RHSA-2018:1	-	CVE-2018-7858	Patch	RedHat Linux 6 and 7 Patch Catalog - reposync
bdc-docker	Red Hat Update for krb5 (RHSA-2018:0666)		CVE-2017-11368,CVE-2017-7...	Patch	RedHat Linux 6 and 7 Patch Catalog - reposync
bdc-docker	Red Hat Update for xdg-user-dirs (RHSA-201...		CVE-2017-15131	Patch	RedHat Linux 6 and 7 Patch Catalog - reposync

FIGURE 3: TrueSight Vulnerability Management Dashboard for Operations

TrueSight Vulnerability Management includes intuitive dashboards that automatically link vulnerabilities to identified patches and create an attack plan to deploy countermeasures on demand. This solution gives IT operations and security teams the data they need to prioritize and remediate threats based on their potential impact to business. Capabilities include the ability to:

- **Provide a "to-do"** list to address threats, based on policy and impact, ensuring the most critical issues are fixed first, and using criteria that protects uptime and maintains stability.
- **Provide security a clear view into operational plans**, enabling visibility into planned actions, predictive SLAs, and burndown views to give them the ability to more actively control the security levels of an organization.
- **Create an automated and standard process** for the security and operations teams to enable the relentless pursuit of threats, which significantly reduces the time taken to close the window of vulnerability.



	A	B	C	D	E	F	G	H
1	Name	OS	OS Platfor	OS Release	OS Version	OS Vendor	IP Addresses	Target Key
2	ldn-exchclpr-02	Microsoft Windows Server 2012 Standard Ve	x86_64	Server 2012	Server 2012	N/A	[10.204.249.77]	yd6ByOFblC2FtJtvEEup7Q==
3	oracluster-1.calbro.local	Red Hat Enterprise Linux Server release 7.1 (l	x86_64	7.1	7.1	N/A	[192.168.2.20, 192.168.1	gs1TggdUJE0+KUFECk10DQ==
4	ldn-exchpr-01	Microsoft Windows Server 2012 Standard Ve	x86_64	Server 2012	Server 2012	N/A	[10.220.6.64, 10.210.85	DF4+XAvT1Grdc9IlcKlRwQ==
5	orastandalone.calbro.local	Red Hat Enterprise Linux Server release 7.1 (l	x86_64	7.1	7.1	N/A	[192.168.1.55]	5sFduUKgBC0lL+Im+HCMaQ==
6	bna	Microsoft Windows Server 2008 R2 Standarc	x86_64	Server 2008 R2	Server 2008 R2	N/A	[172.21.127.28, 192.168.	L5Ns0f OTBsD4lxe0Ma1xA==
7	ip-172-31-100-243	Amazon Linux AMI release 2016.09	x86_64	2016.09	2016.09	N/A	[172.31.100.243]	FM7gqSPvOvQDaNa/Gf7dTg==
8	ldn-exchpr-03	Microsoft Windows Server 2012 Standard Ve	x86_64	Server 2012	Server 2012	N/A	[10.210.85.227, 10.220.4	7Wh49jlokzPjdOztlllyXlA==
9	ldn-exchpr-02	Microsoft Windows Server 2012 Standard Ve	x86_64	Server 2012	Server 2012	N/A	[10.210.85.226, 10.202.1	BJAY5ToIXkcWfM2ssaQBhA==
10	ec2amaz-md6s429	Microsoft Windows Server 2016 Datacenter	x86_64	Server 2016	Server 2016	N/A	[172.20.128.1, 172.31.30	lEzwUX+FFY7UIBfncuUy2g==

TARGET	VULNERABILITY NAME	PORT	CVE	REMEDIATION TYPE	REMEDIATION NAME
Target	Vulnerability Name	Port	CVE	Select	Remediation Name
bdc-docker	Red Hat Update for qemu-kvm (RHSA-2018:1	-	CVE-2018-7858	Patch	RedHat Linux 5 and 7 Patch Catalog - reposync
bdc-docker	Red Hat Update for krb5 (RHSA-2018:0666)		CVE-2017-11368,CVE-2017-7...	Patch	RedHat Linux 5 and 7 Patch Catalog - reposync
bdc-docker	Red Hat Update for xdg-user-dirs (RHSA-201...	-	CVE-2017-15131	Patch	RedHat Linux 5 and 7 Patch Catalog - reposync

FIGURE 4: TrueSight Vulnerability Management: View of Unscanned Assets

> **"TrueSight Vulnerability Management will help me patch vulnerabilities more quickly, so I can keep the hackers out of our systems."**
>
> ~John Leach, Senior Network Administrator, CBC Federal Credit Union.7

Discovery enables IT and data center managers to analyze assets from multiple views to identify what systems or applications are affected or vulnerable to an attack.

Discovery enables you to:

- Document inventory for compliance requirements.
- Identify servers that could be back door entry points.
- Understand the business impact of a threat and which assets may be affected.
- Control configuration access rights, encryption, and depth of discovery actions.

The integration with Discovery also enables teams to see dependent applications. Both security and operations teams can estimate the potential impact of a patch before it is released. This powerful set of capabilities is available for TrueSight Vulnerability Management to use with both TrueSight Server Automation and TrueSight Network Automation. This capability breaks through IT operational silos and enables teams to manage servers and networking devices from the same tool.

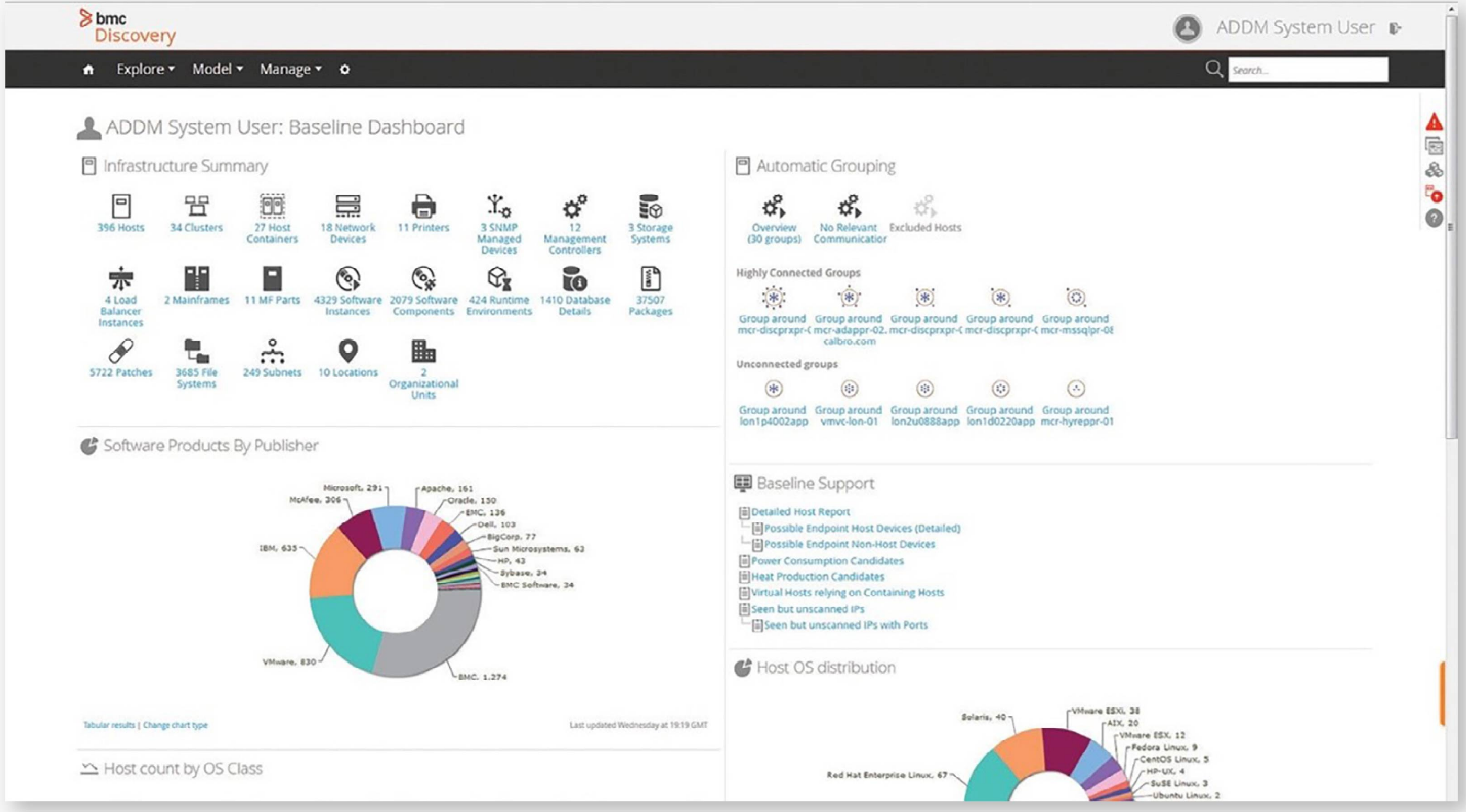


FIGURE 5: Discovery – Fast track IT asset discovery with up to 100% accuracy in 15 minutes

CONCLUSION

SecOps allows businesses to move beyond manual compliance exercises and maintain audit readiness, foster collaborative decision making between security and operations teams, and close windows of risk. Silos between the operations and security teams have not only slowed down agency processes, but also created gaps in security. These gaps in remediation leave IT systems and data vulnerable. Defending against these types of attacks has become increasingly challenging as threats grow more advanced and persistent in the digital economy.

Businesses cannot keep pace with these threats using manual efforts to check the security of their IT assets, install security patches, and quickly remediate any deficiencies that could make them susceptible to an attack. They are embracing the benefits of SecOps, including **reducing the time spent fixing known vulnerabilities, completing more audits in less time, and reducing their security risks—all with BMC SecOps solutions**.

FOR MORE INFORMATION

To learn more about BMC SecOps solutions, please visit **bmc.com/it-solutions/secops-security-operations**

About BMC

BMC helps customers run and reinvent their businesses with open, scalable, and modular solutions to complex IT problems. Bringing both unmatched experience in optimization and limitless passion for innovation to technologies from mainframe to mobile to cloud and beyond, BMC helps more than 10,000 customers worldwide reinvent, grow, and build for the future success of their enterprises.

www.bmc.com