Technical Review

BMC TrueSight Automation for Servers

Date: January 2021 **Authors:** Kerry Dolan, Senior Validation Analyst; and Alex Arcilla, Validation Analyst

Abstract

This ESG Technical Review documents remote testing of BMC TrueSight Automation for Servers with a focus on assessing security vulnerabilities, applying patches, and determining compliance.

The Challenges

When ESG research respondents were asked about their most important considerations for justifying IT investments, improving cybersecurity, increasing employee productivity, and enabling digital transformation were the top three most cited considerations (see Figure 1).[1] These can all be addressed with better management of the server infrastructure. Organizations find it difficult and time-consuming to keep hundreds or thousands of servers properly configured, patched, and in compliance with security and regulatory requirements. Failure to accomplish these tasks consistently can expose an organization to security vulnerabilities and breaches, regulatory fines, and productivity drains.

Figure 1. Top Ten Most Important Considerations for Justifying IT Investments

Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020.

Labor-intensive, manual server management not only results in high error rates, but also in failure to meet availability SLAs and to scale as needed. Automation with proactive, policy-based server management can optimize the production environment for users, freeing up IT staff time for strategic projects. DevOps can also leverage this automation to ensure that their server footprint can continuously support software development and delivery cycles that efficiently respond to customer needs.

The Solution: BMC TrueSight Automation for Servers

BMC TrueSight Server Automation for Servers (TSAS) is a key part of the BMC's infrastructure automation and security solution suite that includes network automation, public cloud and container configuration management, and compliance offerings. Organizations use TSAS to manage physical, virtual, and cloud servers across Windows, Linux, and UNIX operating systems through a single pane of glass. TSAS also enables precise changes to be executed with fine-grained, role-based access controls that keep systems secure and stable.

TSAS helps IT not only to manage servers and understand configuration status, but also actively remediate problems—without requiring scripting. Organizations can discover servers, audit their configurations, and change configurations when required (see Figure 2). If a change to an individual system or group does not work as expected, administrators can quickly roll it back, saving time and reducing risk.

TSAS enables administrators to employ policy-based management of server configurations and consistent, reliable server management regimens with less administrative effort and cost. Organizations can leverage built-in automation to further reduce operational expenses while increasing overall security and compliance.

TSAS simplifies:

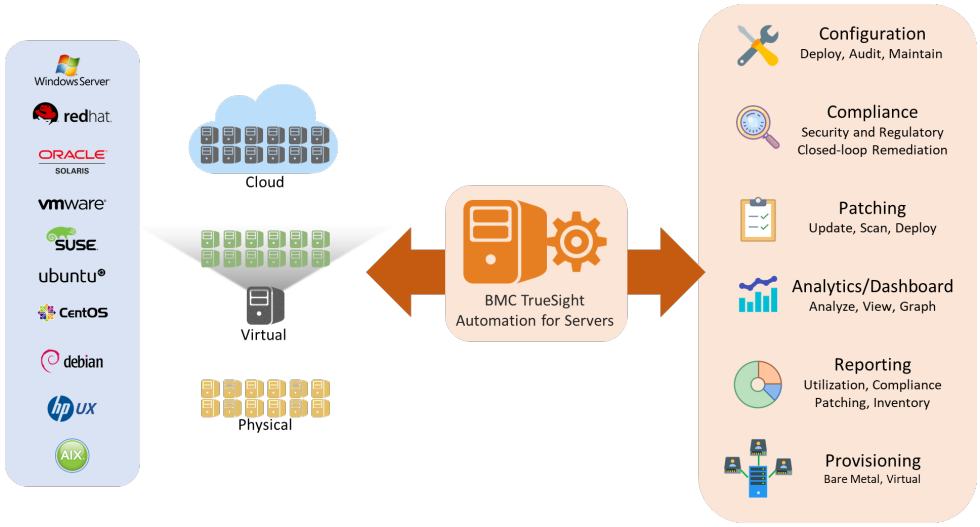
- *Vulnerability management:* Import—automatically or manually—vulnerability scan data from popular vulnerability scanning solutions, and map the vulnerabilities found to managed assets and the business services they support. Apply intelligence and advanced analytics to help prioritize remediation efforts and build remediation plans. Visualize the overall security state of the server estate and track progress as vulnerabilities are addressed. (The associated Vulnerability Dashboard can reside either on-premises or in the cloud.)
- *Patch automation:* Define patch policies to regularly check for missing patches. Provide lines of business and application owners with self-service patching to address missing patches and fix vulnerabilities, minimizing business disruption and decreasing the time it takes to secure your environment.
- *Compliance Automation:* Scan server environment to identify compliance issues with out-of-the-box (OOB) support for common regulatory standards, including CIS, DISA, HIPAA, PCI-DSS, and SOX. Track non-compliance and integrate remediation with change processes to be audit-ready.
- *Configuration Management:* Define standardized server configurations and identify any drift. Maintain configurations through automated remediation.
- *Service Provisioning:* Provision physical and virtual servers provisioning. Automate software deployment and OS hardening.
- *Reporting:* View real-time and historical configuration information via easy-to-use dashboards, with OOB reports for compliance, inventory, provisioning, patching, and job execution activities.
- *Task automation:* Incorporate customized tasks such as network shell commands, preexisting scripts, or configuration changes to automate tasks from end-to-end.

To automate management of cloud-based resources, TSAS leverages Smart Agents. A Smart Agent generates requests to automatically enroll new targets, such as Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instances, in TSAS, and communicates with an Application Server[2] via a Smart Hub. The Smart Agent can reduce the time and effort spent on

[2] An Application Server controls communication between TSAS components and remote servers and databases.

enrolling new targets and provides up-to-date information about the state of each Remote System Call Daemon (RSCD)[3] agent.

Figure 2. BMC TrueSight Automation for Servers

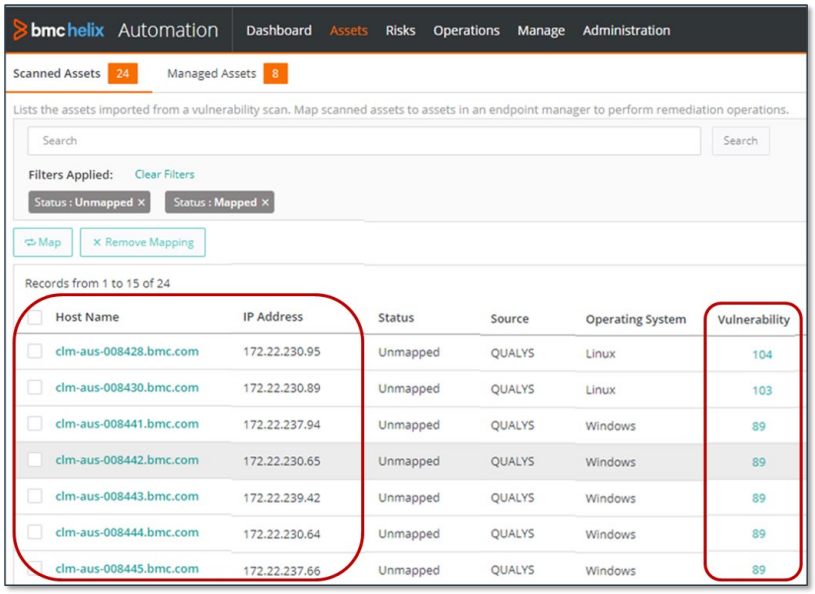


Source: Enterprise Strategy Group

TSAS integrates with BMC Discovery solutions to gather additional application/business service context about servers deployed in the IT environment. It also integrates with common IT service management solutions to help in logging vulnerability and compliance incidents, generate change requests, and submit for approval to authorize remediation actions. TSAS applies intelligence to quickly identify, prioritize, and fix security vulnerabilities and manage the compliance status of on-premises and cloud infrastructure.

ESG Tested

ESG performed remote testing of BMC TSAS version 20.02. Testing focused on automated vulnerability management, simplified patching, and compliance.



ESG began by importing security scanner data to identify existing server-related vulnerabilities within an IT environment (see embedded figure to the left). To detect vulnerabilities, many organizations use vulnerability scanners from vendors such as Qualys, Tenable, and Rapid7. These tools produce large reports that must be parsed, analyzed, and compared to available remediations.

TSAS uses a lightweight agent to communicate with each application server using an encrypted "speak when spoken to" protocol or Smart Agents. SSH or other transport is not required. Server connections can be made quickly and scale easily.

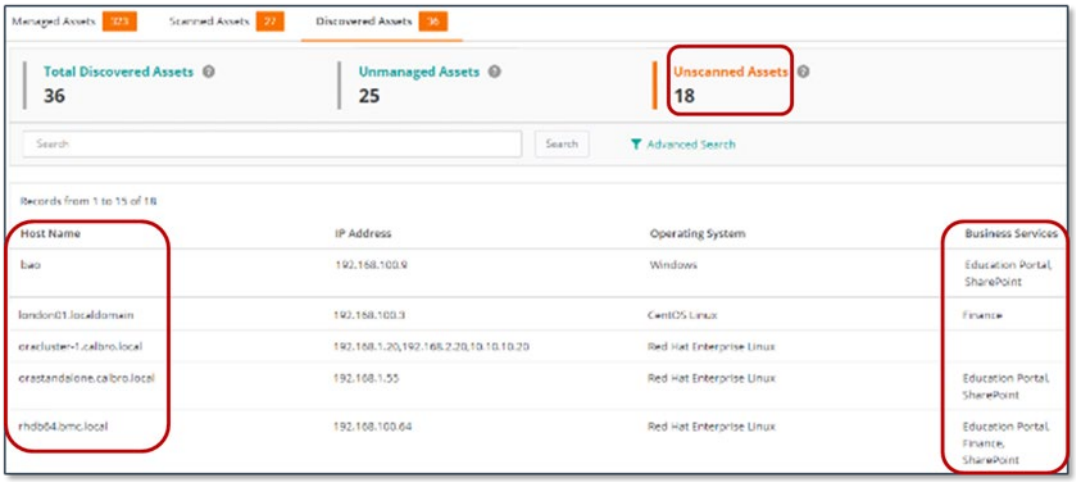
[3] An RSCD agent is software that must be installed and running on each remote server that TSAS accesses.

By inventorying servers in the current environment and counting outstanding vulnerabilities, an administrator can begin to assess outstanding issues to address.

ESG proceeded to integrate our scanned data with BMC Discovery Data. While the scanned data uncovered vulnerable spots, BMC Discovery generated a list of servers overlooked by the initial security scan conducted (or server blind spots). After integrating our security scan data with the data from BMC Discovery, ESG saw that there are an additional 18 servers to examine (see Figure 3). We also saw the applications running on these servers.

ESG saw how the integration of both sets of data helps to gain more visibility into the current IT environment and the extent of vulnerabilities to address. An administrator could use this information to know other servers that may be exposed to vulnerabilities and warrant further attention. Also, the administrator could see those applications that are at risk on these discovered assets.

Figure 3. Integration of Scanned and BMC Discovery Data

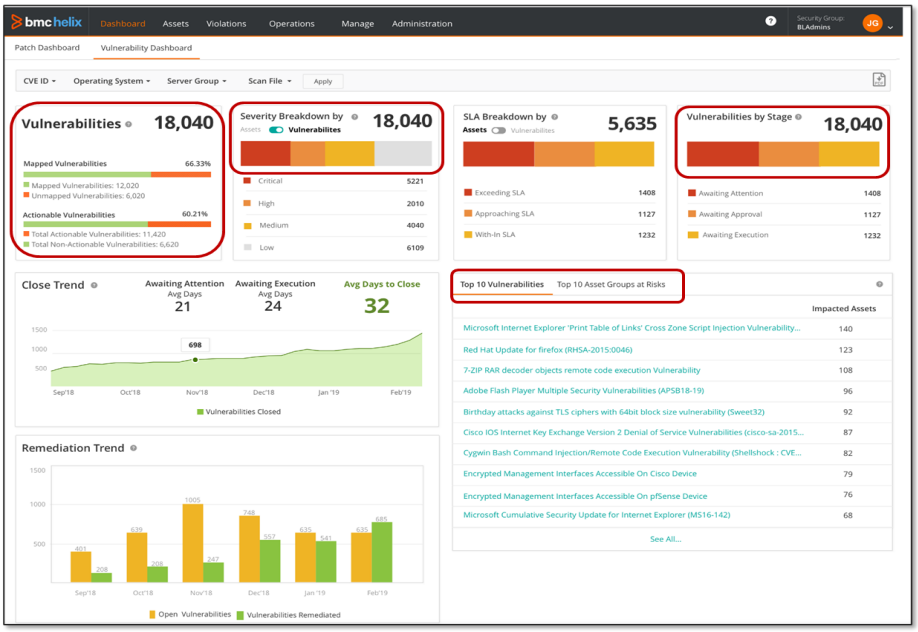


Once data has been integrated, ESG observed how an administrator can map scanned data to all uncovered assets. By taking this step, TSAS automatically discovered servers that require the most attention based on current business needs. Although the administrator has uncovered a large number of existing vulnerabilities shown in the previous screens, mapping and risk scoring can help to prioritize issues to resolve.

After mapping hosts to vulnerabilities, ESG then viewed the Vulnerability Dashboard (see Figure 4) and noted three details:

- A total of 18,040 vulnerabilities were uncovered and categorized by severity level—Critical, High, Medium, and Low.
- Stage of addressing identified vulnerabilities—Awaiting Attention, Approval, or Execution.
- Lists of the top ten vulnerabilities and top asset groups (servers) at risk.

Figure 4. BMC TSAS – Vulnerability Dashboard



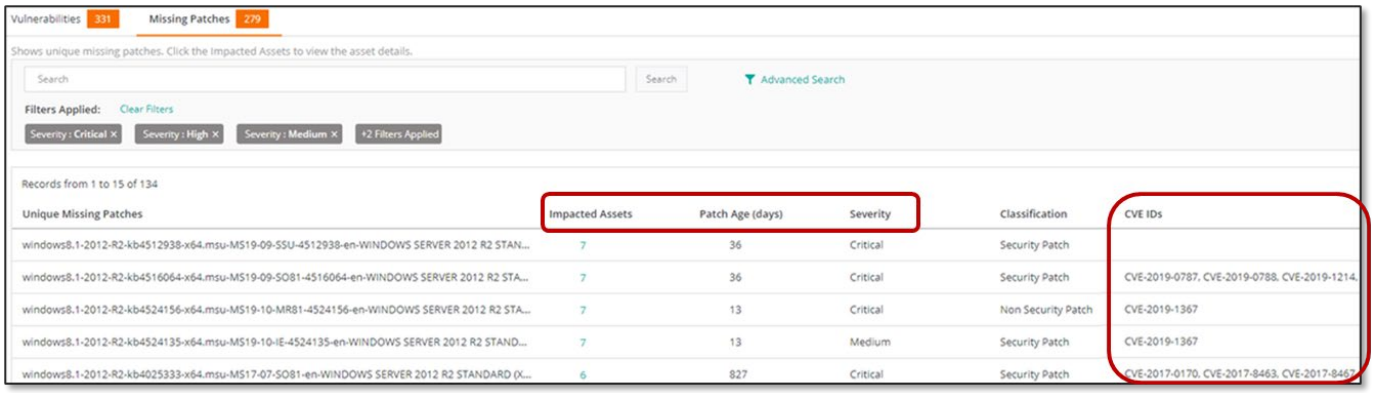
With these specific details, ESG noted how an administrator can assess the current situation, be aware of the criticality of vulnerabilities, know current status, and determine which issues to prioritize based not just on affected hosts but, more importantly, the applications that may be affected negatively. This dashboard ultimately provided a consolidated view to help determine what actions to take.

ESG also observed how the integration of previously collected data and the Vulnerability Dashboard can save time and effort in evaluating patterns and trends and, more importantly, prioritizing which vulnerabilities to address. Performing such tasks and integrating data manually from multiple point solutions can be time-consuming. The more time spent on such tasks, the longer the IT environment remains exposed to the exploitation of a vulnerability or security breach.

ESG then reviewed the **Missing Patches** dashboard (see Figure 4). The list revealed patches that have yet to be installed to protect an organization's servers from existing vulnerabilities. Compiling this list involves patch catalog updates automatically collected for a myriad of operating systems (OSs), such as Red Hat Linux, Solaris, Ubuntu, SuSE Linux, and Microsoft Windows.

To determine the vulnerabilities that the patch can address, ESG noted that the dashboard enables the administrator to refer to Common Vulnerabilities and Exposures (CVE), a list of publicly disclosed computer system security flaws that is free for download and use (see Figure 5). IT teams have traditionally used this list, augmented by vulnerability risk scoring, to prioritize security efforts and proactively address areas of exposure or vulnerability.

Figure 5. BMC TSAS – Tallying Missing Patches

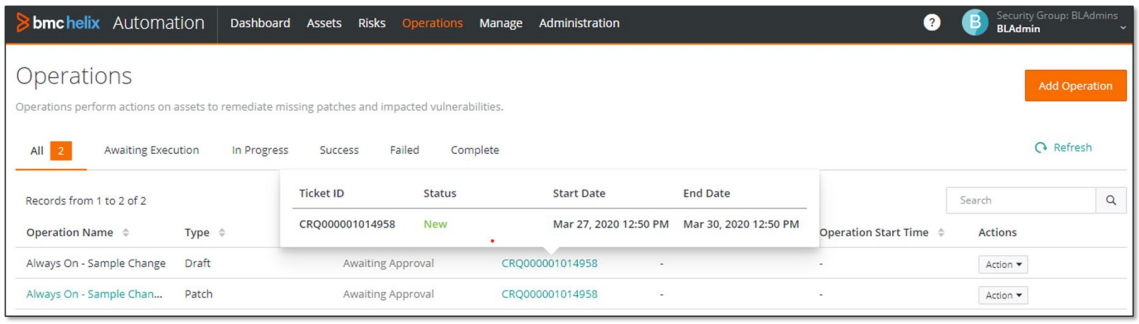


Along with the patch name, the dashboard revealed the age of the patch, the severity of not installing the patch, and the number of assets to be impacted when the patch is installed. Using the information collected in the dashboard, an administrator can assess the patches to immediately install based on the associated details provided. For example, many patches may be classified "Critical," but based on the patch age and the vulnerabilities addressed according to the corresponding CVEs, an administrator can prioritize installation of one patch over others.

While ESG noted that TSAS helped identify vulnerabilities within an organization's server footprint, we also saw how TSAS can support DevSecOps in maintaining the overall security of development environments. As DevOps employ more agile development practices to continuously deliver code updates, security vulnerabilities still need to be recognized and managed. Automation can help to reduce this risk in DevOps practices so that business demands are continuously met.

ESG then examined how an administrator can view and automate how vulnerabilities are resolved. We navigated to the **Operations** tab of the TSAS interface and examined two operations already entered (see Figure 6). Depending on the vulnerabilities or patches that an administrator wants to address, an operation can coordinate multiple actions and automate their execution. Specific tasks executed by an operation include ticket creation, change scheduling, approvals, execution, deployment verification, closure, and documentation.

Figure 6. BMC TSAS – Automated Change Management

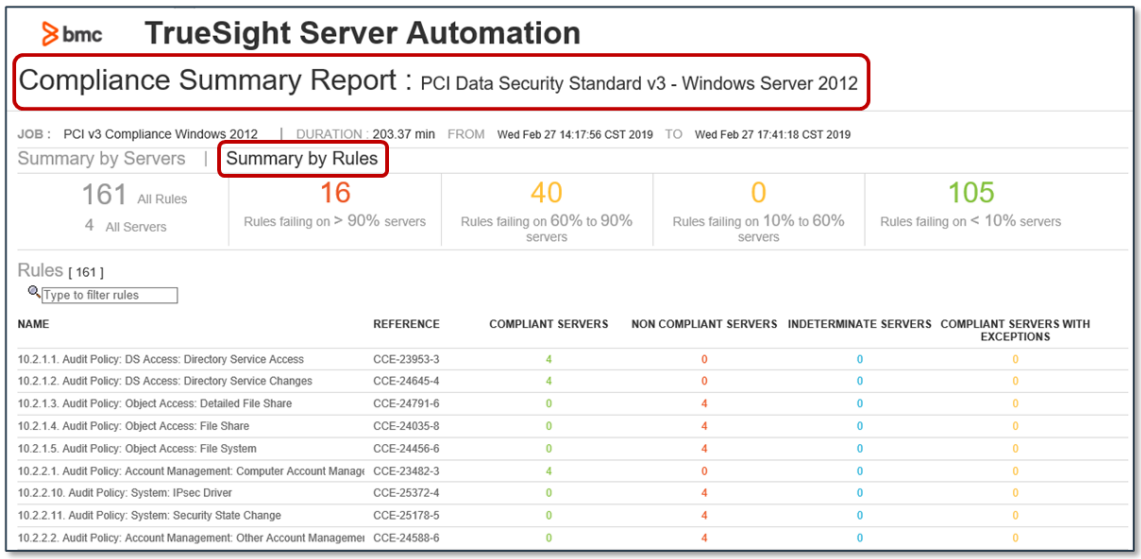


ESG noted that the ability to coordinate actions for remediating a vulnerability or applying a patch using one interface is invaluable, as opposed to using multiple system interfaces. We saw how the ability to initiate and automate change management activities from a single interface can decrease time and resources related to maintenance. Automating change management can also help DevOps to focus on developing and releasing applications instead of managing changes to their infrastructure.

Next, ESG reviewed how TSAS helps to determine compliance status based on existing regulations. We focused on assessing compliance against PCI Data Security Standard v3 for Windows Server 2012. With TSAS, continuous updates are made to compliance regulations, rules, and remediation tasks for all supported operating systems. In Figure 7, ESG saw how TSAS

revealed the current compliance status, based on the latest updates to the PCI standard. We noted the level of detail in this report, including the total number of servers affected, the extent of rule violation across all servers, and the breakdown on the level of non-compliance by server.

Figure 7. Auditing Compliance by Rules



bmc TrueSight Server Automation

Compliance Summary Report : PCI Data Security Standard v3 - Windows Server 2012

JOB : PCI v3 Compliance Windows 2012 | DURATION : 203.37 min FROM Wed Feb 27 14:17:56 CST 2019 TO Wed Feb 27 17:41:18 CST 2019

Summary by Servers | Summary by Rules

161 All Rules
4 All Servers

16 Rules failing on > 90% servers
40 Rules failing on 60% to 90% servers
0 Rules failing on 10% to 60% servers
105 Rules failing on < 10% servers

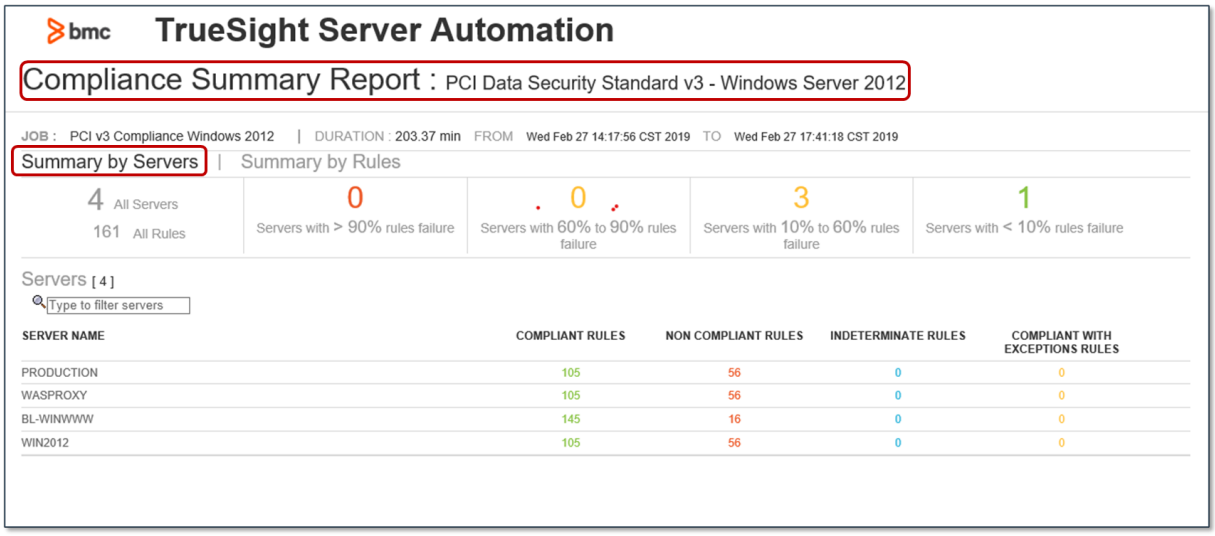
Rules [161]

Type to filter rules

NAME	REFERENCE	COMPLIANT SERVERS	NON COMPLIANT SERVERS	INDETERMINATE SERVERS	COMPLIANT SERVERS WITH EXCEPTIONS
10.2.1.1. Audit Policy: DS Access: Directory Service Access	CCE-23953-3	4	0	0	0
10.2.1.2. Audit Policy: DS Access: Directory Service Changes	CCE-24645-4	4	0	0	0
10.2.1.3. Audit Policy: Object Access: Detailed File Share	CCE-24791-6	0	4	0	0
10.2.1.4. Audit Policy: Object Access: File Share	CCE-24035-8	0	4	0	0
10.2.1.5. Audit Policy: Object Access: File System	CCE-24456-6	0	4	0	0
10.2.2.1. Audit Policy: Account Management: Computer Account Manage	CCE-23482-3	4	0	0	0
10.2.2.10. Audit Policy: System: IPsec Driver	CCE-25372-4	0	4	0	0
10.2.2.11. Audit Policy: System: Security State Change	CCE-25178-5	0	4	0	0
10.2.2.2. Audit Policy: Account Management: Other Account Manageme	CCE-24588-6	0	4	0	0

We also reviewed how TSAS determines compliance by server. In Figure 8, ESG saw how TSAS shows the level of PCI standard compliance for four servers operating on Windows Server 2012 (see Figure 8). (OOB content is available for other flavors of Windows and other operating systems.)

Figure 8. Auditing Compliance by Server



bmc TrueSight Server Automation

Compliance Summary Report : PCI Data Security Standard v3 - Windows Server 2012

JOB : PCI v3 Compliance Windows 2012 | DURATION : 203.37 min FROM Wed Feb 27 14:17:56 CST 2019 TO Wed Feb 27 17:41:18 CST 2019

Summary by Servers | Summary by Rules

4 All Servers
161 All Rules

0 Servers with > 90% rules failure
0 Servers with 60% to 90% rules failure
3 Servers with 10% to 60% rules failure
1 Servers with < 10% rules failure

Servers [4]

Type to filter servers

SERVER NAME	COMPLIANT RULES	NON COMPLIANT RULES	INDETERMINATE RULES	COMPLIANT WITH EXCEPTIONS RULES
PRODUCTION	105	56	0	0
WASPROXY	105	56	0	0
BL-WINWWW	145	16	0	0
WIN2012	105	56	0	0

With both reports, an administrator can quickly assess the extent of non-compliance against any standard at any given time. ESG can see how TSAS saves both time and effort in deriving this level of detail. Instead of having to manually determine compliance of every server across all applicable standards (depending on the applications being run), TSAS automatically determines compliance and enables an administrator to take automated corrective action.

Why This Matters

Maintenance windows are not what they used to be—in many organizations, maintenance windows are down to a few hours per month instead of a day every weekend. Keeping servers manually patched and in compliance with security and regulatory requirements is difficult.

ESG validated that BMC TSAS can do the heavy lifting, updating patch catalogs and compliance rules intelligently across operating systems, auditing the server environment, and remediating with just a few clicks. Organizations can manage OS and security patching and regulatory compliance with a fraction of the resources they would otherwise need. While other solutions might simplify a compliance audit, they provide no tools to fix what you find. TSAS provides "closed-loop remediation" in order to act immediately on what the audit discovers. Organizations can always be audit-ready. Failure to comply with regulations can have serious consequences, including significant fines, reputational harm, and lost revenue; TSAS's compliance capabilities can help organizations stay out of trouble with minimal cost and effort.

The Bigger Truth

Server management may not seem exotic and exciting, but it is crucial for a well-functioning IT infrastructure. Myriad tasks must be completed to maintain golden image configurations, keep systems patched with the latest operating system updates, ensure security using automated vulnerability management, and keep systems in line with corporate governance and regulatory compliance mandates. However, the pace of business today does not allow for stale processes that take a long time. Whether you have hundreds, thousands, or hundreds of thousands of servers, automating configuration, patching, and compliance processes are essential. For most organizations, time-consuming server management tasks take skilled labor away from more strategic activities.

BMC TSAS offers a solution with extensive automation that can make your environment more secure and functional in a timely fashion, and still retain the flexibility you need to manage servers as your organizational needs demand. TSAS enables intelligent, policy-based task automation to avoid unintended changes and outages, increase consistency, reduce errors and omissions, and free up staff time.

ESG validated that TSAS provides configuration, patching, and compliance capabilities that can simplify server management, improve productivity, and reduce costs and risk. The ability to conduct automated nightly security compliance audits and automatically remediate non-compliant conditions reduces risk by enabling timely corrective action. And, instead of getting systems compliant occasionally for an auditor, organizations can actually be compliant all the time. After all, patching and compliance updates are designed to add functionality to your environment, increase security, and protect you from penalties. They are not just a thorn in the side of IT administrators.

ESG was impressed with the capabilities that TSAS delivers. It can help IT transform from a reactive "fire fighter" to a proactive service provider, ensuring smoother server operations across thousands of endpoints, for both IT administrators and DevOps teams.