ESG Lab Review

BMC's TrueSight Server Automation (Formerly, BladeLogic Server Automation)

Date: June 2018 **Author:** Kerry Dolan, Senior IT Validation Analyst

Abstract

This ESG Lab Review documents remote testing of BMC's TrueSight Server Automation (TSSA), formerly BladeLogic Server Automation solution, with a focus on configuration, patching, and compliance features.

The Challenges

When ESG research respondents were asked about their most important considerations for justifying 2018 IT investments, improved security/risk management, increased employee productivity, business process improvement, and improved regulatory compliance each made the top ten most often cited considerations.[1] These can all be improved with better management of the server infrastructure. Administrators 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, regulatory fines, and productivity drains.

Figure 1. Top Ten Most Important Considerations for Justifying 2018 IT Investments

Source: Enterprise Strategy Group

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, and free up IT staff time for strategic projects.

[1] Source: ESG Research Report, *2018 IT Spending Intentions Survey*, February 2018.

The Solution: TrueSight Server Automation

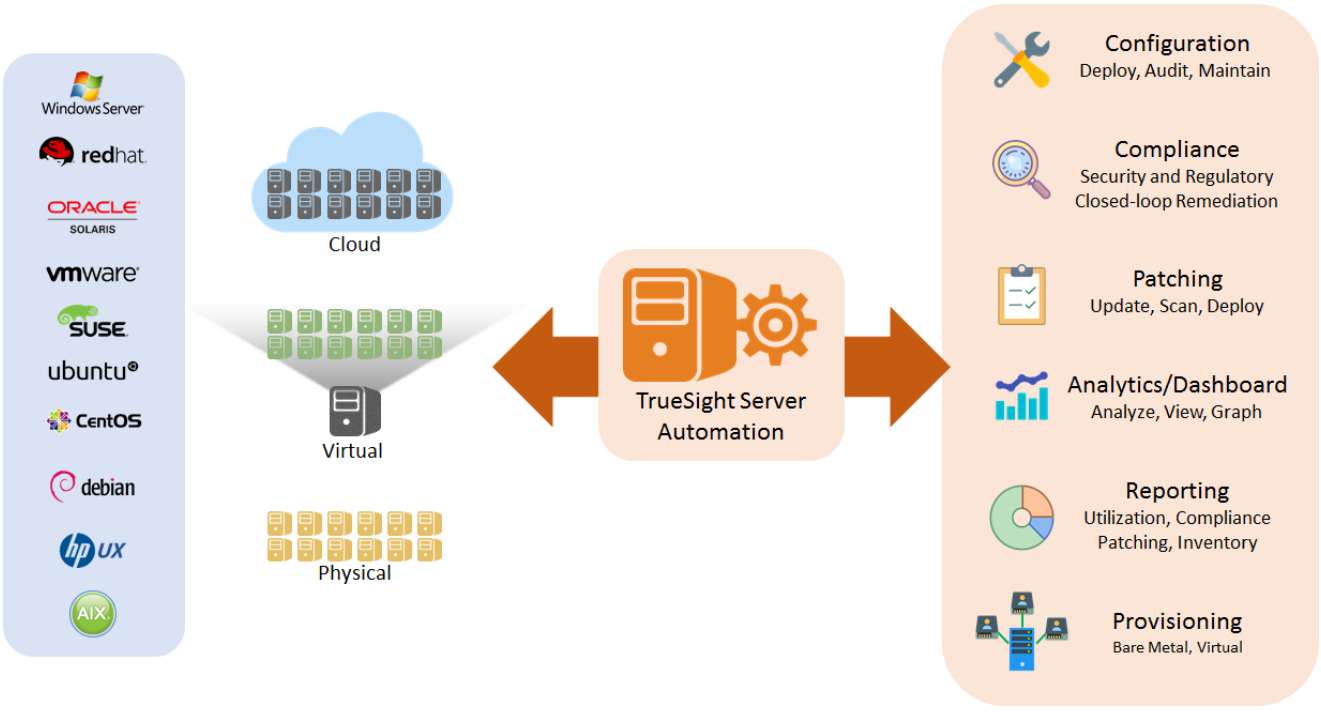
TSSA is part of the BMC data center automation suite that also includes network and process automation. Organizations use TSSA to manage physical, virtual, and cloud servers across Windows, Linux, and UNIX operating systems through a single pane of glass. TSSA also enables precise changes to be executed with fine-grained, role-based access that keeps systems secure and stable.

At a high level, TSSA helps IT to not just manage servers and understand their status, but also actively remediate problems—without requiring scripting. Organizations can discover servers, audit their configurations, make changes to configurations, and deploy software quickly and easily. If a change to an individual system or group doesn't work as expected, administrastors can quickly roll it back, saving time and reducing risk. This comprehensive ability to identify problems *and fix* them is a key aspect of the solution. TSSA enables administrators to employ a policy-based, consistent, reliable server management regimen with less administrative effort and cost. TSSA features simplify:

- *Compliance*. Discover, monitor, remediate, and integrate change control to remain compliant and audit-ready. Preconfigured regulatory policies include CIS, DISA, HIPAA, PCI-DSS, SOX, and more.
- *Patching*. Control server lifecycles with regular patching to optimize new features and maintain security, while reducing downtime.
- *Configuration*. Automatically maintain configurations to organizational standards with granular control.
- *Provisioning*. Receive OS-aware packaging, unattended installs, and provisioning through image-, script-, or template-based approaches.
- *Reporting*. View real-time and historical details and dashboards for compliance, inventory, provisioning, patching, and deployment.
- *Task-automation.* Incorporate customized tasks such as network shell commands, preexisting scripts, or configuration changes to automate end-to-end tasks.

TSSA is integrated with IT service management and governance processes, including other BMC solutions such as TrueSight Vulnerability Management and Remedy.

Figure 2. BladeLogic Server Automation



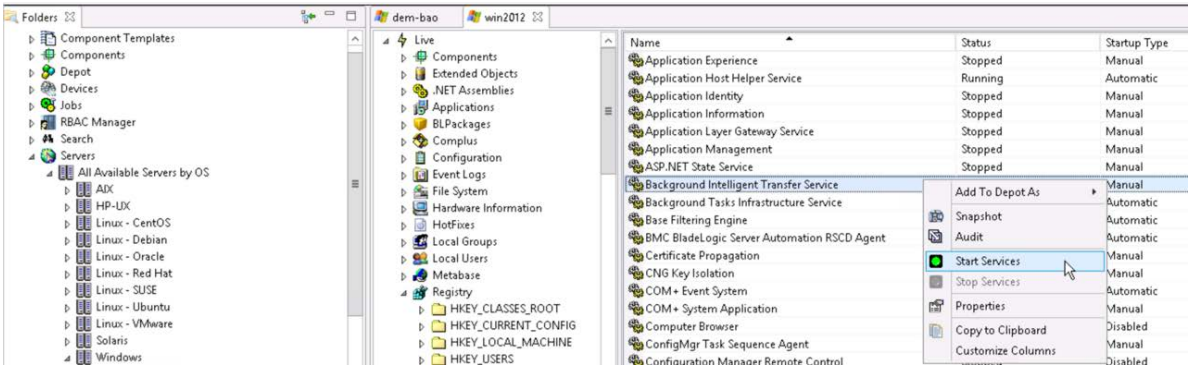
Source: Enterprise Strategy Group

ESG Lab Testing

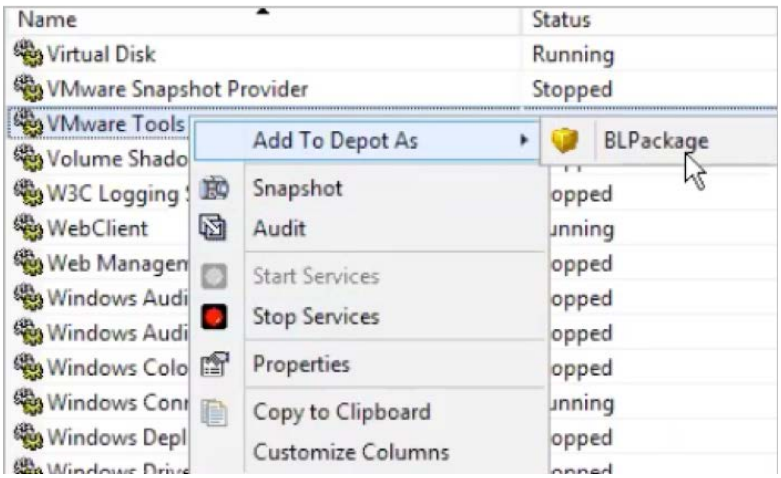
ESG Lab performed remote testing of TSSA on a test bed in Phoenix, AZ, leveraging TSSA version 8.9 on a Windows 2012 R2 Standard server with 16 GB of RAM. The test bed included Windows 2008 and 2012, Red Hat and SUSE Linux, Ubuntu, Debian, and Oracle Solaris servers. Testing focused on configuration, compliance, and patching capabilities. For this validation, ESG used the client user interface that is targeted toward expert users. TSSA has a separate web portal-based interface for operators or infrequent users that is easier to use, but less functional than the client user interface. It should be noted that this testing covered only a subset of the extensive capabilities that TSSA offers.

Configuration

ESG Lab started by examining the ***Live Browse*** feature. For any server, we could view details including hardware, memory, compute resources, boot history, domain role, etc. TSSA uses a powerful but lightweight agent to communicate with each application server. Because it uses a proprietary, encrypted "speak when spoken to" protocol, it doesn't require SSH or other transport; this enables it to make server connections quickly and scale easily. For each server, we could view installed objects and services, drill down to individual items, and take actions such as starting services, snapshots, and audits. The screenshot above shows the objects available for the Windows application *blapp*.

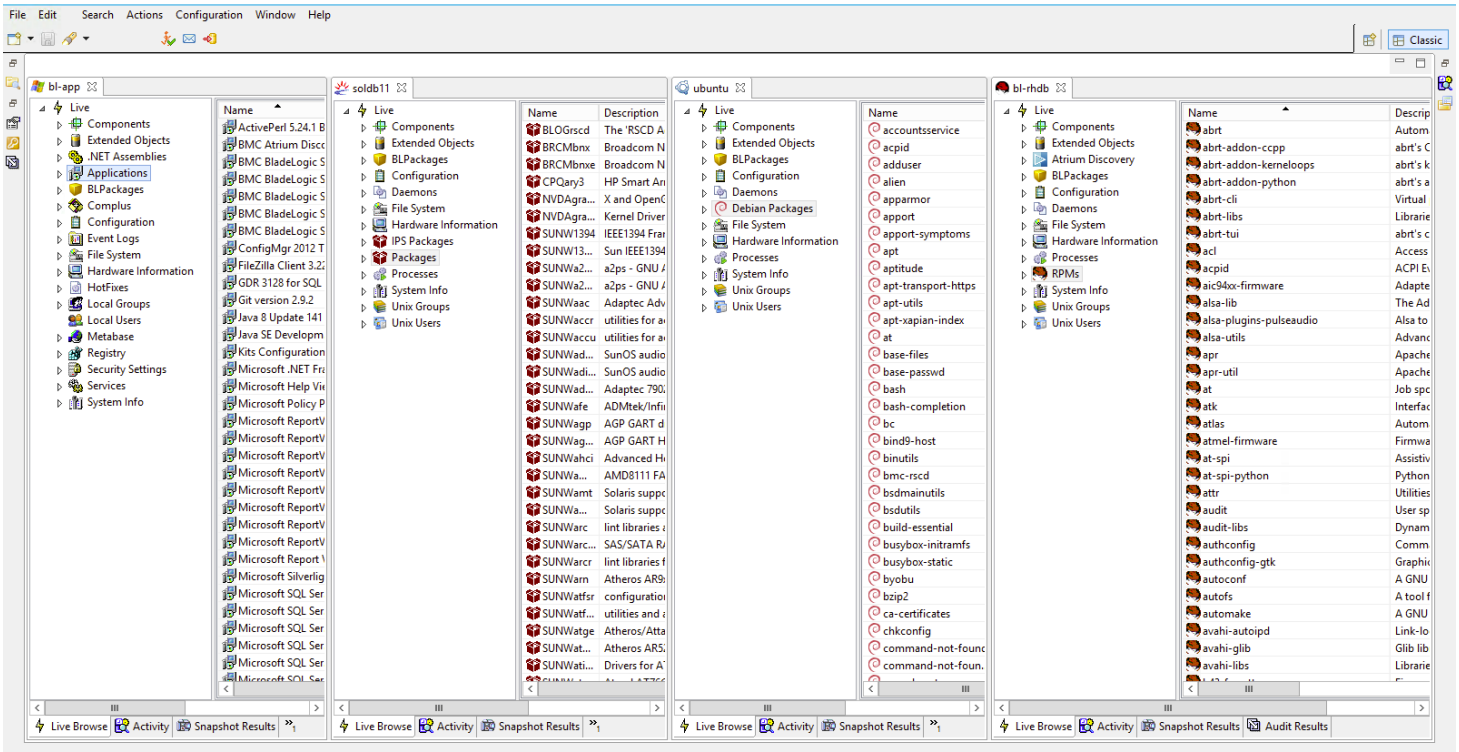


TSSA makes it easy to capture even a single configuration from an endpoint and package it for deployment or remediation. After drilling down on ***Services*** for *blapp*, ESG Lab selected *VMware Tools*, right-clicked, and selected ***Add to Depot as BL Package***. TSSA then created the software package and saved it. This process is vastly simpler than building a service from CLI or trying to script it. In addition, this fine-grained ability to track a single service, rather than the entire services table with multiple objects, makes the process faster, easier, and more reliable. It is equally simple and fast to right-click on ***Audit*** to compare with other systems in the environment, or ***Snapshot*** to do change tracking or to preserve the system state. In addition, TSSA understands the different formats that operating systems use, so it can parse configurations and capture them without error, enabling administrators to change a single configuration across the entire environment. Software can also be uninstalled with a simple right-click.



A key attribute is that TSSA tasks have the same look and feel across different platforms. Figure 3 shows four servers with four different operating systems in the same TSSA GUI: a Windows server with Applications open; an Oracle Database 11 on Solaris with Packages open; an Ubuntu server with Debian Packages open; and a Red Hat Linux server with RPMs open. This enables the administrator to manage all the systems across the environment with the same tool, at the same time, with the same look and feel.

Figure 3. Consistent Cross-platform Look and Feel



Source: Enterprise Strategy Group

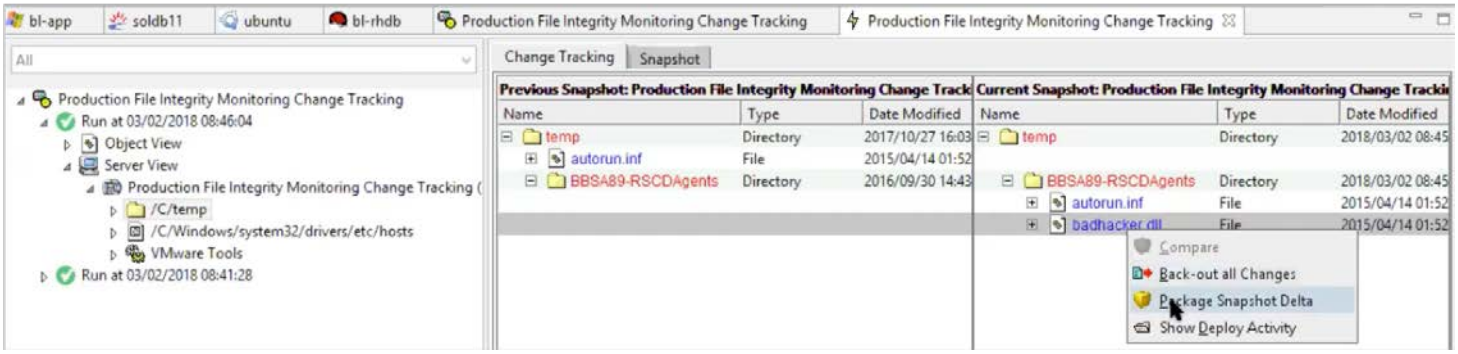
Creating a Snapshot for File Integrity Tracking

ESG Lab executed configuration tasks, starting with a snapshot of the environment to use for file integrity change tracking. The simple steps enable administrators to choose the number of servers to snap, and to select specific server objects and configurations, with notifications and scheduling. We could select specific servers or smart groups tailored to company needs, such as particular compliance status, application tier, location, department, etc. ESG Lab configured the snapshot to capture the *C:/temp* folder, *C/Windows/system32/drivers/etc/hosts* configuration file, and *VMware tools* Windows service for the *blapp* server. Once we had clicked ***Finish***, we watched as TSSA captured information.

Next, to simulate changes that can occur in the real world, we added two files to the *BBSA89-RSCDAgents* subfolder in the *C:/temp* folder for *blapp*: *autorun.inf* represented an authorized change, and *badhacker.dll* represented an unauthorized change. ESG Lab next viewed the process of auditing the environment for changes by rerunning the snapshot job on *blapp*. An advantage of TSSA is that this snapshot only collects changed data, making it fast and low-cost. If there are no changes, or only a megabyte here and there, that's all TSSA collects. Other solutions take a full snapshot of the environment, taking up storage space, time, and cost.

In this snapshot, the *temp* folder in the ***Snapshot*** window was displayed in bold, red text to indicate changes, including the date of modification; the folders that had no changes were not displayed in that screen. Drilling down in the changed folder, we noted the two files that had been added. Change tracking can also be scheduled and reconciled against authorized changes using change management systems such as BMC Remedy.

We could roll back all the changes in an automated fashion. In this case, TSSA automatically creates and launches a ***BL Deploy*** job. However, part of TSSA's power is the ability to roll back only a single change, which we did by right-clicking on *badhacker.dll* and selecting ***Package Snapshot Delta***. With a few clicks—and no scripts—we configured TSSA to create a package to roll back that change.



To deploy it, we created a ***BL Deploy*** job. This includes sending a change management approval request if needed, and configuring the target server, notifications, and scheduling. Options include:

- Administrators can schedule tasks to be simulated, staged, and committed at different times. For example, they can simulate a task at 3 pm to be sure the right permissions and storage are in place, then schedule it to be staged at 8 pm and finally committed at 11 pm at the beginning of the maintenance window. This way, the task begins immediately, rather than having the administrator simulate and stage it, taking up part of the maintenance window.
- Jobs can be configured to pause when the maintenance window ends and start up again with the next window. This prevents the job from continuing into production time and requiring a disruptive reboot.
- TSSA enables administrators to automatically create a change control ticket or tie into an existing ticket, saving valuable administrative time.
- Administrators can use either native software packaging technologies for each operating system or TSSA packaging (such as BL deploy) that lets them intelligently interact with multiple operating systems without the complication of different packaging technologies.

Once this task was completed, *badhacker.dll* was no longer configured in the *C:/temp* folder. We also looked at a similar task using the ***Audit*** job, which many organizations use to keep servers configured to a defined standard, such as to a "golden image." With this task, the changes (such as extra or missing files) are listed in a separate window, making it easy for administrators of large server farms to identify non-compliant servers and bring them into compliance.

Why This Matters

Keeping hundreds or thousands of servers optimally configured is a daunting task that takes up significant IT administrator time—and administrators are expensive. Manual server management and scripting are also error-prone. Multiple platforms—Windows, several flavors of Linux, and legacy systems like AIX, all with numerous versions to support—complicate management even further, especially with multiple, separately managed point tools that provide different capabilities.

ESG Lab validated that TSSA provides a single server management tool with configuration automation that supports numerous platforms with the same look and feel, simplifying tasks and saving time and money. With TSSA, junior staff can manage servers, freeing up high level administrators for more strategic projects. Organizations eliminate concerns about server tools working together, and users can leverage the applications they want without complicating server management. TSSA enables policy-based management and ongoing validation so that servers maintain the right capabilities and avoid conflicting changes and chaos.

Patching and Compliance

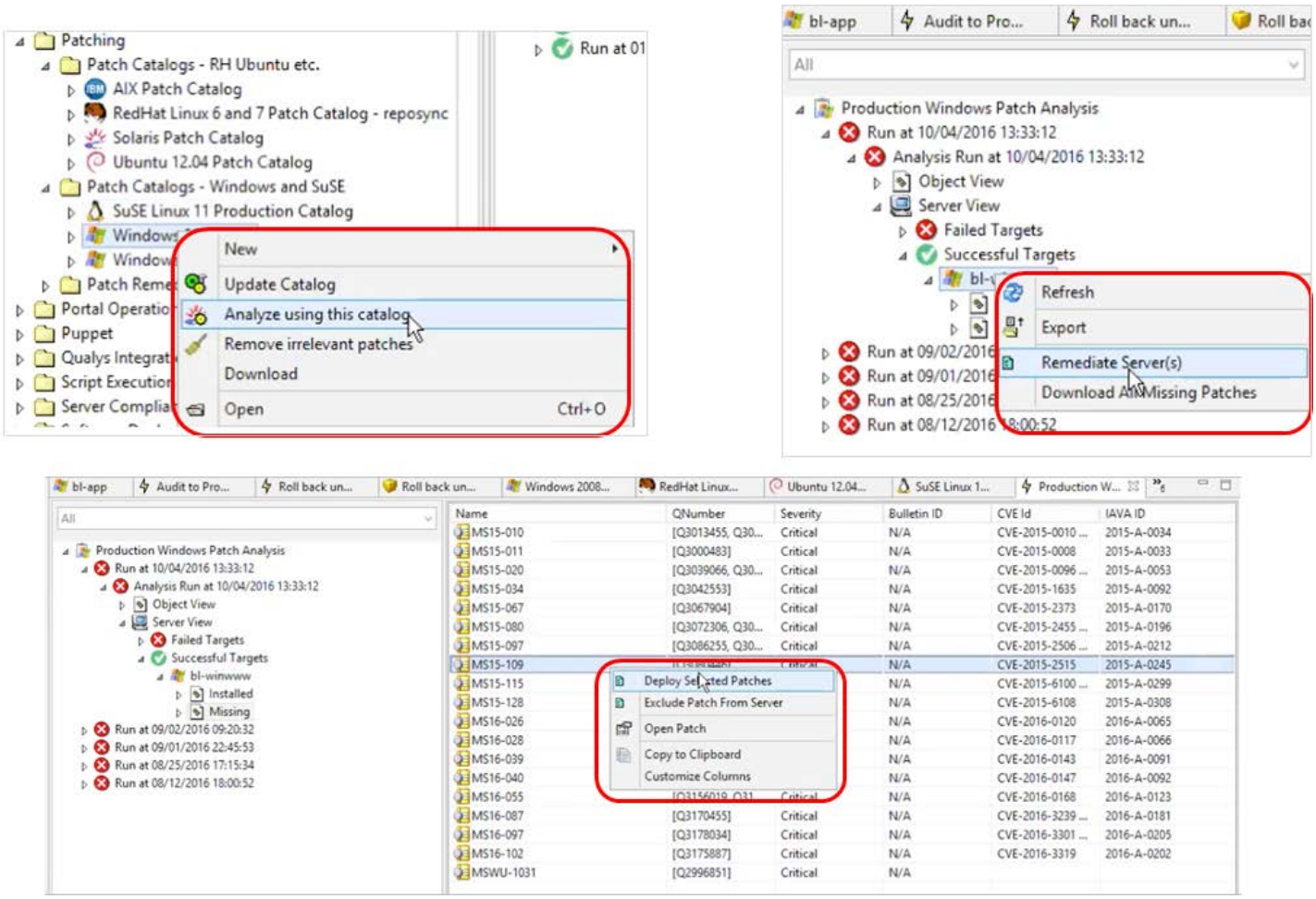
Patching and compliance tasks are essential for optimizing functionality, reducing risk, and maintaining security levels. TSSA automation can accomplish these goals while gaining back productive time.

Patching

Keeping servers up to date with OS patches across platforms is a tedious, time-consuming task, and TSSA automates that process. The top left side of Figure 4 shows patch catalogs for AIX, Red Hat Linux, Solaris, Ubuntu, SuSE Linux, and Windows all in one screen. Catalog updates can be scheduled to run on a regular basis. From the Windows patch catalog, ESG Lab right-clicked and selected ***Analyze using this catalog*** to get the patch status of a set of Windows servers in the environment. The analysis showed which servers were missing which patches, including bulletins and hotfixes, and their severity rating.

The top right of Figure 4 shows failed and successful targets; in this case, three of the servers were unavailable, hence the red Xs. From the ***Successful Targets*** list, ESG Lab selected the *blwinwww* server, and had options to remediate all servers or download missing patches. We drilled down on that server to show installed and missing patches (Figure 4, bottom). After selecting one of the critical patches, we right-clicked and selected ***Deploy Selected Patches***. We had options to complete them now or to simulate, stage, and commit them later. With the flexibility to remediate all servers and patches, or to select specific servers and/or patches, organizations have the power to optimize the server environment to suit their needs.

Figure 4. Patching and Remediation



Source: Enterprise Strategy Group

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. BMC has a solution called TrueSight Vulnerability Management (TVSM) that can import these vulnerability scans, automatically map vulnerabilities to known remediations, assign severity, and help operators prioritize remediation actions. TSVM works with patching solutions including TSSA to execute remediation actions such as patching or configuration changes. TSVM was not part of this ESG Lab validation.

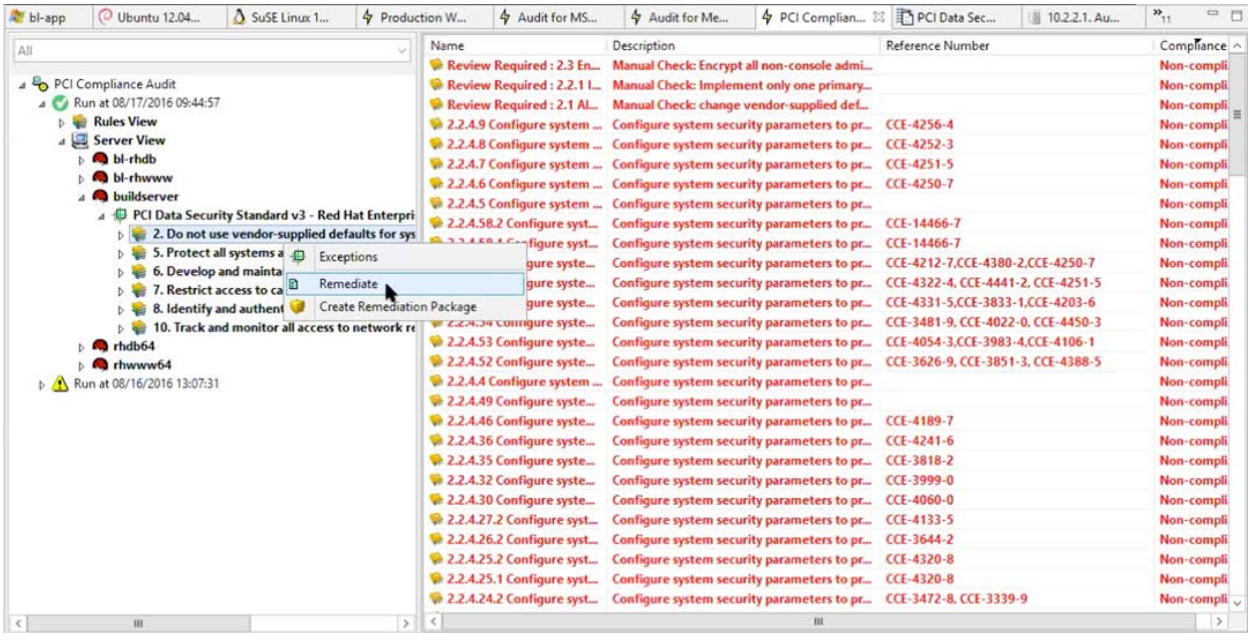
Compliance

TSSA also provides out-of-the-box compliance templates for numerous regulations across industries, including SOX, DISA, HIPAA, PCI-DSS, CIS, and more. These regulations may be mandatory depending on the industry, country, or organization's business activities. But even if not mandatory, compliance may help bolster the security posture of the organization and improve standardization, leading to better stability and performance. The templates provided by TSSA describe the requirements that must be met at a server configuration level, enabling administrators to more easily audit the entire environment for compliance. Administrators can view each rule and drill down into the details of the condition and remediation activities.

A distinguishing feature of TSSA is that remediation packages can be deployed to bring your servers back into compliance. Typically, administrators must translate the compliance standards into server administration rules on their own, and then create scripts to both audit their environments and remediate individually for each operating system—a complex, continual task. TSSA employs a team to continually update the compliance rules and write remediation tasks for all supported operating systems. Administrators need only a few clicks to go from audit through remediation.

In many organizations, preparing for a compliance audit by a regulatory agency strikes panic, resulting in teams of people working for weeks to document the state of their servers since the last audit. Once the audit is complete, they must then spend time designing and implementing a remediation plan. This takes significant corporate resources. With TSSA, organizations can continually audit and update their status, and can remediate with just a mouse click (see Figure 5), including exception handling for flexibility. In addition, TSSA's extensive reporting features include drill down into compliance rules, definitions, and reasons why servers are/were not compliant at any time period, details that can prove the level of compliance over time to auditors.

Figure 5. One-click "Closed-loop" Remediation for Compliance



Source: Enterprise Strategy Group

In addition, compliance checks are done on the TSSA infrastructure, not on the endpoints. As a result, organizations can expand their compliance checks without taxing endpoints and causing productivity interruptions.

Why This Matters

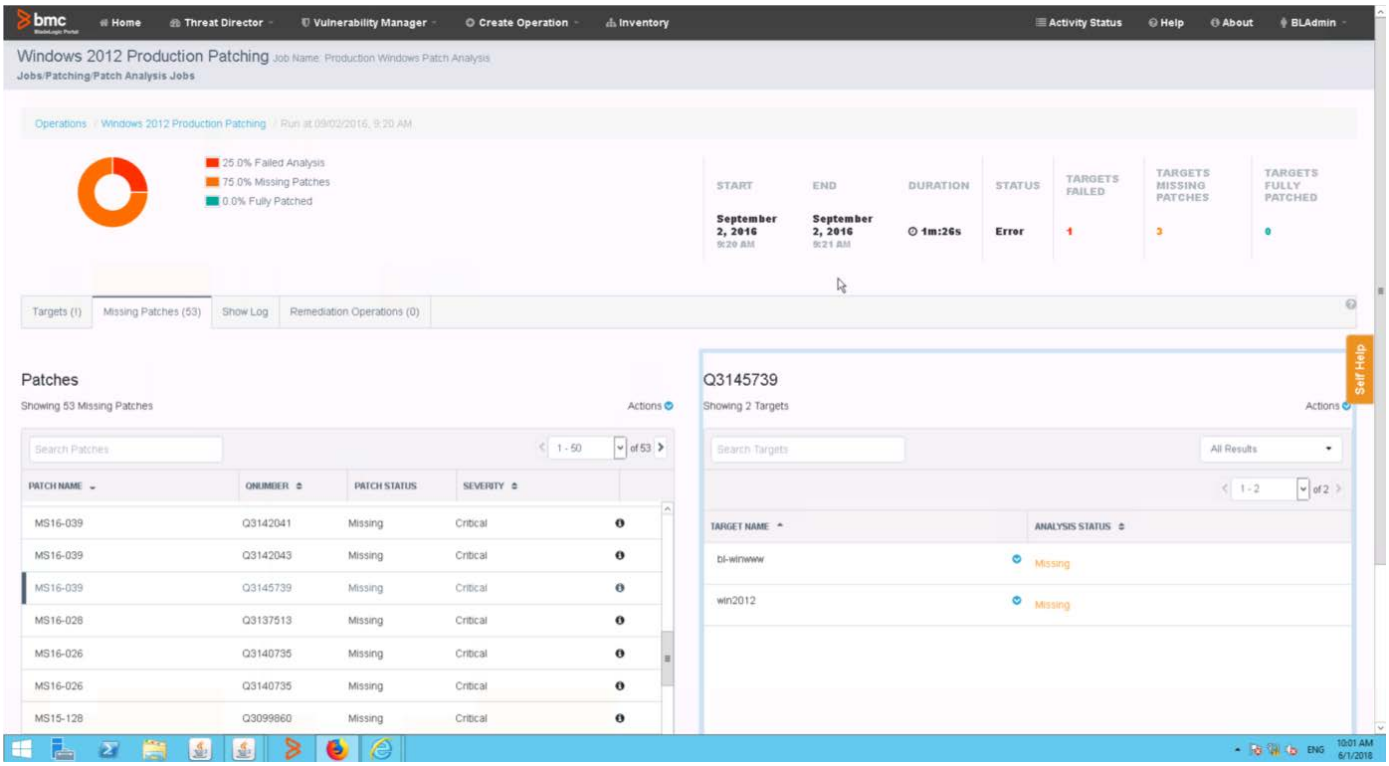
Maintenance windows aren't what they used to be—in many organizations, maintenance windows are down to a few hours per month instead of a day every weekend. Keeping servers manually patched and in compliance with security and regulatory requirements is difficult.

ESG Lab validated that TSSA 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. TSSA provides "closed-loop remediation" so you can act immediately on what your audit discovers. This enables organizations to be audit-ready at all times. Failure to comply with regulations can have serious consequences, including significant fines, reputation harm, and lost revenue; TSSA's compliance capabilities can help organizations stay out of trouble with minimal cost and effort.

Operator GUI

As mentioned earlier, TSSA has a separate user interface that is targeted at operators and infrequent users such as application owners or service owners. While the client UI enables experts to efficiently perform comprehensive administration tasks, the web-based UI enables organizations to delegate tasks to lesser-skilled users with a much shorter path to proficiency. Service owners can quickly use the web-based UI to perform tasks such as patching or compliance checks without requiring additional expertise. In addition, TSSA experts can package tasks in the web-based UI for execution by lesser skilled operators. This patching screenshot illustrates its simplicity.



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 with the latest security patches, and keep systems in line with corporate governance and regulatory compliance mandates. However, the pace of business today doesn't 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 is essential. For most organizations, time-consuming server management tasks take administrative time away from more strategic activities.

BMC's TrueSight Server Automation 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. TSSA enables intelligent policy-based changes to avoid unintended changes and outages, increase consistency, reduce errors and omissions, and free up staff time.

ESG Lab validated that TSSA provides configuration, patching, and compliance capabilities that can simplify server management, improve productivity, and reduce costs and risk. The ability to automate a nightly audit to security standards reduces risk by enabling immediate remediation. 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 Lab was impressed with the capabilities that TSSA delivers. It can help IT transform from a reactive "fire fighter" to a proactive service provider, ensuring smoother server operations across thousands of endpoints. The addition of patch orchestration would provide even more value, but TSSA is already making policy-based management easy. So, if you want to simplify and speed configuration, patching, compliance, and provisioning, and also reduce risk, improve productivity, and save time and money, be sure to look at TSSA.