Technical Review

BMC TrueSight Automation for Networks

Date: October, 2019 **Author:** Tony Palmer, Senior Validation Analyst

Abstract

This ESG Technical Review documents testing and analysis of BMC's TrueSight Automation for Networks, with a focus on configuration, patching, vulnerability management with automated remediation, and compliance features.

The Challenges

When ESG research respondents were asked about the most important considerations for justifying IT investments to their organizations' business teams in 2019, improved security/risk management, increased employee productivity, business process improvement, and improved regulatory compliance each made the top ten most-cited considerations.[1] These can all be improved with better management of network infrastructure. Administrators find it difficult and time-consuming to keep hundreds or thousands of network devices 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 2019 IT Investments

Source: Enterprise Strategy Group

[1] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019.

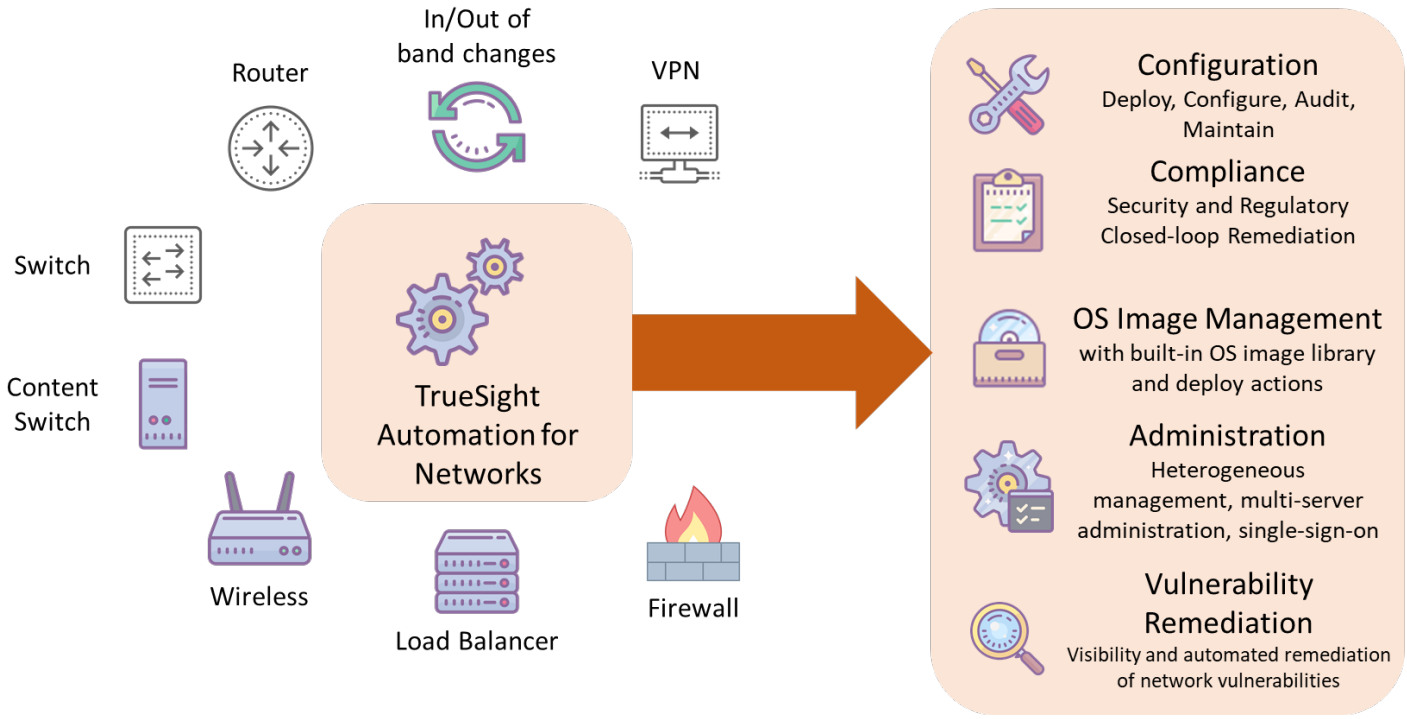
Manual network management is not only labor-intensive, but it also results in high error rates, failure to meet availability SLAs, and inability to scale on demand, as needed. Automation with proactive, policy-based network management can optimize the production environment for users, and free up IT staff time for strategic projects.

The Solution: TrueSight Automation for Networks

TrueSight Automation for Networks is part of the BMC data center automation suite that also includes server and process automation. Organizations use TrueSight Automation for Networks to automate the management of security vulnerabilities, configurations, compliance, and provisioning. TrueSight Automation for Networks also enables precise changes to be executed with fine-grained, role-based access that keeps systems secure and stable.

At a high level, TrueSight Automation for Networks helps IT to manage networks and understand their status while actively remediating problems—without requiring scripting. Organizations can discover devices, 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, administrators 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. TrueSight Automation for Networks enables administrators to employ a policy-based, consistent, reliable network management regimen with less administrative effort and cost.

Figure 2. BMC TrueSight Automation for Networks



Source: Enterprise Strategy Group

TrueSight Automation for Networks is a part of BMC's suite of IT operations and automation solutions and integrates with IT service management and governance processes. TrueSight Automation for Networks features simplify:

- **Vulnerability management**—Fast, automated, detection of vulnerabilities—without scans—and automated remediation based on Cisco security advisories and the National Vulnerability Database (NVD).
- **Compliance**—Built-in templates for regulatory compliance, plus closed-loop change tracking.
- **Configuration management**—Use SmartMerge to automatically generate scripts to execute changes or roll back entire configurations without rebooting.
- **Real-time status**—Get configuration, compliance, or security data from across the entire network in minutes.
- **Scalability**—Includes a multi-server administration portal for scalability and ease of use.

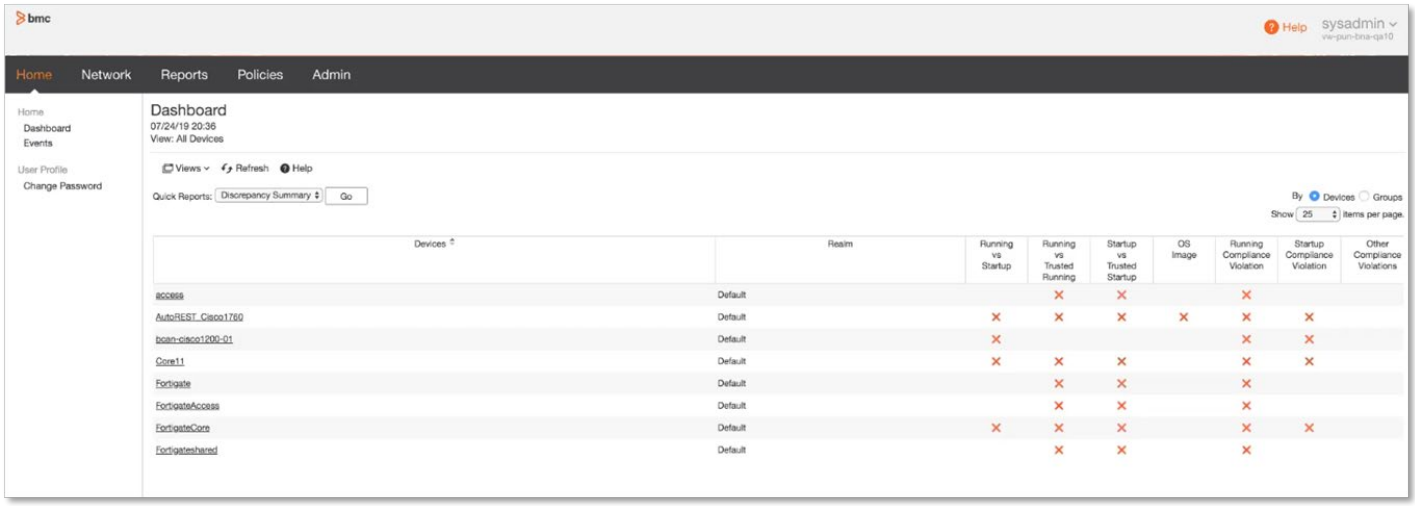
ESG Testing

ESG performed remote testing and analysis of TrueSight Automation for Networks. Testing focused primarily on configuration, compliance, and vulnerability management capabilities. For this validation, ESG remotely logged in to a test environment and spoke with a customer using TrueSight Automation for Networks in a large-scale production environment. It should be noted that this testing covered only a subset of the extensive capabilities that TrueSight Automation for Networks offers.

Configuration and Administration

ESG started by examining the *Dashboard*. For any device, we could view details in a discrepancy or compliance context, with indications of discrepancies including comparisons between running and startup configurations, running and trusted configurations, and startup and trusted configurations, or calling out compliance violations.

Figure 3. BMC TrueSight Automation for Networks Dashboard



Source: Enterprise Strategy Group

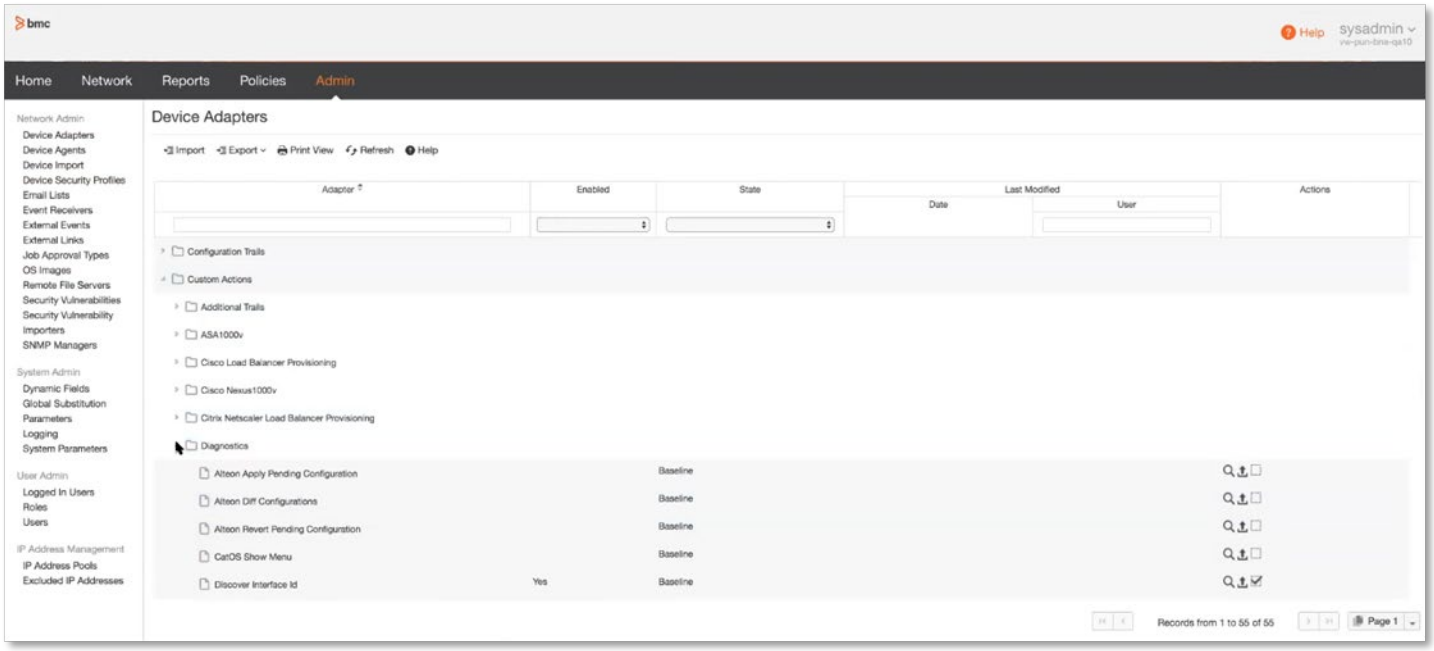
TrueSight Automation for Networks uses a powerful but lightweight agent to communicate with each network device. Because it uses a proprietary, encrypted "speak when spoken to" protocol, it doesn't require SSH or other transport; this enables it to make connections quickly and scale easily. For each device, we could drill down to individual items, and take actions such as making configuration changes, patching, and OS upgrades.

A key attribute is that TrueSight Automation for Networks tasks have the same look and feel across different platforms. Figure 3 shows eight devices from three different vendors in the same TrueSight Automation for Networks GUI. This enables an administrator to manage all systems across the environment with the same tool, at the same time, with the same look and feel.

This fine-grained ability to track complex violations and complex solutions comes from the rules that admins create that any specific device should have. TrueSight Automation for Networks understands the different formats that different vendors' devices use, so it can parse configurations and capture them without error, enabling administrators to change a single configuration across the entire environment with one click, or execute a complex configuration change, again across an entire environment, with one click.

TrueSight manages devices using the concept of Device Adapters, seen in Figure 4. Organizations can create custom Device Adapters, custom actions, and a full spectrum of administrative automation, including job approvals, vulnerability importers, security profiles, etc. This process is vastly simpler than managing devices via independent GUIs or CLIs or trying to script everything.

Figure 4. Device Adapters

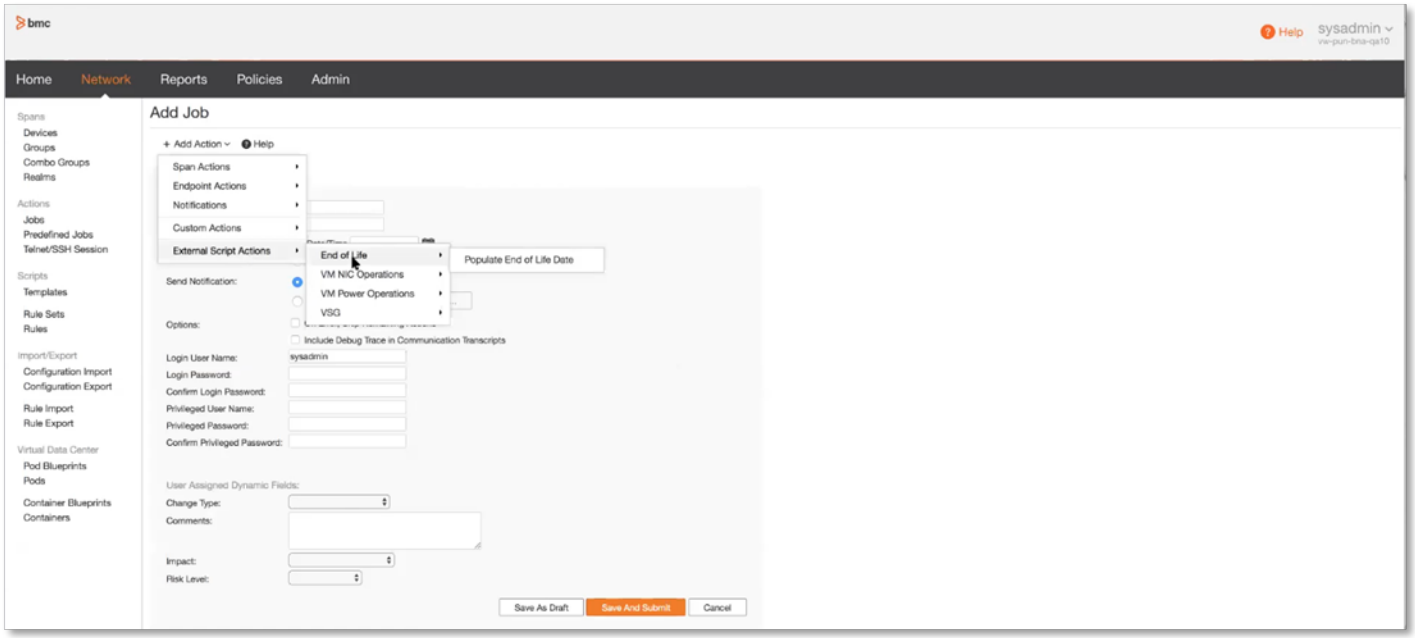


Source: Enterprise Strategy Group

Creating a Job

ESG navigated to the ***Network*** menu and selected ***Jobs***, seen here in Figure 5.

Figure 5. Jobs



Source: Enterprise Strategy Group

Jobs trigger operations on devices. There are many out-of-the-box actions available, such as image snapshot—taking a backup of a device's configuration. Once a snapshot has been taken, the configuration can be deployed. Another important action is to quarantine an endpoint. If a device is malfunctioning, an admin doesn't want the infected device to corrupt

other devices. Notifications can be configured for appropriate responders or teams. There are several custom actions which are preconfigured for various devices, and organizations can use these as a basis to create their own.

External script enables organizations to call an external script using network automation, so that organizations end up with a single pane of glass for any kind of operation they need to execute. Another interesting use case is for tracking end-of-life data when organizations can populate end of life or end of support for all devices in the network, ensuring that devices can be easily retired in a timely fashion.

TrueSight Automation for Networks options include:

- Administrators can schedule task simulation, staging, and commit at different times. For example, they can simulate a task at three pm to be sure the right permissions and configuration are in place, then schedule it to be staged at eight pm and finally committed at 11 pm at the beginning of their maintenance window. This way, the task begins immediately, rather than requiring the administrator to simulate and stage it, taking up part of the maintenance window.
- Jobs can 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.
- TrueSight Automation for Networks enables administrators to automatically create a change control ticket or tie into an existing ticket, saving valuable administrative time.

Why This Matters

Keeping hundreds or thousands of devices optimally configured is a daunting task that takes up significant network administrator time—and administrators are expensive. Manual network device management and scripting are also error prone. Multiple platforms—routers, firewalls, switches, and SD-WAN controllers, from numerous vendors, all with multiple versions to support—complicate management even further, especially with multiple, separately managed point tools that all provide different capabilities.

ESG validated that BMC TrueSight Automation for Networks provides a single network management tool with discovery and closed-loop change and configuration automation that supports numerous platforms with the same look and feel, simplifying tasks and saving time and money. With TrueSight Automation for Networks, junior staff can manage day to day operations, freeing up high level administrators for more strategic projects. Organizations eliminate concerns about multiple vendors' tools working together. TrueSight Automation for Networks enables intent-based networking via policy-based management and ongoing validation so that networks maintain the right capabilities and avoid conflicting changes and chaos.

Vulnerability Management and Compliance

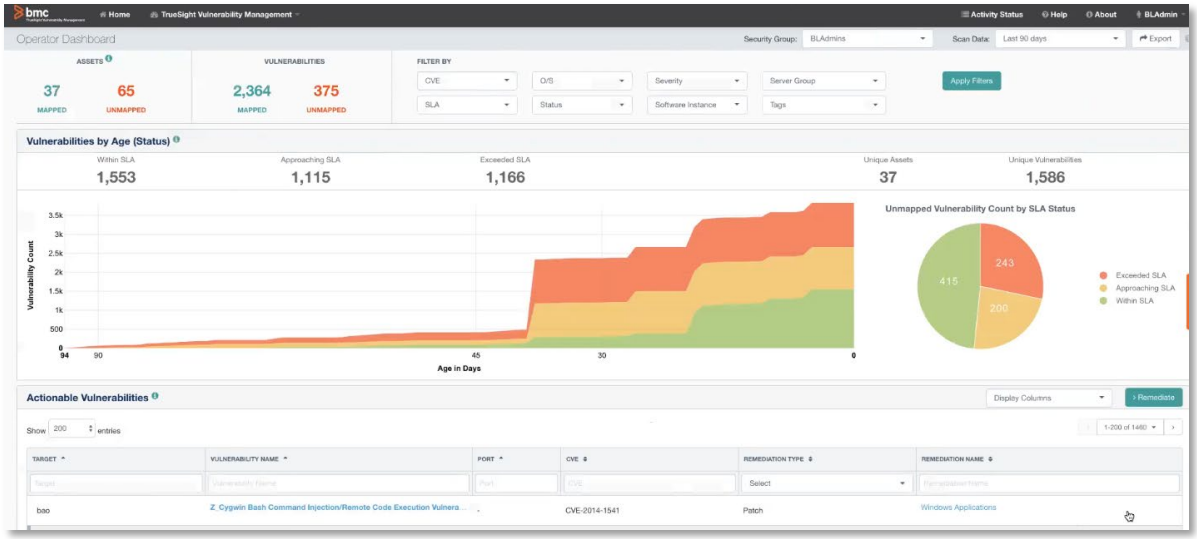
Vulnerability management and compliance tasks are essential for optimizing functionality, reducing risk, and maintaining security. BMC TrueSight Automation for Networks can help organizations accomplish these goals, moving to a more continuous compliance ready state, while gaining back productive time.

To detect vulnerabilities, many organizations use vulnerability scanners from vendors such as Nessus, Qualys, and Rapid7. These tools produce large reports that admins must parse, analyze, and compare to available remediations. BMC TrueSight Automation for Networks leverages TrueSight Vulnerability Management (TSVM) that can import these vulnerability scans, automatically map vulnerabilities to known remediations, assign severity, and help operators prioritize remediation actions. TSVM works with vulnerability remediation solutions including TrueSight Automation for Networks to execute remediation actions such as patching or configuration changes.

Vulnerability management is a four-step process: First, organizations import vulnerability reports, map their assets to managed devices, and map vulnerabilities to remediation. BMC automates all this activity on the back-end.

In the final step, teams remediate vulnerabilities. Organizations can use manual mapping for any vulnerabilities that can't be automatically mapped.

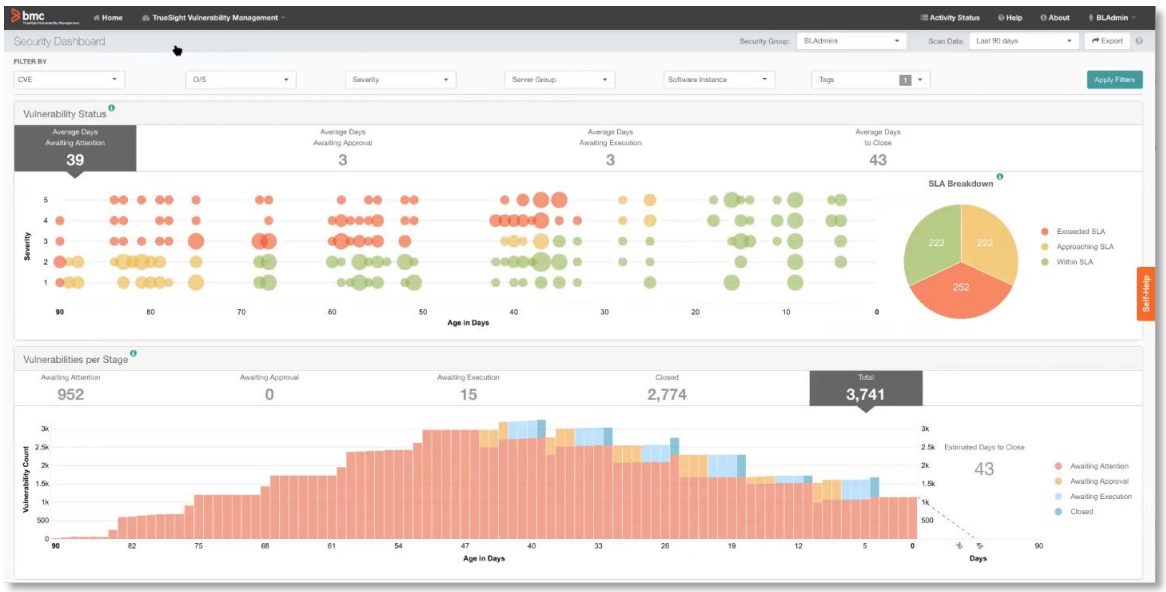
Figure 6. The Operator Dashboard



Source: Enterprise Strategy Group

The TrueSight Vulnerability Management operator dashboard provides an at-a-glance view of the state of the environment, with important metrics including the numbers of assets and vulnerabilities that are mapped and unmapped, as well as the age of vulnerabilities (see Figure 6). The graph is color coded based on SLAs defined by the customer and correlates to compliance. Within SLA indicates that an asset complies, and approaching SLA indicates *close* to compliance, while exceeding SLA indicates out of compliance. The security dashboard, seen in Figure 7, provides a heatmap that cross-correlates severity with the number of devices affected, and the age in days of the vulnerabilities.

Figure 7. The Security Dashboard



Source: Enterprise Strategy Group

A distinguishing feature of TrueSight Automation for Networks is that remediation packages can be deployed to bring your network back into compliance. Typically, administrators must translate compliance standards into 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. TrueSight Automation for Networks provides the flexibility for organizations to interpret and apply regulatory and security rules such as CIS and DISA in exactly the way that it matters to them, which can vary greatly from organization to organization. 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 TrueSight Automation for Networks, organizations can continually audit and update their status, and can remediate with just a mouse click, including exception handling for flexibility. In addition, TrueSight Automation for Networks' extensive reporting features include drill down into compliance rules, definitions, and reasons why devices are/were not compliant at any time period, details that can prove the level of compliance over time to auditors.

In addition, compliance checks execute on the TrueSight Automation for Networks infrastructure, not on the endpoints. As a result, organizations can expand their compliance checks without taxing endpoints and causing productivity interruptions.

BMC TrueSight Automation for Networks in the Real World

ESG spoke with a customer using BMC TrueSight Automation for Networks for vulnerability management. The client is a service provider with approximately 125,000 devices under management. The environments contain about 90% Cisco devices, with Riverbed, Juniper, F5, and a few other vendors represented. The primary use case for this customer is vulnerability management, but they also help other teams in the organization with large-scale changes and compliance management. Prior to adopting BMC TrueSight Automation for Networks, it was a very labor-intensive, manual process, with the vulnerability teams gathering notifications and passing tickets to the resolver teams. It was quite a painful process because it had to go through many people, who saw vulnerability management as extra work that was unnecessary. The large number of false positives helped contribute to that attitude. They are still early in the project, but they had thousands of devices that had been managed individually for years with manual scripting. A *severity one* incident was caused by a misplaced space after a comma in a script that was exceedingly difficult to find and fix. While BMC TrueSight has been a revelatory experience, there are areas for improvement, mainly because of the size and scope of their environment. They run several instances with 20 to 30,000 devices under management on each. The ability to manage all their instances as a real-time cluster would be a management improvement for this client. To be fair, the client is quite happy with how BMC has listened to their concerns and continues to address them.

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 devices manually patched and in compliance with security and regulatory requirements is difficult.

ESG validated that TrueSight Automation for Networks can do the heavy lifting, updating patch catalogs and compliance rules intelligently across vendors and platforms, auditing the environment, and remediating with just a few clicks. Organizations can manage vulnerability and security patching and regulatory compliance with a fraction of the resources they would otherwise need.

While other solutions might simplify a compliance audit, many provide no tools to fix what you find. TrueSight Automation for Networks provides "closed-loop remediation" so you can act immediately on what your audit discovers. This enables organizations to be continuously audit-ready. Failure to comply with regulations can have serious consequences, including significant fines, reputation harm, and lost revenue; TrueSight Automation for Networks' compliance capabilities can help organizations stay out of trouble with minimal cost and effort.

The Bigger Truth

Network management may not feel exciting, but it is critical for a well-functioning IT infrastructure. Admins must execute numerous tasks precisely and consistently to maintain trusted configurations, keep devices patched with the latest OS updates, ensure security with consistent configurations, and keep the network in line with corporate governance and regulatory compliance mandates. The pace of business today doesn't allow for error-prone manual processes that consume lots of time. Whether your organization has hundreds, thousands, or hundreds of thousands of network devices, automating configuration, patching, and compliance processes is essential. For most organizations, time-consuming network management tasks take administrative time away from more strategic activities.

BMC's TrueSight Automation for Networks offers a solution with extensive automation that can make your environment more secure and functional quickly, and still retain the flexibility you need to manage networks as your organizational needs demand. TrueSight Automation for Networks enables intent-based networking with intelligent, policy-based changes to avoid unintended consequences and outages, improve compliance audit readiness, reduce errors and omissions, and free up staff time.

ESG validated that TrueSight Automation for Networks provides configuration, patching, and compliance capabilities that can simplify network management, improve productivity, and reduce cost and risk. The ability to automate audits to security and compliance standards reduces risk by enabling immediate, automated remediation. In addition, rather than the all-too-common practice of getting systems compliant occasionally for auditors, organizations can be *continuously* compliant. Patching and compliance updates should add functionality to your environment, increase security, and protect you from penalties. They should not be a thorn in the side of IT administrators.

ESG was impressed with the capabilities that TrueSight Automation for Networks delivers. It can help IT transform from a reactive stance—fighting fires—to a proactive service provider, ensuring smoother operations across thousands of network devices. The addition of multi-instance orchestration would provide even more value, but TrueSight Automation for Networks is already making intent-based networking easier. So, if you want to simplify and speed configuration, patching, compliance, and provisioning, while reducing risk, improving productivity, and saving your organization time and money, you'd be smart to take a close look at BMC TrueSight Automation for Networks.