vyomlabs
An EMERGYS Company

bmc

Solution White Paper

How to Streamline Compliance Through Automation

Close security loopholes faster and be audit-ready all the time

Table of Contents

Executive Summary

Here are the harsh facts: the old ways of implementing security and compliance mandates are no longer acceptable, and the risk of high-profile consequences from incomplete or insufficient attention has never been greater.

Companies that experience breaches face significant penalties or even criminal prosecution for the CIO, the CISO, and other IT leaders. If you are an operations leader responsible for maintaining optimal configurations in your organization's infrastructure (including physical and cloud-based servers) or the head of a security team responsible for auditing and reporting on compliance with corporate or regulatory mandates, then your **business must find ways to meet organizational and legal requirements, even with the increased pressure on budgets, fewer resources, and increasingly frequent audits.**

This white paper will provide actionable tips and guidance to help you achieve better results such as:

- How to achieve a state of **continuous compliance of being audit-ready all the time**
- Ways to **streamline handoffs between security and operations** staff to maximize effectiveness, and reduce rework and manual tasks
- How to accelerate remediation and patching to reduce the attack surface

Most organizations find it challenging to stay vigilant and keep up-to-date with compliance policies, but a strong foundation in compliance is one of the bedrocks of a successful security strategy. Armed with an approach to compliance and vulnerability management, change management, and discovery will remove debilitating process bottlenecks and enable organizations to build an effective security posture.

The Status of Security Today

- There has been a 29% increase in total cost of a data breach since 2013, with the average total cost of a data breach at $4 million USD (2016 Ponemon Cost of Data Breach study)
- PCI violations are costly – fines can be assessed of up to $500,000 per incident, $100,000 per month, and $90 per cardholder record compromised

WHY IS COMPLIANCE DIFFICULT?

In general, compliance means conforming to a rule, such as a specification, policy, standard, or law. In IT, **compliance means describing a desired configuration state that IT organizations aspire to achieve.** This standard may be purely internal, such as an operational standard requiring the latest security patches, or it may be external. External compliance standards might include both best practices and requirements imposed by industry or government bodies, such as Payment Card Industry Data Security Standard (PCI DSS) for retailers, Sarbanes Oxley (SOX) for publically traded companies, or Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) for U.S. federal contractors and agencies.

THE IMPACT OF THE SECOPS GAP

Security compliance and policy compliance are sometimes seen as different disciplines, with regular but relatively infrequent compliance policy audits separate from ongoing vulnerability assessment and remediation. **Security (Sec) teams focus on shortening the window of vulnerability, while operations (Ops) teams concentrate on ensuring performance and availability of business systems.** This disconnect may result in neither priority being satisfied, causing issues to fall into the gap. Hence the term, **the SecOps gap.**

Today, this process is generally disconnected, with one team defining or adopting a certain standard and performing audits against that standard. However, the auditing team usually does not have access to correct any issues that have been identified, so they must send a list of those issues to the operations team for action.

The entire process is performed by hand, with certain subtasks being automated and data exported manually from one tool and re-imported into another. This disconnected approach is extremely time consuming, costly, and error-prone.

Does this happen in your organization? The security team runs a vulnerability scan from a solution like Qualys® Tenable or Rapid 7® and drops the report on the desk of an operations team member saying, “This list is ready to be checked for compliance.” Now the operations person must review this huge report and try to determine which systems are mission critical or a high priority and try to fix those issues first. He or she will likely fix the issues by hand, and probably not before the security person stops by with another report. There is no easy way to check if there is already a patch or configuration available, and no way to schedule the remediation with minimal impact to the business. Even worse, they have to manage the change process manually by opening a change ticket, waiting for approvals, and then manually documenting the change. And the final insult is that both the operations and security teams are only looking at the assets they know about, which are likely manually tracked on an Excel spreadsheet. **The frequency of audits is increasing and the manual approach is falling very short.**

The two teams’ mismatched priorities present another problem. Once a vulnerability has been identified, it is best for the organization to address that issue as rapidly as possible, shrinking the window of time in which an attacker may exploit it. Operations teams must focus on the availability of systems to users. Deploying patches or making configuration changes, when not managed properly, can easily result in downtime. As a result, the operations department has processes to minimize the impact of planned and unplanned downtime. In particular, manual remediation has a substantial opportunity cost because of the high authorization level required to access the systems and the corresponding high level of skill required of staff. There is also a certain element of risk involved in making changes by hand: commands may be entered incorrectly or correct commands may be entered in the wrong interface. Finally, the disconnected nature of the manual process risks breaking the transmission of information, resulting in incomplete compliance coverage or remediation and the loss of information in the SecOps Gap.

Alternative Solutions

Point products may be used for parts of the process, such as vulnerability scanning, but the end-to-end process is not typically integrated or automated. A disconnect between the audit and remediation processes means that identified vulnerabilities and compliance violations may not be remediated completely or in a timely manner. Scripting or custom development in general leads to technical debt, as developed functionality must be updated and ported to support new platforms and technologies. Documenting compliance actions also requires substantial manual work to export and merge data from different tools.

Costs

Organizations facing the SecOps gap spend too much time, energy, and money manually tying processes together with mismatched sets of requirements. More importantly, if they don't continually scan for security and compliance issues and automate the process of correcting them, as well as have an automated way to keep track of ever expanding infrastructure, organizations will eventually suffer security breaches and find themselves in a very difficult situation. Negative consequences of a breach may include:

- **Direct costs** (damage to hardware/software, cost of remediation)
- **Indirect costs** (negative perception from media, organizational disruption due to investigation, possible reactive action not in line with strategic goals)

Both the possibility of a breach and its impact can be substantially reduced with a strategic approach to automation that brings the security and operations teams together to streamline communication for better hand-off and smarter outcomes.

To be successful, companies must transform these disciplines from disconnected initiatives that are time consuming, risky, and often incomplete into a single, unified process that is routine, secure, and comprehensive. Knowing that no systems have been overlooked and that the audit on each of those discovered systems is detailed and in-depth makes the audit results trustworthy and therefore more immediately actionable. Automated remediation with built-in validation ensures that any issues detected during the audit are addressed rapidly and actually corrected. Finally, automated documentation means that the data that management uses for decision making are known to be up-to-date and comprehensive, eliminating second guessing of the reported situation and reducing the risk of accidentally causing an unplanned outage or rolling a system back to a non-compliant version repeatedly. **As a result, the security and operations teams have what they need: visibility with control.**

INTRODUCING BMC COMPLIANCE SOLUTIONS

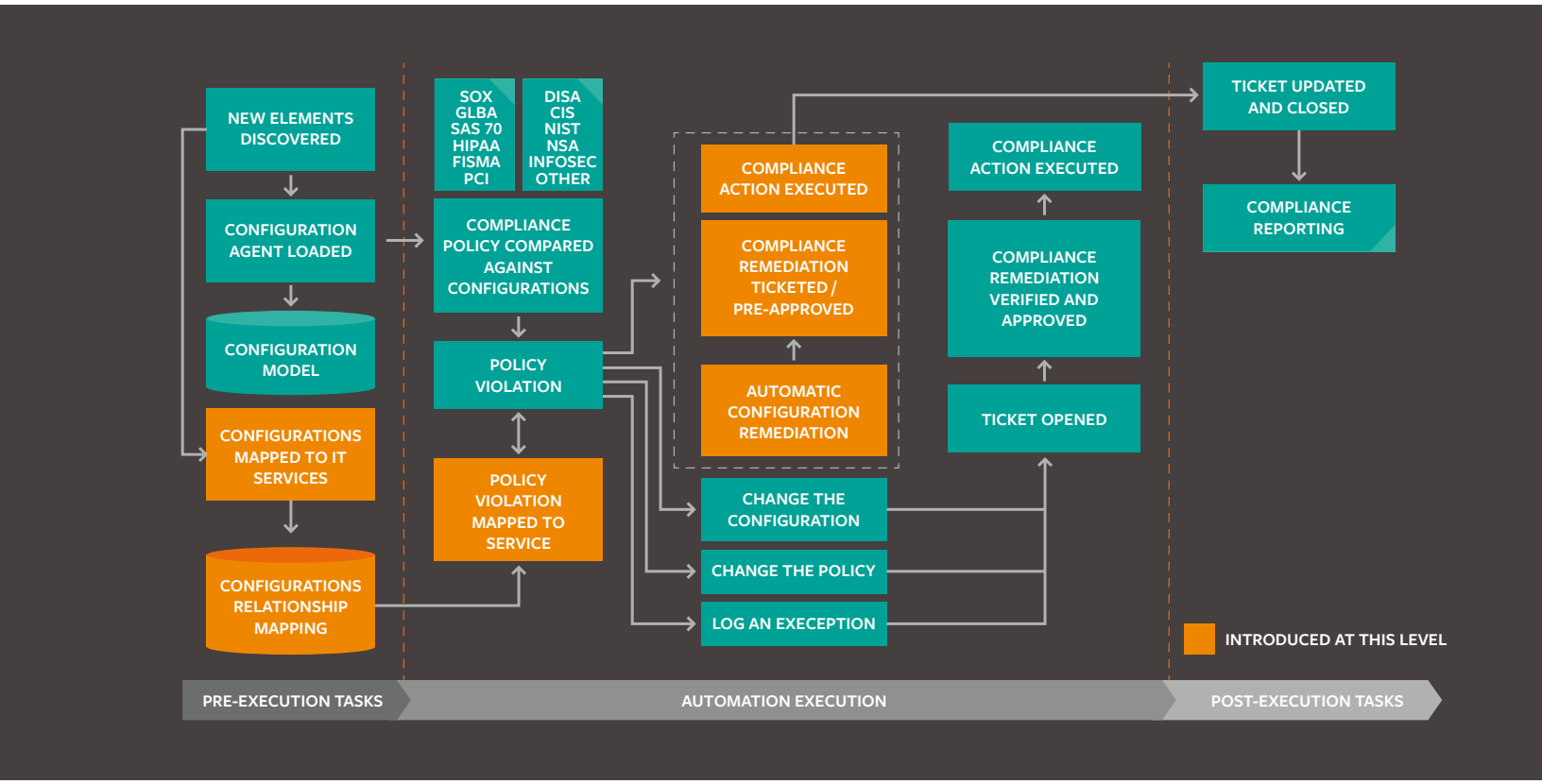
Here's the good news: there is an easier way. BMC Compliance Solutions, which include BladeLogic, Discovery, and Remedy products closes the SecOps gap that separates security from operations teams. They help remove the barriers that keep companies from achieving their goals around governance, risk, and compliance (GRC). Bringing together enterprise-ready BMC capabilities and third-party vulnerability assessment solutions orchestrates them into a single, unified process that provides end-to-end automation. **Combining the detailed discovery and oversight from the security team with the diligent manicuring of the operations team to intelligently correct any deviations from the desired configuration state of the infrastructure reduces risk, improves enforcement, and frees IT personnel to focus on achieving the strategic goals of the business.** For situations requiring a judgment call before automatically updating the out-of-compliant system, the solution highlights the situation in question and enables rapid human approval and oversight of the change.

Four Key Phases of BMC Compliance Solutions

- **Discover:** Automated **discovery** delivers a complete picture of what is in the IT environment, as well as dependencies between different infrastructure components. The resulting inventory is an up-to-date baseline with a complete list of systems that need to be audited for compliance, including any unofficial and temporary modifications to the known environment. It conducts passive, agentless discovery of systems on the network. Based on patterns of how individual systems communicate with each other, it maps out dependencies and business applications, which allows IT to prioritize effort (i.e., security response) based on the potential business impact of a breach or an outage.
- **Define:** Security teams can then **define** what the state of that environment should be, using patching information from vendors, third-party best practices, industry-specific policies, and particular requirements of each situation. Operations can leverage a number of predefined policies ready for use. Thanks to its detailed, actionable definition of the desired state, regular, scheduled, and automated audits are immediately available for action. Granular configuration visibility helps avoid false positives that would otherwise create an alert to a vulnerability that does not exist, as well as reduce false negatives that would otherwise miss a potentially harmful vulnerability.
- **Audit:** Security and operations teams depend on tools and reports to conduct thorough **audits** without having to limit coverage due to the enormous effort of completing this step manually. Now, the team can audit on a regular basis to identify any departure from the desired state. They can compare live configurations to a reference system and troubleshoot issues caused by configuration discrepancies or they can evaluate the current state to a "known good" state from a prior period and use the snapshots to aid in troubleshooting. Another option is to compare the current state to out-of-the-box policies such as Sarbanes-Oxley (SOX) 404, Health Insurance Portability & Accountability Act (HIPAA), Payment Card Industry Digital Security Standard (PCI DSS), or Center for Internet Security (CIS), or they can use these standard policies as templates to build customized operational policies. It is easy to match patching levels to the latest recommendations from the vendor. In some instances, IT can define white or black list policies that grant or deny certain privileges. Add in the invaluable data of vulnerability assessment tools and the teams have actionable intelligence at their fingertips, including reports and logs.
- **Remediate:** The remediation phase is designed to understand the difference between the desired and actual states. The **remediation** determines what action to take in response. Automated remediation is immediately available to address any identified issues and return the environment to the desired state in a timely and predictable manner. Remediation can be scheduled or triggered on demand, without the need of scripting. If an issue occurs, there is a built-in mechanism to easily rollback to a prior "known good" state. Because of the high risk of errors when a change occurs, remediation can be used as a surgical tool, making only the changes that are required.

The Result – Secure Operations: Now it is possible to ensure control and visibility of all actions by keeping track of changes to the environment and why the change was made through the govern phase. For instance, there are many perfectly valid reasons for configurations to drift over time. Having those reasons properly documented ensures staff don't revert to an inappropriate state. In the same way, it may not be possible to deploy certain patches because of application compatibility issues. By coordinating with the change management process, teams can enforce change windows and avoid collisions or unplanned outages. Compliance may not necessarily require a configuration to be changed, and security requirements may be satisfied in other ways, but it is important to document and track the exceptions. If exceptions to standard compliance practice are not formalized in this way, the risk is that they generate large numbers of false positive alerts or worse, fail an audit.

BMC Compliance Solutions automate the entire process: understanding the current state of the environment, defining a desired security and compliance baseline, comparing that desired state with the actual state, correcting the discrepancies, and creating the required reporting and logs. It shrinks the SecOps gap, reducing the compliance time and costs and ensuring that continuous compliance is achieved and verified, without breaks in coverage or documentation. It integrates with existing IT change processes and leverages the skills and processes used by IT teams today.



The Security Operations Workflow

What Are the Benefits?

- Turns burdensome management chores, often driven by quarterly or annual audits, into an easy background process, and if properly implemented, eliminates the risk of failed audits
- Shortens the time in which companies are exposed to vulnerabilities, reducing the risk of a catastrophic breach
- Reduces the total cost of auditing, security, and compliance initiatives substantially by applying automation to the process, freeing up the most valuable and important personnel to concentrate on strategic issues

CONCLUSION

The goal of most organizations is to ensure that systems meet regulatory requirements and security best practices. The role of operations is not to freeze changes to systems, but to make those changes in a way that is safe and meets the business needs of the organization. This means that the entire process must be holistic and include:

- **Regular automated discovery** to ensure that all relevant systems are covered
- **A desired compliance or security state** that is defined with sufficient granularity to be useful
- **Ongoing audits and vulnerability assessments** to identify any departure from the desired state
- **Automated remediation** to bring the system back into compliance with that desired state
- **Governance to help apply compliance policy** in harmony with other business priorities

With BMC Compliance Solutions, you get:

- Comprehensive discovery of application infrastructure
- Granular flexibility to define compliance profiles, including out-of-the-box policies for the most common mandates such as CIS, PCI-DSS, SOX, or DISA STIG
- Live comparisons to audit against policies and regulations
- Application of known patches with one touch
- Drift control to automatically remediate errors and identify exceptions
- Integrated change management to govern the compliance process

Fight back against hackers and let BMC Compliance Solutions help you secure your operations while improving effectiveness and accelerating execution.

FOR MORE INFORMATION

To learn more about BMC Compliance Solutions, please visit: **bmc.com/SecOps**

465218