bmc

Solution White Paper

Breakthrough Security and Compliance Practices for the Digital Enterprise

Reduce business risks with strategic, intelligent automation

Table of Contents

Executive Summary

Today's IT environments are so dynamic and complex that traditional manual administration makes it virtually impossible to keep pace with changing business opportunities and challenges, such as scaling to support new applications and users. **Manual administration is not just unsustainable—it's dangerous.** Delays in responding to security threats and compliance issues can have devastating effects:

- Security breaches
- Failed audits
- Financial losses
- Loss of customers and reputation
- Other serious business consequences

To sustain a high level of security and compliance, IT teams must implement a comprehensive, aggressive automation strategy that establishes and tracks key performance indicators. **Automation helps to optimize resources, increase efficiencies, lower costs and improve quality of service.** This white paper describes principles and best practices for implementing automation as a strategic asset in the ongoing effort to achieve security and compliance excellence in a dynamic IT environment.

SECURITY AND COMPLIANCE ARE NEVER "ONE AND DONE"

In many organizations, security and compliance efforts are reactive: the staff scrambles to meet a critical, immovable, and urgent deadline that can involve a newly discovered vulnerability such as WannaCry (CVE 2017-0144), an impending audit, or the implementation of new regulations. Similarly, the newest security threat generates an all-out race to implement defensive measures. Too often, IT and security teams fall into a pattern: focusing on deadlines and security emergencies as separate events, moving on after they pass, and then going through the same laborious, manual process all over again. However, failing to build repeatable, automated, and efficient ongoing processes can ultimately conspire against the IT organization and the entire business.

One-off, manual compliance and security efforts are falling short, particularly as the frequency of audits, regulatory changes, and new threats increases.

In today's dynamic IT environments, the results of last quarter's audit may say very little about the business' current compliance posture. According to the Ponemon Institute 2017 Cost of Data Breach Study[1], the average cost per lost or stolen record was $141.

Adopting a strategic, continuous approach to compliance and security management calls for automation. Investing in automation tools, formalizing workflows and documentation, instituting incentives, making new hires, refining and expanding automation—all these efforts need to be undertaken with the long term in mind.

BREAKTHROUGH AUTOMATION FOR SECURITY AND COMPLIANCE

To address their most urgent compliance and security challenges, **organizations need to take a comprehensive, policy-based, and automated approach.** Following are some key principles to consider:

Provision with security and compliance in mind

Up-front provisioning of servers, network devices, and other elements should be done with a clear focus on compliance and security. Strive to gain capabilities for automating rapid provisioning of multi-tier IT services across cloud and non-cloud environments.

Depending on their specific environment and technologies, organizations should be able to create compliant, secure and hardened images that can be deployed establishing a solid baseline for security. Initial provisioning, regardless of whether through unattended, scripted, image-based or template-based installs should enforce relevant policies and guidelines. By leveraging sophisticated automation platforms, organizations can gain immediate access to pre-configured policies for a range of mandates, including PCI DSS, HIPAA, and patches for security threats such as Heartbleed or Ghost. These consistent approaches are vital in setting the stage for a sound compliance program.

Orchestrate change for continuous security and compliance

Too often, security teams face the complexity of hybrid application stacks, quickly evolving compliance requirements, and increasingly sophisticated security threats—overwhelming IT personnel with managing day-to-day operations alone. Too often, these organizations cannot perform continuous scans for security and compliance. Instead, they resort to manual processes, which delay remediation, keeping resources in insecure state and increasing the odds of a security breach.

It is vital for IT teams to establish process automation based on workflows that span a range of infrastructure elements—including applications, platforms, and tools—and to gain the ability to orchestrate critical activities surrounding compliance, security, and business enablement. Orchestration that integrates automation with IT service management enables operators to initiate automated change management procedures. Following are specific considerations for orchestrating change:

- **For servers.** IT should be able to provision servers and configure changes with ease. Regulatory and operational compliance audits should be conducted on a continuous basis. Remediation of known vulnerabilities should also be automated. Automation should be applied across all servers that matter to the business, including to the operating systems of physical servers and virtualization and cloud-based server platforms.

1 2017 Cost of Data Breach Study: Global Analysis. Ponemon Institute, June 2017

- **For databases.** It is critical to establish automation across heterogeneous database environments. Routine administrative tasks and compliance processes should be automated wherever possible, based on standardized models. Establish pre-flight checks providing automated validation that environmental variables are configured correctly before a new database is provisioned. Toward this end, administrators should have capabilities for discovering and recording complex database configuration and interdependency information. These models should establish standards for provisioning, configuration, deployment, and patching. It is only through intelligent automation that organizations can rapidly and reliably implement change across demanding, heterogeneous environments.
- **For network devices.** As it does for servers, automation also benefits provisioning, configuring, and patching of network environments. Policy-driven actions reduce errors, improve performance, and promote compliance.
- **For change management.** Many regulatory mandates require proper tracking and documentation of changes to the IT environment, including updates necessary to prevent vulnerabilities. IT operations can automate ITIL® best practices for change management and approvals to close the loop for continuous compliance. This includes documenting changes made to servers, databases, networks, and cloud services.

Create intelligent policies for servers, clouds, and databases

Automation policies should be intelligent and aligned with the unique needs of the specific environment to which they are being applied, whether physical servers, clouds, networks, or databases. Leveraging automated discovery and contextual intelligence, these policies should be based on vendor patch information, industry and corporate best practices, compliance requirements, and more.

For example, all authorized users should have a complete picture of relevant actions that have been taken in an environment and the reasons why prior changes have or have not been made. If a server patch is incompatible with an application running on a server, that information should be captured to avoid inadvertent implementation of the patch. It is important to formally document these exceptions so that false positives or failed audits can be prevented. In addition, IT teams should be able to coordinate change management processes to enforce change windows and avoid collisions or unplanned outages.

Make vulnerability scans actionable

Historically, configuration compliance has been a two-step process. First, on a regular basis, the security team conducts an audit that compares the current state of IT systems to relevant policies, standards, and legal requirements. Second, the operations team performs the remediation process to correct discrepancies between standards and current implementations. **Often, these processes are hampered by a significant disconnect between security and operations—the so-called SecOps gap.**

One team conducts the audit and another handles remediation. While static vulnerability reports may be handed over, the two teams lack unified visibility. For instance, the security team may not know that a server lacks the latest patch because of a known compatibility issue with an application. Or the operations team may not have a sense of urgency to remove a vulnerability based on an understanding of the potential threat. Not only are these two teams disconnected, they are operating with different priorities. Security teams are focused on addressing vulnerabilities as soon as possible to mitigate threats. On the other hand, IT operations teams are concentrating on optimizing system availability and implementing patches with minimal business disruption. Exacerbating matters, non-integrated point products are often used for part of the process, such as vulnerability scanning.

To combat the SecOps gap, organizations need to make vulnerability assessments much more actionable. Instead of static reports, these assessments need to provide IT operations teams with rich, contextual insights so they can remediate quickly, understand how to prioritize remediation, how to schedule the remediation to minimize business impact, and so on.

It is also important to equip security teams to conduct automated audits that offer live configurations to reference systems and make it easy to troubleshoot issues caused by discrepancies. In addition, it should be easy to evaluate the current state versus the last known good state.

Automate remediation for known vulnerabilities

Manual remediation efforts carry a high opportunity cost for the business. These efforts require management and oversight by seasoned, high-level personnel, who not only earn higher salaries but also may be diverted from strategic work. Further, manual remediation takes more time, posing the risk that vulnerabilities and compliance violations may not be corrected promptly.

When known vulnerabilities are involved, automated remediation should be enabled to address any identified issues immediately and return the environment to the required state. **Remediation should be scheduled or triggered on demand, without the need for developing scripts.** If manager approvals are required as part of the remediation, they should also be automatically triggered as

appropriate. If an issue arises, built-in mechanisms should enable the system to be rolled back to its last "known good" state. Intelligent automation also allows organizations to minimize unnecessary changes and can significantly reduce associated errors.

To automate repetitive tasks, human interactions, and system-to-system business processes, an intuitive interface that facilitates the design and implementation of workflows can significantly increase usage and productivity. This interface will also extend the skills often held by specialists to generalists so they become capable of remediation across a broader range of infrastructure.

How to measure the value of automation

Often, once an initial return on investment has been realized or a stakeholder's expectations have been met, the tracking of metrics stops. **To maximize the success of automation, however, it is critically important to track metrics consistently over the long term.** Establishing and consistently tracking solid metrics are essential for several reasons. First, results can inform an objective assessment of automation efforts and provide insights for increasing their value. Second, with tangible metrics to point to, IT organizations will be much better positioned to gain funding for future automation initiatives.

Measure value incrementally and continuously

Put another way, **if automation activities aren't measured, logged, and reported, the value they deliver won't be well understood,** and it will be difficult to establish and sustain the support of key participants and stakeholders.

Begin assessing these measurements in the earliest possible phase of the project—ideally, before any automation initiative is kicked off. The data captured will provide an accurate "before" picture of the area or process. Then, once automation is instituted, ongoing tracking of these measurements will allow organizations to assess the changes, how much performance has improved, and whether additional steps should be taken.

BENEFITS OF AUTOMATION

There are many quantifiable benefits that can be realized with an effective automation strategy.

- **Reduction in security risk.** Automation can significantly reduce the elapsed time between identification and remediation of a vulnerability reducing the time the organization is exposed to risk.
- **Reduction in labor costs.** By automating manual efforts such as patching and provisioning, organizations can save time and reduce labor costs.
- **Reduction in outages or performance issues arising from poorly applied patches.** When patches are applied manually to individual components, errors are likely, often leading to outages and performance issues. Effective automation significantly reduces the risk of human error.
- **Reduction in fines for noncompliance or breach.** By leveraging automation, organizations can more quickly and effectively address their SLA and regulatory mandates to reduce the frequency of compliance breaches and associated penalties.

Regardless of the specific procedures being automated, a set of common metrics should be used to gauge the value being delivered. The following table offers suggested metrics for tracking the business value delivered by specific IT automation efforts.

Each category can include multiple key performance indicators (KPIs), each with a specific calculation method. A few sample calculations are included below. The results of these calculations can be translated into business value, such as accelerating services delivery, reducing downtime, increasing resilience, and reducing risk.

Patch Speed KPIs

- Number of servers lacking patches
- Number of SLA violations
- Frequency of maintenance window overrun

Patch Cost KPIs

- Cost of unplanned downtime due to patching incidents
- Monthly/annual SLA violation charges
- Annual labor cost to patch components, groups

Patch Risk KPIs

- Distribution of Patch compliance state
- Failure rate for patch installation
- Percentage of environment being patched
- Compliance program effectiveness survey results
- Number of outages due to missing patches

Assessment Speed KPIs

- Policy audit time
- Number of assessment cycles possible annually
- Time required to consolidate configuration reports for audit

Assessment Cost KPIs

- Number of IT staff involved in assessment activities
- IT staff productivity impact during assessments

Assessment Risk KPIs

- Percentage of IT environment unassessed
- Lack of well-documented configuration exception procedures
- Number of audit failures due to delays producing configuration reports

Compliance Speed KPIs

- Number of audit cycles possible annually
- Percentage of environment that is compliant
- Number of security bulletins addressed

Compliance Cost KPIs

- Cost of unplanned downtime (lost revenue)
- User productivity impact during downtime
- Amount of noncompliance violation charges
- Amount of SLA/audit violation charges

Compliance Risk KPIs

- Number of IT components out of compliance
- Number of failed internal/external audits
- Number of policy violations

Intelligent Speed KPIs

- End-to-end process time from non-compliant to compliant state
- Number of pre-approved compliance changes
- Number of compliance changes requiring approval

Intelligent Cost KPIs

- Amount of penalties for noncompliance
- Productivity impact of compliance activities
- Cost of unplanned downtime (lost revenue)

Intelligent Risk KPIs

- Number of failed internal process audits
- Percentage of compliance by policy type
- Percentage of compliance by business service
- Historical downtime metrics

GETTING STARTED WITH AUTOMATION

Like effective compliance and security, automation isn't a one-and-done proposition. Successful organizations embark on preliminary initiatives and increase automation sophistication and capabilities over time. Initial efforts are typically led by individuals who add automation efforts to their primary roles. However, as soon as possible, some individuals should be dedicated solely to automation initiatives. Toward that end, it's highly advisable to establish cross-functional automation specialist roles early to ensure decisions and activities support longer-term strategy. **Over time, the number of people involved in automation should grow, while those responsible for handling manual, repetitive tasks will decrease.**

Initial automation tasks typically will be smaller in scale, for example, targeting a specific technology. As automation matures, initiatives can expand to processes, technologies, and teams across the enterprise.

Following are some key considerations for establishing and ramping up effective automation efforts in your organization.

STAFFING

Get the right people involved and equip them with the help, information, and incentives they need to succeed. Automation involves three roles:

1. **Automation enabler.** Champions key automation activities, for example, helping with cloud service justification, design, release, and service support.

2. **Automation operator.** Responsible for carrying out automation activities and processes. These individuals help design, plan, and document process workflows; work with different teams to ensure automation is supported; and select the right automation technologies.

3. **Automation stakeholder.** Anyone affected by automation activities, including users of automated processes. Many should be asked for input and approval of automation design and delivery plans.

In general, automation is led by individuals with backgrounds in IT architecture, development, operations, and IT service management. Successful automation teams need a range of skills, including project and process management, workflow development, scripting, IT tools integration, and knowledge management. They should have a good understanding of such automation technologies as workload brokers, orchestration tools, and script toolkits. Beyond technical skills, team members need the ability to collaborate effectively with different organizations such as Finance or Governance, Risk, and Compliance departments to achieve automation objectives that result in secure and compliant IT environments.

Finally, staff expertise should match the specific automation objective, such as a particular technology domain. However, if automation spans multiple domains, a service management background may be most valuable.

ESTABLISHING CONTROLS

Automation success is contingent upon effective, sustained collaboration across the organization. However, from a compliance standpoint, **it is essential to establish clear roles and implement strong access controls that support them.** Separation of duties, which requires multiple administrators to conduct specific tasks related to security of sensitive processes and assets, is often mandated by regulatory standards such as SOX or PCI-DSS. Reinforcing separation of duties and a least privilege access policy, role-based access controls provide granular visibility into and secure control over provisioning, patching, and more. Together, they can mitigate the damage a single malicious administrator could inflict. In addition, establishing role-based reporting capabilities allows appropriate team members to access the information they need, while minimizing potential exposure of sensitive intelligence.

BUILDING A CULTURE OF AUTOMATION

An organization's culture should support the move to automation. The following attributes characterize a culture of automation:

- **Continuously improving.** After establishing workflows and policies, the organization should set up processes for periodic reviews and adjustments to address regulatory and environmental changes and new vulnerabilities.
- **Inclusive.** Individuals from across the IT organization and the larger enterprise should be encouraged to provide automation ideas.
- **Shifting workloads.** Along with automating routine tasks, automation efforts should be geared toward shifting workloads from more-experienced to less-experienced team members. For example, when automation of triage tasks allows front-line service desk agents to address a higher percentage of tickets, second and third level staff can be relieved of handling time-sensitive tickets. Development of in-house custom scripts that automation approvals by highly skilled and experienced engineers enables less-experienced staff members to fulfill these responsibilities, freeing senior staff members to concentrate on high-value, strategic efforts, including further automation.

ESTABLISHING POSITIVE INCENTIVES

Automation can often be justified by the fact that it reduces headcount. However, few IT professionals will buy into an effort intended to eliminate their jobs, and therefore may resist automation initiatives. Therefore, **managers must establish clear, positive, and realistic career paths for staff whose jobs are impacted by automation.** Automation strategies must align with employee incentives, including creating career paths for people with the right skills to transition to other areas of IT or on to more strategic projects.

CONCLUSION – BREAKTHROUGH WITH AUTOMATION AND INTELLIGENT COMPLIANCE

IT organizations are being hampered by manual operations tasks, a situation that can cost the organization dearly. If IT takes too long or is inconsistent or inaccurate in provisioning, configuring, or updating infrastructure and services, the business may be at risk from security vulnerabilities and noncompliance penalties.

BMC solutions empower your organization to gain the initial benefits of automation quickly, while maximizing those benefits over time. BMC automation technologies help you optimize agility while maintaining essential governance and compliance controls. Whether your team is tasked with complying with internal policies or external mandates as PCI DSS, HIPAA, or protecting against security threats, BMC solutions can help.

- **TrueSight Vulnerability Management**. Helps IT Operations and Security get visibility into vulnerabilities across the organization, add operational context, prioritize action, identify blind spots and trigger automated remediation.
- **TrueSight Server Automation**. Provides a policy-based approach for IT administrators to manage their data centers with greater speed, quality, and consistency. With broad support for all major operating systems on physical servers and leading virtualization and cloud platforms, server administrators can easily install, configure, patch and maintain servers with ease. Rich, out-of-the-box content helps IT automate continuous compliance checks and remediation for regulatory requirements such as PCI-DSS or security standards like DISA.
- **TrueSight Network Automation**. Enables IT operations staff to improve service delivery across all network platforms and leverage best practices and regulatory standards for a policy-based approach to network management. The solution enables real-time compliance audits and reporting, as well as finding and isolating suspicious endpoints until remediation takes effect.
- **TrueSight Cloud Security**. Automates security testing and remediation for multi-cloud services and containers, to manage configurations consistently, securely, and with an audit trail.
- **TrueSight Orchestration**. Lets IT staff look at the big picture and automate tasks via workflows that span multiple applications, systems, or infrastructure with fewer resources and higher-quality, more-predictable outcomes.

With these capabilities, you can effectively close the SecOps gap and meet your organization's goals for governance, risk mitigation, security, and compliance.

To learn more about IT automation for enhanced security and compliance, we encourage you to access the following resources:

- **End to End Data center Automation**: How to develop an end-to-end automation strategy including patching and compliance
- **Five Key Elements of Complete IT Compliance**: Why bridging the SecOps gap keeps complex and dynamic IT environments fully secure and compliant
- Check out a **Vulnerability Management Demo**

FOR MORE INFORMATION

To learn more about implementing strategic automation, visit **bmc.com/secops**

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.

BMC—The Multi-Cloud Management Company. www.bmc.com

468033