bmc

Thought Leadership White Paper

Transform Your Approach to Device Compliance

Automate and improve the entire compliance lifecycle for industry, government, and internal standards

Table of Contents

Executive Summary

Compliance poses an increasingly complex challenge to enterprises. Industry and government compliance mandates, as well as internal corporate standards, can add up quickly. Meanwhile, in dynamic enterprise IT environments, new applications, updates, and patches come online every day. Further complicating matters, **consumerization and shadow IT require IT teams to discover and track hardware and software elements far beyond their traditional purview.** Although comprehensive compliance is fast becoming an impossible quest, the consequences of a lapse can be critical:

- Regulatory actions and penalties
- Business disruption
- Security breaches
- Damage to corporate reputation

When ensuring compliance, data centers are often looked at first, but IT must also pay close attention to end-user devices—given their diversity and distribution, they can be the weak link that puts the business at risk. Organizations need a new approach that makes it simple to quickly specify the standards to be met and ensure comprehensive compliance without overburdening IT. This paper describes **a simplified approach to device compliance that transforms the entire compliance lifecycle, from definition to remediation.**

WHY IT STRUGGLES WITH COMPLIANCE MANDATES

Compliance is a requirement for virtually every organization. Compliance mandates can come from industry organizations, government agencies, or as part of a corporate policy.

Industry Mandates

Some industries have organizations that define policies that companies must adhere to in order to be in compliance. For example:

- The Payment Card Industry Data Security Standard (PCI DSS) is a requirement for any business that accepts payment cards from customers.
- ISO 9000 is a series of standards, developed and published by the International Organization for Standardization (ISO), which defines, establishes, and maintains an effective quality assurance system for manufacturing and service industries.

Government Mandates

Many businesses must also comply with federal regulatory mandates. Examples include:

- The Sarbanes-Oxley Act (SOX) governing financial institutions
- The Healthcare Insurance Portability and Accountability Act (HIPAA) regulating healthcare organizations
- The Security Content Automation Protocol (SCAP), which initially focused on U.S. federal government agencies but is increasingly being adopted as a set of best practices that can improve security at any organization

Corporate Policies

In addition to industry and government mandates, most organizations also define their own internal IT standards, such as:

- Use case-specific protocols governing data access, use, and storage
- Whitelists and blacklists of acceptable third-party software and websites
- Standardized desktop backgrounds to support branding

Complementing third-party mandates with requirements tailored to the specific needs of the business, these IT standards are an equally important element of compliance. Together, third-party mandates and IT standards comprise an extensive list of requirements to be identified and implemented.

A New Era for Compliance

Achieving and maintaining full compliance with this complex matrix of requirements would be challenging enough in a static IT environment. The burden grows exponentially in the highly dynamic and diverse environments typical of the modern organization. Each month, **thousands of standard updates and patches** across hundreds of applications are released. Also, as new security vulnerabilities emerge, IT must apply urgent out-of-band patches to protect the organization. It's not unusual for an IT department to have hundreds of thousands of patches waiting in the queue at any given time—a vast and seemingly hopeless backlog.

The rising sophistication and empowerment of end users adds to the growing difficulty of ensuring compliance. **With consumerization and shadow IT now prevalent, IT must discover and track hardware and software elements far beyond the traditional scope,** including assets purchased or deployed directly by business users and groups. Most commonly, IT must find a way to discover, configure, secure, and manage end-user devices such as laptops and mobile devices purchased by employees themselves.

IT can't gain control over the compliance challenge through incremental improvements in speed or efficiency. Instead, **IT needs a new approach designed to transform the entire compliance lifecycle, from definition to remediation.**

ACCELERATING AND AUTOMATING THE COMPLIANCE LIFECYCLE

Effective compliance depends on reducing manual work and improving accuracy from beginning to end: from standards definition, through enforcement and monitoring, to remediation.

Device Discovery and Inventory

The biggest issue that faces IT today is how to quickly identify and apply compliance to all devices within their control. Without automated processes in place to inventory all the devices that are in the environment, including both new and existing ones, and detect changes to them, IT will be unable to ensure accurate and comprehensive compliance adherence. This becomes even more critical in environments where IT has limited or no involvement in the purchase and configuration of new devices, such as in organizations supporting BYOD programs.

Failure to detect new devices can quickly undermine compliance efforts—with potentially devastating results.

IT departments that can quickly identify new devices as they enter the environment can put into place processes, both automated and manual, to address the situation and prevent issues from arising. Successful compliance lifecycle processes include alerting when new devices are identified, assessing vulnerabilities, and implementing the correct processes to resolve devices found to be out of compliance. As a result, IT can **make compliance an integral part of the device management lifecycle.**

Automate enforcement of compliance mandates and company policies during every segment of the device management lifecycle.

Rapid Definition of Compliance Mandates

Effective device compliance depends on an understanding of the full set of requirements an organization must meet, including government and industry regulations as well as internal company policies. Given the scope of the challenge, organizations need to seize opportunities to automate as many aspects of device compliance as possible. Successful IT groups rely on automated tools not only for discovery, but also to identify non-compliance and steps needed for remediation.

To streamline the time-consuming process of identifying, aggregating, and implementing multiple standards, **IT should make use of any available opportunities to automate device compliance detection.** Some mandates, such as SOX and PCI DSS, allow only partial automation on devices and do not provide templates. Others, such as SCAP, allow the entire policy to be automated; IT can simply import an XML template and begin scanning devices for compliance.

Once automation of the most critical compliance requirements has been addressed, IT can incorporate the company's own policies—for example, locking down USB ports to prevent data exfiltration or specifying a known good software state for user devices to prevent them from undermining security or performance. In this way, IT can arrive at a complete definition of the compliance requirements for end-user devices much more quickly and efficiently.

Automated Compliance Monitoring and Remediation

Once devices are compliant with external and internal mandates, IT needs a way to ensure that any lapses are remediated before they affect the business. For example:

- **A company must address PCI DSS violations within a specific interval of time** to avoid losing the ability to process payments—a business-critical risk for any retailer or service provider.
- **A delay in implementing a security patch can leave the company exposed to a highly damaging cyberattack** or data theft with serious consequences for its business relationships and financial performance.

Many companies rely on automated alerts and reports for compliance violations, but this information can be of limited use. It doesn't help IT much to learn that there are 13,000 violations across the enterprise, including hundreds each of the most common lapses. Automated remediation is essential to bring out-of-compliance devices back to standard. For example, if IT defines a policy to require a certain version of Oracle® Java® on client devices, it should also be able to define a rule for handling devices found to be running a different version, such as replacing the noncompliant version automatically with the standard, without the need for staff intervention. Notifications can be reserved for the few cases where automated remediation has been unsuccessful and/or personal attention is needed.

Freed from constant alerts of routine violations and repetitive manual remediation, IT can focus on higher-level compliance activities and other strategic tasks.

NEXT STEPS

As the costs for non-compliance continue to rise through increasing regulatory fines, settlements, and restitution, organizations are increasing their staff to try and stop financial losses, as well as reputational losses. As reported recently in the Wall Street Journal, both the numbers and the salary levels of compliance professionals within enterprises are growing rapidly:

> "Hefty fines and other penalties have jolted companies, especially banks, into a compliance hiring spree, as governments at home and abroad tighten business laws and regulations and ramp up their enforcement activity."[1]

To get the costs of both non-compliance and compliance under control, IT needs to identify areas in which it can reduce costs and increase effectiveness.

1 Gregory J. Millman and Samuel Rubenfeld, "Compliance Officer: Dream Career?" *The Wall Street Journal,* January 15, 2014.

As part of a comprehensive compliance strategy, IT should communicate the goals of device compliance throughout the organization, as well as the potential risks of being out of compliance. By working with other departments within the organization, IT can share the goals by:

- Identifying areas where compliance is needed
- Communicating the costs of non-compliance
- Sharing the steps and processes that IT is implementing to ensure compliance
- Defining devices that cannot be introduced into the environment due to the inability to bring them into compliance

CONCLUSION

The growing complexity of device compliance calls for a new approach by IT. Manual methods for defining requirements and remediating violations can actually increase backlogs and risks for the business. Instead, IT should apply automation across the entire compliance lifecycle, from device discovery and inventory, to compliance templates that jump-start the definition process, to rules for handling violations without the need for IT intervention. In this way, IT can:

- **Ensure comprehensive compliance** with both third-party and internal mandates across all end-user devices, including personally-owned devices used under a BYOD program
- **Address compliance gaps quickly and efficiently** to minimize risk to IT and the business
- **Control the rising cost of both compliance and non-compliance** by increasing staff productivity and reducing lapses

FOR MORE INFORMATION

To learn more about device compliance and how many organizations benefit from BMC Client Management, please visit **bmc.com/it-solutions/client-management.html**

467567