bmc helix

Automated Security for the Hybrid Cloud Enterprise

Achieve best-in-class security and compliance with BMC Helix Remediate

Table of Contents

IT has Never Been More Complex – or Under Greater Attack

Today's IT leaders face a new and unique challenge: transform from an operational team that "keeps the lights on" to an engine of innovation and business growth. Yet while the digital transformation mandate is clear, the path to success is complex.

IT must not only sustain its maintenance responsibilities alongside innovation initiatives, it must improve them to both power the business more effectively and open up bandwidth for future-focused projects. The team must navigate the move to the cloud and juggle regulatory and internal compliance requirements. And perhaps most importantly, IT must protect against always-evolving security threats, which continue to increase in number and intensity.

In a 2018 global Deloitte survey, CIOs named "transforming enterprise business operations" and "driving top-line growth and revenue" as their top two key mandates.[1]

[1] https://www2.deloitte.com/us/en/insights/topics/leadership/global-cio-survey.html

Security On-Premises: The Need to Move Beyond Manual Processes

Manual tasks constitute one of IT's biggest impediments to change. Because IT staff perform a relatively high percentage of tasks manually, little time remains for innovation. Manual tasks not only take resources away from projects focused on business growth, they can increase system downtime, disrupt the delivery of critical business services, and cause inefficiency and change rollbacks.

- 80% of unplanned outages are due to ill-planned changes made by administrators or developers
- 89% of IT decision makers believe that their organization should be spending more on innovation
- 77% believe that they're spending too much on basic maintenance and support of systems and IT infrastructure

Organizations with predominantly manual vulnerability management processes can experience a lack of collaboration and teamwork between Security and Operations teams, compromising organizational security. IT Security runs vulnerability scans to identify constantly evolving weaknesses but they do not own the implementation of the steps needed to close them. When Operations receives scan data from the Security team, it lacks context and requires slow, extensive, tedious analysis to make it actionable.

Security challenges don't stop there. Manual methods of deploying security patches and configuration changes can't keep up with the high volume of vulnerabilities and rapidly expanding attack surface. Security and Ops staff are overwhelmed and many vulnerabilities go unaddressed. The stakes have never been higher - a data breach can have reverberating effects on revenues, brand image, reputation, goodwill, customer retention, and more - but it has never been harder to protect enterprise systems and data.

- 68% of IT practitioners believe that data breaches occur because patch management is poorly executed
- 57% think that past breaches may have occurred because patches for known vulnerabilities were available but not applied
- 61% say that their organizations are at a disadvantage in responding to vulnerabilities due to manual processes
- 55% agree that IT security spends more time navigating manual processes than responding to vulnerabilities, leading to an insurmountable response backlog

58% of enterprise organizations suffered a security breach at least once in the past year, and 41% of those external breaches exploited a software vulnerability.

Security in the Cloud: The Challenges of Configuration at Scale

Cloud security also requires a specific set of skills, methods, and solutions. In addition, many organizations do not realize that the shared responsibility model for cloud security places responsibility for securing data on the customer, not the cloud service provider. There is a very good reason that 93% of IT executives are very worried about public cloud security.

Public cloud resource misconfigurations remain the #1 cause of cloud security failures, with nearly 1 billion records exposed and reported incidents up 20% year-over-year in 2018.

With cloud, the speed and scale of change are exponentially greater. Autonomous, self-organizing scrum teams continuously update their microservices, each one of which uses dozens or even hundreds of cloud IaaS and PaaS resources. Those resources must be configured appropriately if they are to be secure. Unfortunately, 53% of enterprises mistakenly believe their cloud service provider (CSP) is either wholly or majority responsible for securing their data on their platform.

Some security teams attempt to solve their cloud security challenges with extra-tight governance, but these measures conflict with the pace and culture of innovation. Scrum teams must innovate faster and will use their own credit cards if that's what it takes to succeed. Teams frequently spin up shiny new services from their cloud service provider without considering how to securely configure them. Like many on-prem security processes, cloud configuration testing remains manual and ad-hoc.

The result: cloud security failures can happen to anyone, even organizations with a mature cloud strategy. For example:

- A misconfigured AWS WAF (Web Application Firewall) service exposed PII data (including social security numbers) of 100 million USA customers of Capital One. (July 2019)
- A misconfigured AWS Elasticsearch service exposed 340 million records of USA citizens (Exactis breach, July 2018)
- An unsecured Kubernetes console led to crypto-jacking of Tesla's AWS infrastructure (WIRED, Feb 2018)

The shift to the cloud is a foregone conclusion - 91% of enterprises already use public cloud - but its security is anything but certain. In addition, organizations need IT solutions that enable agility while also ensuring security.

The Foundation for Modern IT Success: Automation

While the challenges of security on-premises and in the cloud are diverse, a single category of solutions can address almost all of them: automation.

Automation can improve security, increase productivity, lower costs, and make changes with greater speed and accuracy. It can also enhance communication, collaboration, and teamwork among Security, Operations, Cloud, and Development teams to help close the "SecOps gap" and deliver greater organizational security. The adoption of automated solutions can enable these groups to work more closely together to quickly and accurately identify, prioritize, and remediate more vulnerabilities in less time.

Automation solutions can cover security, regulatory and rules-based compliance, configuration management, provisioning, software distribution and more - ideally in an integrated way. Automating these components empowers IT to enable agility instead of hindering it. It allows Security teams to be a partner to innovation, not a roadblock, reducing the tendency of developers to use cloud in the shadows. Selective, automated governance replaces draconian methods with measures that streamline productivity instead of standing in its way.

Although the benefits of automation are well known, organizations continue to struggle with strategic implementations.

- Less than half of organizations are using or piloting server automation software (17% full usage, 30% piloting).
- Only 16% of organizations use network automation tools, and 70% still make changes manually using the command line interface on individual devices.
- Just 21% of organizations use comprehensive configuration automation software.
- 55% of organizations are looking to deploy a new cloud security solution within the next 12 months

Automating the complex processes around security and compliance can be challenging - but it's also critical. With best-in-class automation, CIOs and CISOs can achieve their mandate: meet the day-to-day demands of the business, adopt new technologies, invest more in innovation, and strengthen their IT security.

Automation empowers IT to enable agility, not hinder it.

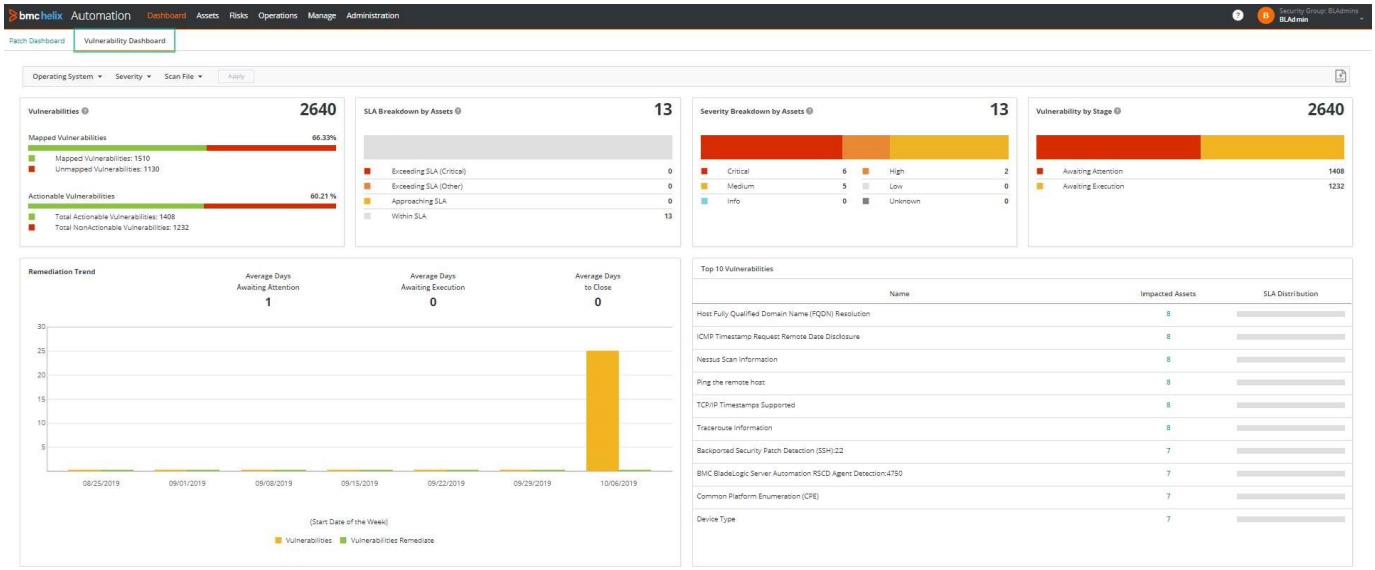
BMC Helix Remediate: Automated Security and Compliance of Your Entire Hybrid Cloud Footprint

BMC Helix Remediate addresses these challenges in a new, integrated way across your entire IT ecosystem. The solution automates the security and compliance of your entire hybrid cloud footprint, including on-prem servers, networks, and public cloud IaaS and PaaS resources, to remove bottlenecks and raise productivity. Discovery integration helps eliminate blind spots, and automated configuration, vulnerability, and patch management fortify your infrastructure consistently and with greater efficiency. Built-in remediation securely configures IaaS and PaaS services, while integration with incident and change management workflows keep operations running smoothly so scrum teams can keep their feet on the gas pedal.

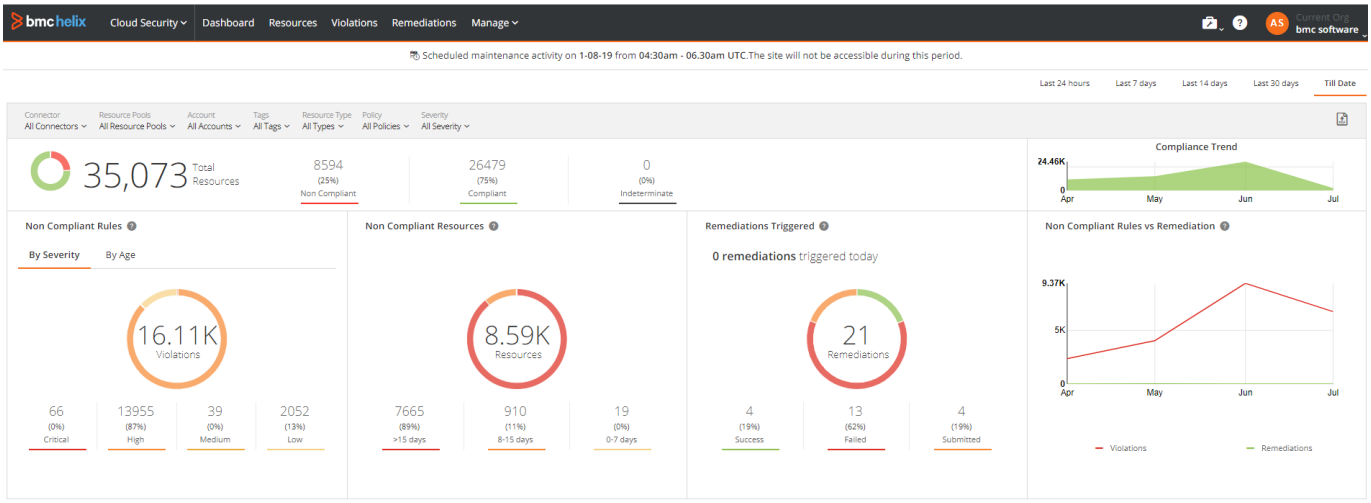
A Hybrid Approach to Security for a Hybrid Cloud World

BMC Helix Remediate is delivered as SaaS and uses a hybrid cloud model for the management of both on-premises and cloud-based infrastructure.

BMC Helix Remediate is deployed in the public cloud of your choice and automates the management of security vulnerabilities and deployment of patches in your on-premises infrastructure. It is augmented with on-premises solutions for servers and network devices that automate the execution of tasks associated with patch management, compliance, configuration management, software distribution, and provisioning.



Visibility to key vulnerability management metrics



Dashboard showing misconfigured resources and remediations

BMC Helix Remediate automatically identifies and remediates misconfigured cloud services and configurations to mitigate security risks and ensure compliance with policies and regulatory standards.

This approach can be a strategic catalyst for cloud migration. It allows the enterprise to move from on-premises to the cloud in steps. The organization gains the opportunity to re-engineer and leapfrog security best practices and deploy solutions that make the public cloud infrastructure more secure than on-premises deployments.

Gartner calls hybrid cloud “the foundation for digital business” and projects that hybrid cloud will grow from $209B in 2019 to $317B by 2022 - a 52% increase.

Why BMC Helix Remediate?

BMC Helix Remediate automates the management of hybrid cloud security vulnerabilities as one comprehensive, integrated solution.

Benefits for on-premises environments:

- Remediate security vulnerabilities in a fraction of the time required by manual methods
- Improve security with simplified patching for increased speed and productivity while reducing risk
- Use advanced analytics and automation to map security vulnerabilities to servers and networking devices, identify business services exposed, set priorities, determine patches or configuration changes required, obtain required remediations, take rapid corrective action, and generate reports
- Manages configurations to help secure your IT environment across your infrastructure (e.g. patch, compliance, configuration management)
- Reduce human error for higher quality deployment of patches, fewer rollbacks, and higher system uptime
- Shift high-cost skilled labor from maintenance tasks to strategic projects
- Power innovation that delivers competitive advantage and greater customer value

Benefits for public cloud deployments:

- Automates security testing and remediation to manage cloud configurations consistently, securely, and with an audit trail
- Cloud security scoring and remediation for public cloud IaaS and PaaS services from AWS, Azure, and Google Cloud Platform (GCP)
- Container configuration security for Docker and Kubernetes
- Leverage integration with closed-loop incident and change management to save labor and increase efficiency
- Enables scrum teams to manage security of their cloud-native apps, removing bottlenecks and accelerating agility

Customer Snapshot

A large Canadian bank reduced security patch implementation time from 2 weeks to less than 24 hours - a 14x increase in speed.

Stay Ahead of the Threat with Security Automation

To succeed in today's business climate, IT must deliver on both day-to-day activities and moonshots - which means using automation to ensure security, productivity, and cost-effectiveness alongside agility, speed, and innovation. BMC Helix Remediate provides exactly that, making security agile while delivering maximum defense against security threats.

For more information

To learn more about BMC Helix Remediate, go to bmc.com/remediate

About BMC

BMC delivers software, services, and expertise to help more than 10,000 customers, including 92% of the Forbes Global 100, meet escalating digital demands and maximize IT innovation. From mainframe to mobile to multi-cloud and beyond, our solutions empower enterprises of every size and industry to run and reinvent their businesses with efficiency, security, and momentum for the future.

BMC – Run and Reinvent **www.bmc.com**