BMC SecOps Solutions

Proactively mitigate security risks with automation and holistic visibility

BMC alignment with federal government SecOps

CHALLENGES

In May 2018, in accordance with a Presidential Executive Order, a Federal Cybersecurity Risk Determination Report and Action Plan was initiated. The risk assessment conducted by the Office of Management and Budget (OMD), in coordination with DHS, confirmed the need to take bold approaches to improve Federal cybersecurity. OMB and DHS determined that **71 of 96 agencies (74 percent) participating in the risk assessment process have cybersecurity programs that are either at risk or high risk.**[1]

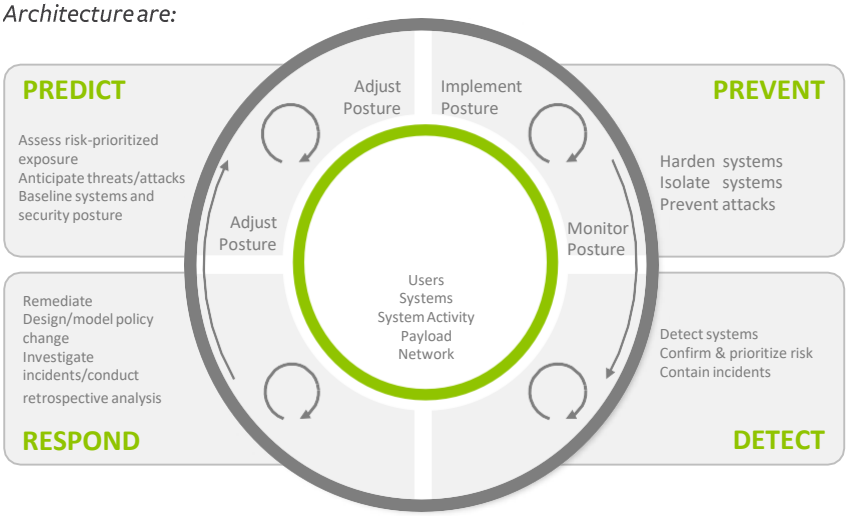
INCREASING THREATS

To effectively operate in today's digital era, **federal organizations increasingly need the ability to deliver new and innovative applications at a much faster pace to manage today's vast amounts of data.** This increased level of data inspires hackers to become much bolder in their attempts to breach systems. Meeting today's demands significantly increases the complexity to manage IT environments. Today's government IT leaders are challenged with managing increased organizational expectations, while also complying with complex regulatory standards, and defending IT infrastructures against an increased amount of cyber threats.

BMC SOLUTION

BMC SecOps solutions automate prioritization and remediation of the most critical vulnerabilities or compliance violations. By combining vital context with unprecedented visibility into data center assets and their relationships, BMC SecOps solutions help improve productivity and scalability by breaking through functional silos to incorporate security into operational processes. Enterprise-grade remediation for known and unknown threats protects network uptime and maintains stability.

Security analytics and machine learning are key components of adaptive security architecture. According to Gartner, the Four Stages of an Adaptive Security Architecture are:



KEY FEATURES

Compliance Controls
- Ensure continuous compliance with a full cycle of system discovery, monitoring, remediation, and integrated change control

Security View of Operational Plans
- **Visualize how quickly risks will be eliminated with graphical views of planned operations actions, predictive SLAs, and burn-downs**

Service and Operational Analytics
- Address risks based on policy and impact to ensure the most critical issues are fixed first, uptime is protected, and stability is maintained

Blind Spot Protection
- Identify assets that are unmonitored and potentially exposed, and automatically map dependencies

KEY BENEFITS

Agile Execution
- Accelerate remediation of vulnerabilities while driving operational excellence with automation to avoid security incidents

Integrated Visibility
- Enable coordination between security and operations teams fueled by integrated and holistic visibility into risks, impacts, and operational plans

Rigorous Controls
- Gain visibility, consistency, and reliability across processes to increase speed, reduce errors, and simplify

27%

of agencies reported that they have the ability to detect and investigate attempts to access large volumes of data[1]

ORGANIZATIONAL CHALLENGE

One of the primary reasons federal organizations struggle against security threats is still the lack of integration and coordination between security and operations departments. Security teams scan for vulnerabilities and then deliver that information to the operations team for action. However, that information frequently lacks the business or operational context the IT operations team needs to take or prioritize action.

Per the 2019 Oracle and KPMG Cloud Threat Report, 1 out of 10 organizations can analyze 75% of their security events.[2]

PRODUCT DETAILS

TrueSight Vulnerability Management

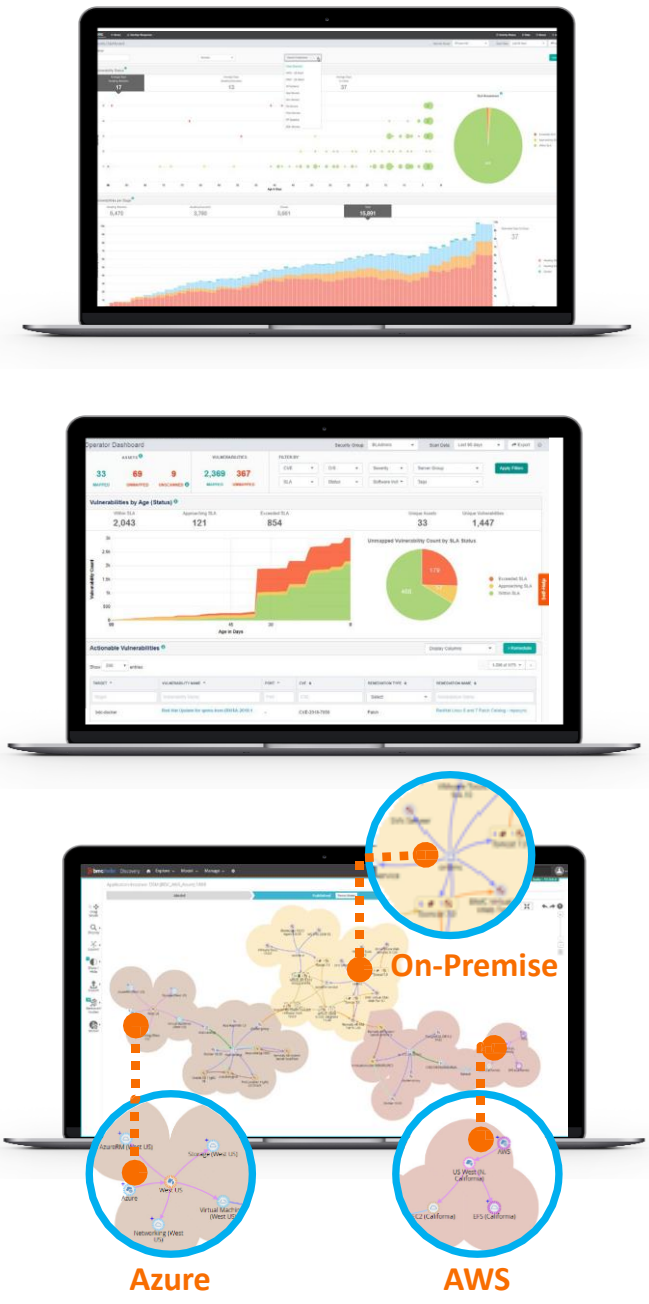
TrueSight Vulnerability Management prioritizes risks and reduces your overall attack surface by providing operations teams with prescriptive and actionable data to address vulnerabilities based on perceived impact and policy. It also offers security teams a transparent view into operational plans by providing visibility into planned actions, predictive SLAs, and burndown views. Through integration with BMC Discovery, teams can identify application context and blindspots—systems previously unknown or unmanaged—and make adjustments.

TrueSight Server and Network Automation

TrueSight Automation for Servers provides a policy-based approach for managing data centers with greater speed, security, quality, and consistency. Broad support for all major operating systems on physical servers and leading virtualization and cloud platforms lets IT install and configure server changes with ease. Rich, out-of-the-box content helps IT automate continuous compliance checks and remediation for security or regulatory requirements. Now IT staff can build, configure, and enforce compliance faster and more reliably. With a simplified web portal, the IT operations team can increase the server to admin ratio, gain productivity, complete audits swiftly, and quickly respond to increasing business demands.

Discovery

Continuously discover the hardware, applications, storage, databases, and other components that make up your data center and map the relationships between them automatically with agentless discovery.



FOR MORE INFORMATION

To learn more about BMC TrueSight, visit
bmc.com/truesight

About BMC
From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent **www.bmc.com**