

Security Starts with BMC Discovery

Reduce risk across your distributed environment with greater visibility, automation, and insight

THREATS ARE MULTIPLYING

IT security teams face relentless pressure from both internal and external sources as the number and intensity of security attacks continue to grow. Thanks to shadow IT, **sensitive data now lives everywhere**. Unused applications and inactive devices, especially when unidentified, open penetration points for security attacks, while third-party software, open source inventory, and assets that lie unsecured outside the datacenter introduce additional risk.

CHALLENGES

Processes for evolving regulatory standards are often manual or poorly defined, and therefore cannot be quickly and easily executed. On top of preventing and addressing threats, security teams must document their methods or face time-consuming audits and expensive fines. Pressure from internal sources is just as strong. The business expects more from IT at both the individual and corporate levels, from users who demand a consumer-level experience to executives who require IT to be a strategic enabler to top- and bottom-line objectives. **Collection of IT asset and inventory data is costly, resource-intensive, and inaccurate**. With information stuck in silos, security and operations teams rely on outdated processes, which results in poor service quality, unnecessary business downtime, and an outdated environment that can't scale.

BMC SOLUTION

BMC Discovery addresses these security challenges and more by providing a complete view of your environment. **BMC Discovery offers deep insight into your full infrastructure**, from data center servers, cloud services, network, and storage to the mainframe, so you can stay ahead of today's ever-growing risk and complexity.



KEY FEATURES

BMC Discovery mitigates risk and reduces business impact.

- **Streamlined data inventory** to identify blind spots and unscanned systems enable rapid assessment of known vulnerabilities
- **Deep business service awareness** when assessing and remediating vulnerabilities in key infrastructure and cloud resources
- **A single point of reference** for visualizing and reporting on resources in a distributed environment
- **Full coverage of a distributed environment** aligned with key business infrastructure to coordinate security with operations teams and provide more valuable reporting and remediation
- **Application and business service context to security alerts** via integration with your SIEM solutions

KEY BENEFITS

- **Mitigate risk:** Respond to threats and vulnerabilities more quickly while improving assessment of business impact
- **Lower time and labor costs:** Reduce the resources required to identify vulnerabilities and execute remediation action
- **Decrease risk of vulnerabilities due to end-of-life software:** Lower the number of deployed legacy OSs and software running in your environment

