

# Security Starts with BMC Discovery

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

## THREATS ARE MULTIPLYING

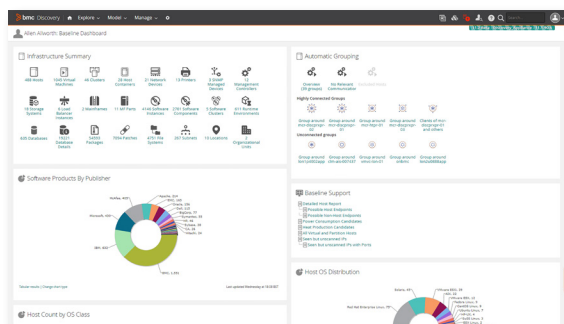
IT security teams face relentless pressure from both internal and external sources as the number and intensity of security attacks continue to grow. Thanks to shadow IT, **sensitive data now lives everywhere**. Unused applications and inactive devices, especially when unidentified, open penetration points 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 With information stuck in silos, security and operations teams rely on outdated processes, which results in poor service quality, unnecessary business downtime, and an outdated environment that can't scale.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

## HOW IT WORKS

With automated discovery and dependency mapping, you can formulate and execute a plan to resolve known vulnerabilities with the least amount of risk. BMC Discovery helps you evaluate business impact more quickly and conclusively, then respond to critical events with reduced risk of incorrect assignment and assessment. With BMC Discovery, you will proactively identify trends, abnormalities, and security vulnerabilities and automatically remediate them before they impact the business.

As part of an integrated approach to security and operations, BMC Discovery offers multiple capabilities:

- **Automated discovery:** Automatically discover infrastructure, hardware, software, cloud resources, and dependencies using agentless methods and pre-defined application patterns.
- **Application modeling:** Map discovered components into business application models from any point of the application via an intuitive graphical interface, reducing the need for deep product knowledge.
- **Version sprawl assessment:** Leverage dashboards that provide instant insight into deployed versions of OSs and software and visibility into their lifecycle status.
- **Security integration:** Use BMC Discovery data across your security-operations ecosystem, including vulnerability management tools, remediation prioritization, and live risk dashboards.
- **SIEM service context:** Boost your security information and event management (SIEM) solutions with integrated discovery data.

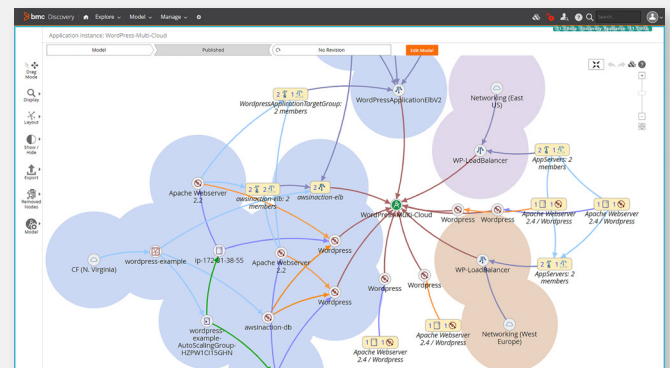
BMC Discovery also impacts top key performance indicators (KPIs) for security teams, including:

- **Time to communicate breaches and their impact to the business** (an NERC and HIPAA requirement)
- **Average time to detect new assets and vulnerabilities**
- **Percentage of controlled services and unpatched systems**
- **Average time to retire/decommission assets**
- **Patch deployment duration** (the time between a patch release and the ecosystem becoming compliant)

## FOR MORE INFORMATION

To learn more about improved security with BMC Discovery, visit [bmc.com/discovery](http://bmc.com/discovery).

- BMC Discovery scales across the largest and most complex multi-cloud environments, including AWS and Azure, offering unparalleled visibility.



BMC is a global leader in innovative software solutions that enable businesses to transform into digital enterprises for the ultimate competitive advantage. Our Digital Enterprise Management solutions are designed to fast track digital business from mainframe to mobile to cloud and beyond.

**BMC digital IT transforms 82 percent of the Fortune 500.**



BMC, BMC Software, the BMC logo, and the BMC Software logo, and all other BMC Software product and service names are owned by BMC Software, Inc. and are registered or pending registration in the US Patent and Trademark Office or in the trademark offices of other countries. All other trademarks belong to their respective companies. © Copyright 2017 BMC Software, Inc.

