e-book

Autonomous Digital Enterprise

ADAPTIVE CYBERSECURITY

bmc

Table Of Contents

Introduction

The Autonomous Digital Enterprise is a vision of the future state of businesses, enabled by the five tenets shown in Figure 1.

Security is an ongoing concern for today's businesses, a constantly-changing, ever-increasing threat landscape with growing regulatory and compliance requirements. Adaptive Cybersecurity is the evolution of security functions that can automatically sense, detect, react, and respond to access requests, authentication needs, and outside and inside threats, and meet regulatory requirements. It's enabled by artificial intelligence (AI), crowdsourcing, and security-integrated DevOps (DevSecOps).

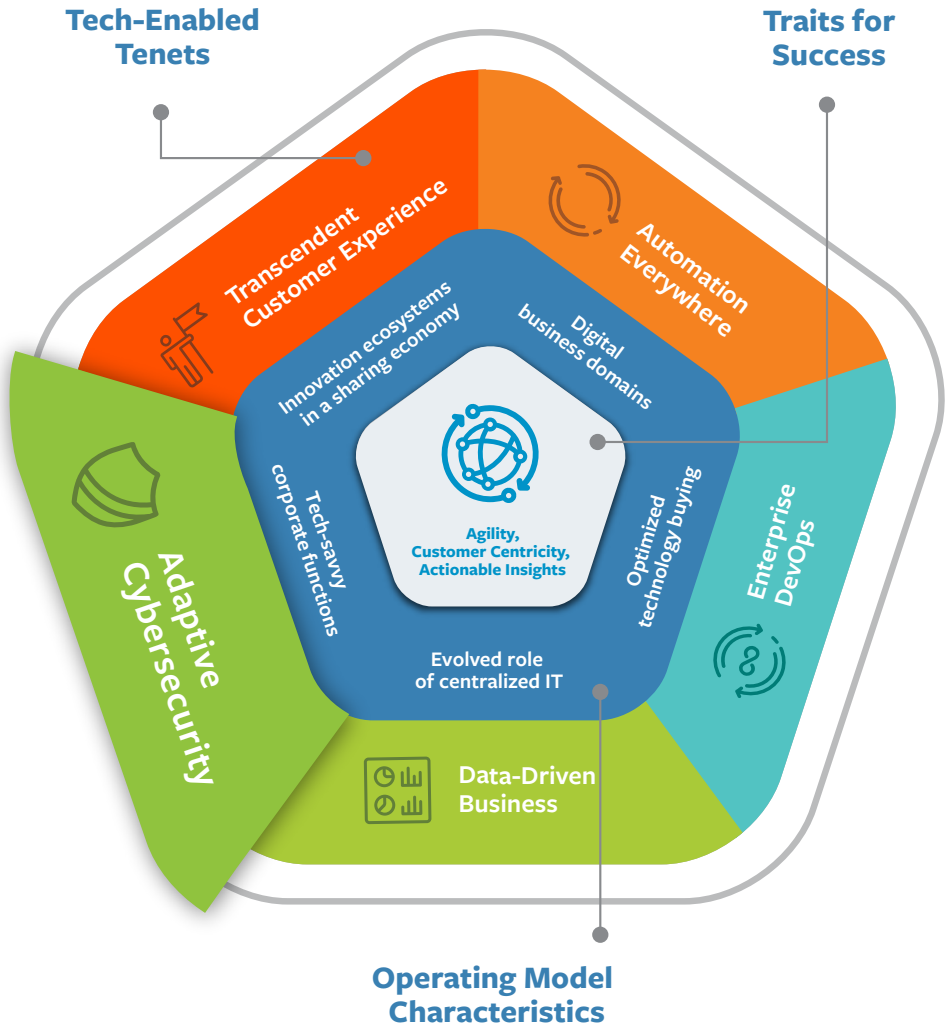
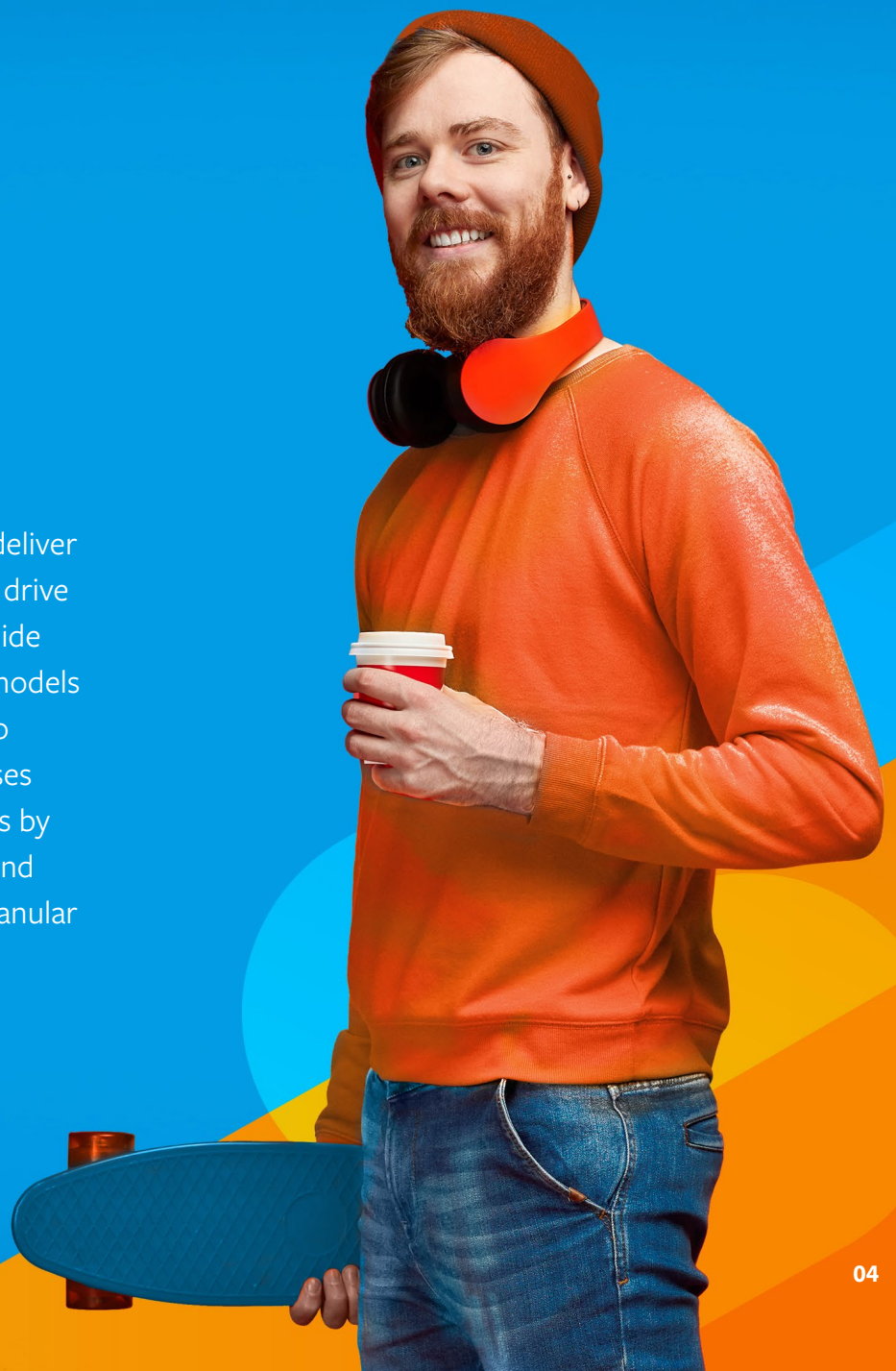


Figure 1: The Autonomous Digital Enterprise

Enabling Technologies

The technology behind Adaptive Cybersecurity works together to deliver a comprehensive security presence. AI and machine learning (ML) drive behavioral analytics of users and entities to combat inside and outside threats. Multi-factor authentication and distributed authorization models provide better access controls. Embedding application security into DevOps functions creates a new DevSecOps functionality. Businesses can enhance their infrastructure security for cloud-based processes by leveraging automated cloud configuration management solutions and cloud service provider tools. Zero Trust security models protect granular resources from the inside out.

In this e-book, we will look at five use cases that demonstrate how Adaptive Cybersecurity can improve current processes, as well as the BMC solutions that can help deliver strategies for success.



Use Cases

Automated Vulnerability Remediation

Remediating vulnerabilities is a constant security concern and it's an area ripe for an automation makeover. According to the National Institute of Standards and Technology[1], there were over 18,000 new security vulnerabilities uncovered in 2019. Current processes are outdated, and grounded in manual, error-prone procedures that jeopardize compliance and increase risk. And they're often siloed so that security departments don't receive all of the information they need. By automating vulnerability scans, asset mapping, and remediation tasks and viewing all of them from a single dashboard, vulnerabilities can be addressed and closed quickly to improve system security and keep up with threats.

18,000
new security vulnerabilities were uncovered in 2019.[1]

[1] *National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing,* National Institute of Standards and Technology, 2020.

Blind Spot Identification

Blind spots encountered during server scans mean the door's already been open for potential breaches and attacks. While identifying blind spots is highly time-consuming, it's also important work and requires the use of both discovery solutions and security scanners. According to IBM[2], a single data breach can cost an impacted company $3.86 million. With blind spot identification, IT security departments can augment security scanner data with discovery information, allowing them to scan and automatically identify every server in the data center and get a complete picture of vulnerabilities for remediation before a breach occurs.

A single data breach can cost an impacted company $3.86 Million.[2]

[2] *IBM 2020 Cost of a Data Breach Report*, IBM, 2020.

Regulatory Cloud Compliance

Accelerated, increasingly complex innovation in the cloud and across hybrid environments—including widespread adoption of containers, microservices, and agile methodologies—is driving higher demands for security and compliance. There's also the tangential higher risk of non-compliance with regulatory controls and the potential release of non-compliant updates.

Automating the "find and fix" of misconfigured cloud resources and integrating it with discovery and change management processes can improve security and compliance across your environment. From a single dashboard, you can quickly detect and remediate misconfigured resources across multicloud environments.

App-Centric Cloud Security

The extensive implementation of containers, microservices, and agile methodologies has increased both the speed at which Dev teams push updates to production and the risk of exposure due to inconsistent security reviews. Consistent, secure configuration across the DevOps lifecycle can help close these underreported and very expensive loopholes.

According to McAfee[3], 99 percent of misconfigurations go unnoticed—a disconnect between the 37 monthly misconfiguration incidents that respondents said they were aware of and McAfee's real-world data that estimates the number to be closer to 3,500 a month. Cloud security company DivvyCloud did the math on that in a 2020 study[4] and came up with a valuation of $5 trillion in losses over the last two years—just for the reported cases.

Using platform as a service (PaaS) and infrastructure as a service (IaaS) during the development, testing, and production phases and integrating with the continuous integration/continuous delivery (CI/CD) pipeline can help ensure consistent, secure configurations. Contextual application topologies that enable scrum teams to easily manage cloud-native app security can accelerate business agility and improve app-centric and multicloud security postures.

99% of misconfigurations go unnoticed.[3]

[3] *Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report*, McAfee, September, 2019.
[4] *2020 Cloud Misconfigurations Report*, DivvyCloud, 2020.

Automated Detection, Response, and Reports on Mainframe Security Events

The mainframe is the workhorse behind the scenes, and while it is often taken for granted as inherently more secure, it is in fact more vulnerable than many realize, though relatively easy to protect. While chief information security officers (CISOs) and enterprise security analysts believe every system should be secure and visible to the Security Operations Center, they can lack the awareness of and ability to resolve mainframe vulnerabilities like zero-day threats, configuration weaknesses, privilege escalation, and ransomware. Any single point of risk is an opportunity for an attacker. It's time to block that opportunity by integrating mainframe security with the security information and event management (SIEM) tools enterprises already own for real-time threat detection and response.

Using tools that automate detection and response enables real-time visibility into mainframe threat events as they happen. Performing analysis and sharing insights like indicators of compromise and audit trails of potentially malicious activities in common security terms empowers security analysts to respond quickly, regardless of their level of mainframe expertise. Automating these functions allows an evolution from manual workflows that depend on lengthy investigations spent correlating data and extending exposure to attacks. Alert volume also decreases as automated tools do a better job of accurately surfacing actionable findings without causing alert fatigue.

BMC Solutions

BMC offers a range of solutions designed to help your organization adopt an Adaptive Cybersecurity posture that addresses the use cases presented above.

BMC Solution	Use Cases				
	Automated Vulnerability Management	Blind Spot Identification	Regulatory Cloud Compliance	App-Centric Cloud Security	Automated Detection, Response, & Reports on Mainframe Security Events
BMC AMI Security	—	—	—	—	✓
BMC Helix Cloud Security	—	—	✓	✓	—
BMC Helix Discovery	—	✓	—	—	—
BMC Helix Vulnerability Management	✓	✓	—	—	—
TrueSight Automation for Servers	✓	—	—	—	—

BMC AMI Security

BMC AMI Security automatically protects, detects, and responds to threats on your mainframe, sharing details with your enterprise SIEM in real-time with actionable insights for incident responders. Continuously protect a critical piece of your infrastructure, leverage your existing security investments, and harden the mainframe against vulnerabilities, insider threats, and data theft. It also provides:

- Enterprise SIEM integration for real-time threat visibility
- Actionable intelligence in common language for fast, effective incident response
- Out-of-the-box policies and the industry's largest library of Indicators of Compromise (IOCs)
- Tools to address compliance with alerts, audits, reports, and comprehensive mainframe visibility

To learn more, please visit **bmc.com/ami-security**

BMC Helix Cloud Security

Designed for the cloud, in the cloud, BMC Helix Cloud Security takes the pain out of security and compliance for resources and containers with automated cloud security posture management. Features include:

- Cloud security scoring and remediation for public cloud IaaS and PaaS services from Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)
- Container configuration security for Docker, Kubernetes, OpenShift, and GKE
- Automated ticketing enrichment through IT service management (ITSM) integration
- Ready-to-use CIS, PCI DSS, and GDPR policies, plus support for custom operational policies
- Automated cloud server security management for AWS EC2

To learn more, please visit **bmc.com/cloudsecurity**

BMC Helix Discovery

BMC Helix Discovery is a single, cloud-native discovery and dependency mapping solution for visibility into hardware, software, and service dependencies across multicloud environments that lets you dynamically model your asset dependencies and proactively manage your environment regardless of the solutions. You can also:

- See assets and dependencies in a single pane of glass, whether on-premises or in the public or private cloud
- Empower security operations to perform essential prevention and detection
- Start mapping from any piece of information—software, hardware, or services
- Reduce service outages with predictable change and configuration management
- Choose a cloud-native service offering

To learn more, please visit **bmc.com/discovery**

BMC Helix Vulnerability Management

BMC Helix Vulnerability Management keeps you ahead of threats by quickly closing on-premises and cloud-based security vulnerabilities. The solution captures and consolidates vulnerability scanner data, augments it with BMC Helix Discovery information, and uses advanced analytics to transform it into actionable information. After mapping vulnerabilities to servers and patches, it identifies the severity and business services exposed, schedules remediation, and takes automated corrective action. Additional features include:

- Real-time visibility to vulnerabilities on unmapped assets, missing patches, and misconfigured resources
- State-of-the-art, simplified patching for rapid vulnerability remediation
- A hybrid deployment model with a software-as-a-service (SaaS) component that's cloud-deployable with on-premises components (i.e., server automation)
- Automated detection and remediation of misconfigured cloud resources to strengthen security and improve compliance with regulations and operational policies

To learn more, please visit
bmc.com/it-solutions/bmc-helix-vulnerability-management

TrueSight Automation for Servers

Get cross-platform server automation for better security, compliance, configuration management, and agility with TrueSight Automation for Servers. Threat remediation includes automated vulnerability management that rapidly analyzes security vulnerabilities, obtains necessary patches, and takes corrective action. Real-time visibility improves patch compliance and automates maintenance windows and change management processes. You can also use the solution to:

- Integrate role-based access control, and use pre-configured policies for CIS, DISA, HIPAA, PCI, and SOX remediation and compliance
- Detect and remediate configuration drift and manage change activities to ensure stability and performance
- Automate build-out of services and applications from virtual machine (VM) provisioning to fully operational
- Assess change impact, get real-time status of jobs, or complete an audit using multiple dashboard views

To learn more, please visit bmc.com/it-solutions/truesight-server-automation

Conclusion

Anticipating threats before they happen, and jumping quickly into action when they do, is an integral component of the digital transformation of every business. Adopting an Adaptive Cybersecurity approach is just one tenet of the Autonomous Digital Enterprise, a forward-looking vision of the future state of business. Companies that want to not only survive but thrive as their business evolves must include the latest security measures and enabling technologies in their planning.

To learn more about how your business can evolve to an Autonomous Digital Enterprise, please visit **bmc.com/ADE.**

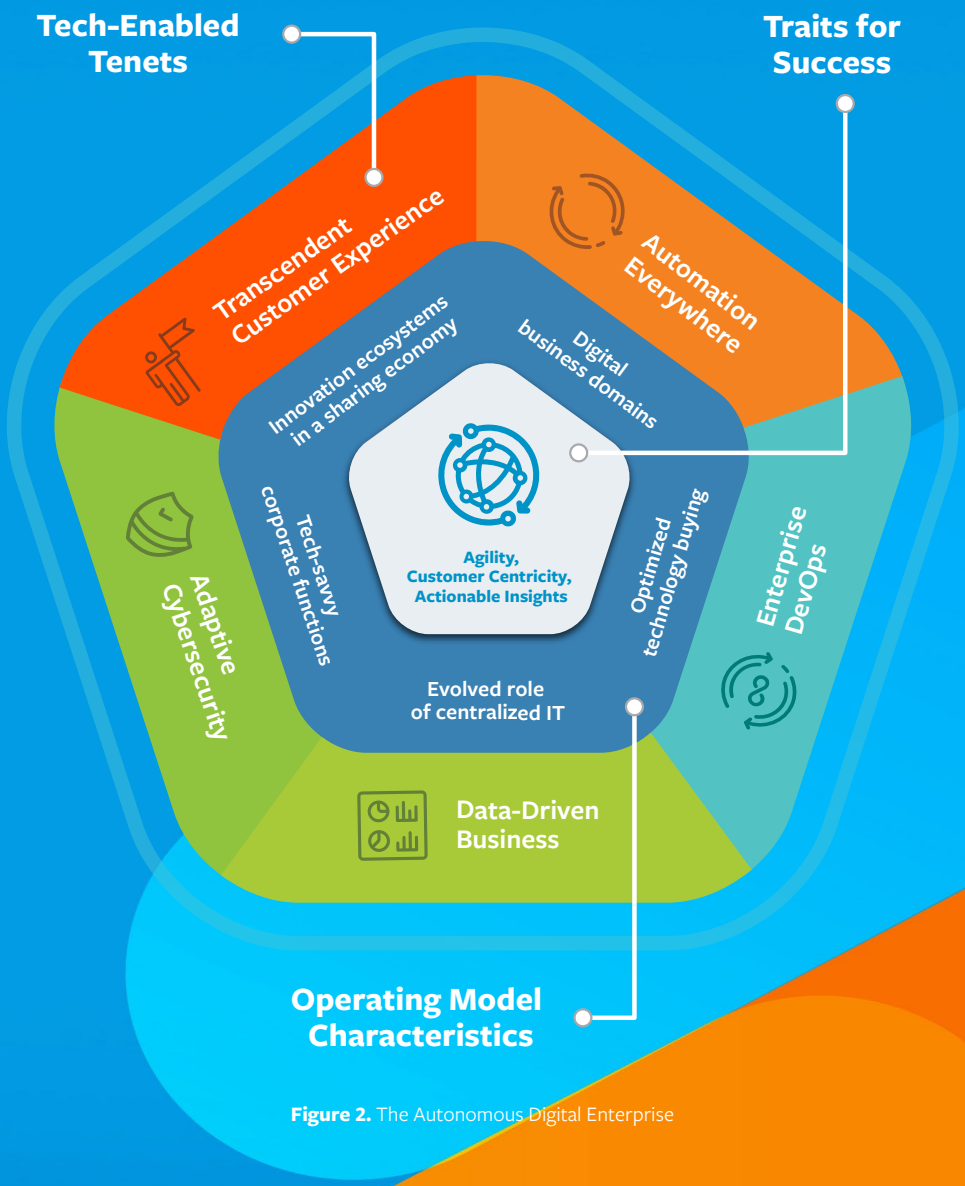


Figure 2. The Autonomous Digital Enterprise

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