5 WAYS TO BUILD A BETTER SECURITY POSTURE THROUGH ADAPTIVE CYBERSECURITY

With more of the world living and working online, securing all of that activity, and specifically the data, has become an even bigger business concern. In addition to the always-evolving and accelerating threat landscape, there are also regulatory and compliance requirements to factor in. Anticipating threats before they happen, and jumping quickly into action when they do, is integral to the digital transformation of every business, especially when IBM estimates in its *Cost of a Data Breach 2020 Report* that a single data breach can cost an impacted company $3.86 million.

That's the driving force behind Adaptive Cybersecurity, one of the tenets of the Autonomous Digital Enterprise (ADE), a framework that focuses on the future state of business as companies adopt emerging technologies and automation to survive and thrive in the face of persistent disruption. Adaptive Cybersecurity is the next 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.

How do you build a better security posture through Adaptive Cybersecurity? In our e-book, we explore five business use cases that bring the ADE tenet to life.

- **Automated Vulnerability Remediation:** Outdated, manual processes can jeopardize compliance and increase risk. By automating vulnerability scans, asset mapping, and remediation tasks and viewing all of them from a single dashboard, security teams can quickly address and close vulnerabilities, improve system security, and keep up with threats.

- **Blind Spot Identification:** Identifying blind spots is highly time-consuming—but important—work. It allows IT security departments to scan and automatically identify every server in the data center, augment scanner data with discovery information, and get a complete picture of vulnerabilities for remediation—before a breach occurs.
- **Regulatory Cloud Compliance:** Accelerated, increasingly complex cloud and hybrid innovations are driving higher demands for security and compliance. 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.
- **App-Centric Cloud Security:** The extensive implementation of containers, microservices, and agile methodologies has increased the speed at which Dev teams push updates to production, and the risk of exposure due to inconsistent security reviews. Help ensure consistent, secure configuration across the DevOps lifecycle with platform as a service (PaaS) and infrastructure as a service (IaaS) during the development, testing, and production phases and integrating them with the continuous integration/continuous delivery (CI/CD) pipeline.
- **Automated Detection, Response, and Reports on Mainframe Security Events:** The mainframe is more vulnerable that many realize, but it's also relatively easy to protect. Automated detection, response, and analysis tools enable real-time visibility into mainframe threat events as they happen, and sharing out insights in common English security terms empowers security analysts at every level to respond quickly.

Adopting an Adaptive Cybersecurity approach is just one tenet of the Autonomous Digital Enterprise. Companies that want to not only survive but thrive as their business—and the culture around it—evolves must include the latest security measures and enabling technologies in their planning.