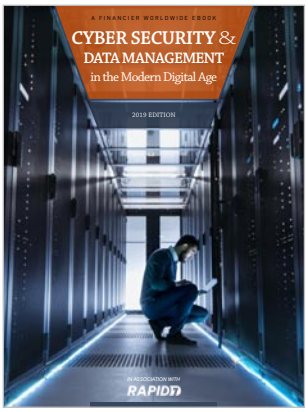


Published by Financier Worldwide Ltd

FOREWORD

Foreword by Todd Lefkowitz who is vice president of global services at Rapid7

FOREWORD

THE UBIQUITY OF DATA COMPROMISE continues to accelerate at an unprecedented pace. Headline after headline related to data breaches and nation-state attacks makes it hard for boardrooms to avoid the discussion. This, coupled with industries and geographies that now mandate more stringent security controls or breach disclosure, brings security relevance to new levels. For security practitioners, this is a welcomed evolution in both process and technology.

Emerging standards and guidelines like the European Union's General Data Privacy Regulation (GDPR), New York's Department of Financial Services Cyber Regulation (NYCRR), Australian Privacy Amendment (Notifiable Data Breaches) and California's Consumer Privacy Act are examples of regulation that are placing new security requirements on institutions that can have real financial repercussions. In the case of failing to disclose a data breach under the GDPR guidelines, the resulting fine can be upwards of 4 percent of revenues, which represents

a material impact.

Boards are interested in understanding how the effects of regulation impact business planning while solving for risk. There is a basic and foundational desire to ensure companies are doing what they can to protect not only their intellectual property and availability but also the privacy of their customers. This includes an understanding of the maturity of security programmes in place, and how this extends to vendors and partners, along with potential merger or acquisition targets. For others, it is cyber resilience for new internet-connected products to market.

The rise of cryptocurrency and ransomware-style attacks, with their devastating impact, have caused boards to question the integrity and maturity of security programmes currently in place. Checking a regulatory box is different than pursuing security best practice. Modern infrastructure is only getting more complex with the explosion of cloud computing.

In modern computing environments, any strategy now needs to include the cloud – whether private, public or hybrid. As more companies embrace their journey to the cloud or leverage software or infrastructure as a service, there is growing

confusion about what security processes exist and how they are implemented. While cloud providers embrace secure computing environments, the dependency lies with the operator to ensure configurations are established and managed correctly.

Cloud or not, is the business prepared and is there an appropriate business continuity or disaster recovery plan in place? While "not if, but when" has become cliché, it is still very much germane to how we think about security in the context of business. The board may not need, or care, to know the fine detail, but it should know a proven, actionable plan exists. The internet affords incredible business innovation, but we must be prepared to advance securely – and our boards' willingness to get involved is a major step forward.

■ *Todd Lefkowitz is vice president of global services at Rapid7.*

ABOUT RAPID7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics and automation delivered through our Insight cloud.

Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behaviour, investigate and shut down attacks, and automate routine tasks.

Over 7200 customers rely on Rapid7 technology, services and research to improve security outcomes and securely advance their organisations.

For more information, visit our website, check out our blog, or follow us on Twitter.

RAPID7

RAPID7

Advance Securely with the Rapid7 Insight Cloud

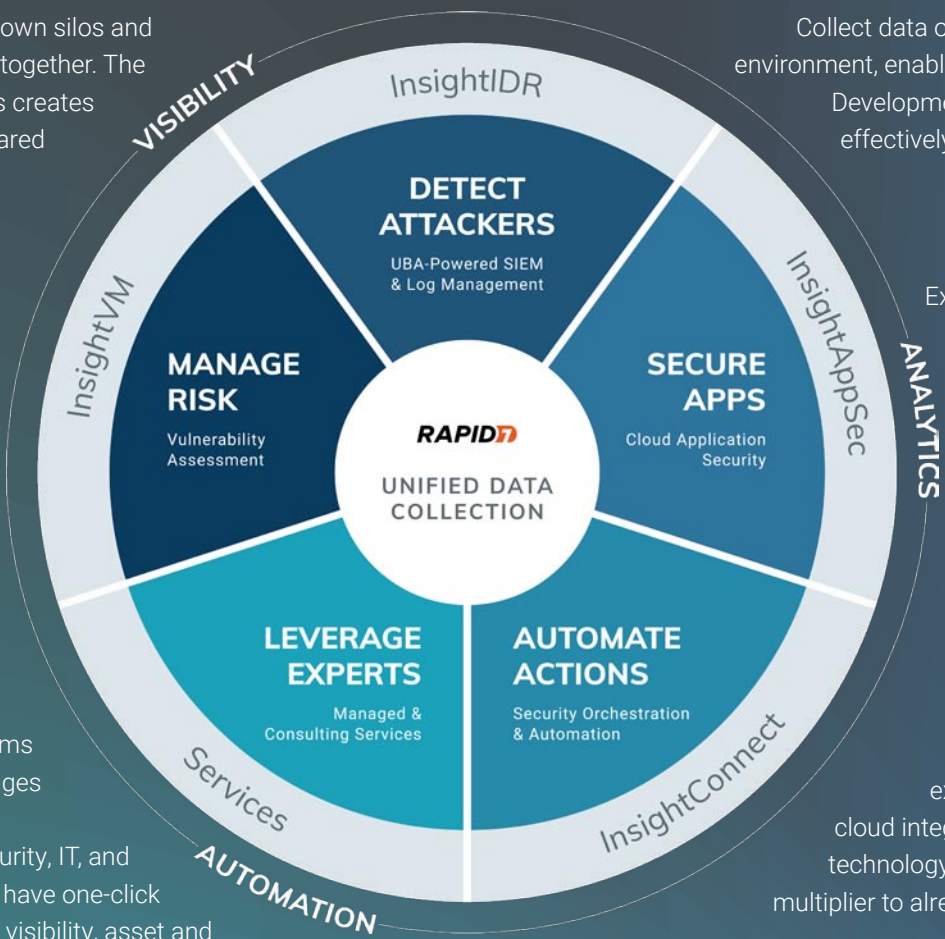
Reducing risk across your entire connected environment doesn't have to be complex. Try Rapid7 Insight for free at **www.rapid7.com/try/insight**.

Your Home for SecOps

It's time to break down silos and securely advance, together. The practice of SecOps creates an alliance and shared mission between Security, IT, and Development to make security an opportunity—not an obstacle.

How can you do it?

Rapid7 Insight is simplifying the complex through shared visibility, analytics, and automation that unite your teams around the challenges and successes of cybersecurity. Security, IT, and Development now have one-click access to network visibility, asset and application vulnerability management, threat detection and response, and orchestration and automation.



Unify Data Collection

Collect data once from across your IT environment, enabling your Security, IT, and Development teams to collaborate effectively as they analyze shared data.

Scale with Ease

Expanding your use of the Insight cloud to include multiple solutions is easy. Once your data collectors are installed, launching new Insight products is just a few clicks away

Integrate Seamlessly

Get faster analysis, prioritization, and remediation with your existing tools. The Insight cloud integrates with your existing technology stack, acting as a force multiplier to already-deployed solutions.

Ready to simplify your security?

Start your free Insight cloud trial at www.rapid7.com/try