RAPID7

WHITEPAPER

Financial Services Industry

| How the Rapid7 Insight Cloud Can Help

TABLE OF CONTENTS

Threats are growing, but not all threats are equal

Cyber-attacks are increasing in regularity and sophistication, with real consequences to organisations of all kinds. A report[1] from the Department of Digital, Culture, Media and Sport revealed almost half of UK businesses (46%) report having cyber security breaches or attacks in the last 12 months. The stakes get higher among medium businesses (68%), and large businesses (75%).

The financial services sector is one of the more prominent targets for such attacks, given its transformation maturity. Although driven in large part by the introduction of the EU's General Data Protection Regulation (GDPR), the financial services sector saw a 1,000% increase in the number of declared events in 2018. Yet, it's important to remember the vast majority of incidents are not related to threat actors, which only account for around 11% of attacks on the financial services industry. The vast majority arise from hardware or software issues. It's also important to note the compliance and regulatory standards, such as PCI compliance, that have been introduced into the industry as a result of the increased risk towards exposure.

As such, it's little wonder financial services is such a targeted sector when you consider the massive shift those organisations have made to digitally transform. They're driven by the desire for brilliant customer experiences through mobile applications for example, as well as creating efficiencies and driving business agility. This is augmented by the challenge of dealing with a global pandemic and an increasingly dispersed workforce. The strive to create an agile enterprise by placing more applications and workloads into what, for many, is a hybrid cloud environment, comes at a price—complexity. It needs to be managed accordingly, with any resulting security issues dealt with. Ideally, these will also be proactively planned for and mitigated.

However, there are measures financial services organisations can take to reduce risk that many aren't actively leveraging. Rapid7's own National/Industry/Cloud Exposure Report (NICER) 2020 found the top publicly traded companies of the United States, the United Kingdom, Australia, Germany, and Japan are hosting a surprisingly high number of unpatched services with known vulnerabilities. This happens especially in financial services, which has approximately 10,000 high-rated common vulnerabilities and exposure (CVEs) across their public-facing assets, despite their vast collective reservoirs of wealth and expertise. As such, this level of vulnerability exposure is unlikely to get better in a time of global recession.

That said, we understand. As far as security is concerned, we know you need to not only manage all of these factors, but also see time to value—fast. Above all, you have to ensure your security strategy supports your business transformation. And at the same time, manage and safeguard an increasingly complex network, applications, infrastructure, and user base from the rapidly increasing number of threats, both internal and external.

[1] Cyber **Security Breaches Survey 2020**

Statistics

64%

64%[2] OF UK ADULTS HAVE BEEN RELIANT ON TECHNOLOGY TO MANAGE THEIR FINANCES SINCE MARCH, UP FROM THE 42 PERCENT BEFORE THE LOCKDOWN.

[2] Yobota Survey

81%

WEB APPLICATIONS, MISCELLANEOUS ERRORS, AND EVERYTHING ELSE REPRESENT 81% OF BREACHES WITHIN FINANCIAL SERVICES AND INSURANCE ORGANISATIONS[3].

[3] Verizon 2020 data breach report

99%

ACCORDING TO GARTNER[4], BY 2023, 99% OF CLOUD SECURITY FAILURES WILL BE DUE TO CUSTOMER ERRORS.

[4] Neil MacDonald, "Innovation Insight for Cloud Security Posture Management," Gartner.com, January 25, 2019

Understanding your challenges

CISO

As the security leader in your organisation, you're a business partner to your C-Suite peers and you need to help the business evolve, securely. To achieve that, visibility is crucial to everything you do. You require a holistic view of everything that's going on to determine your risk levels, and beyond that, ensure you have the capabilities to deal with it, should anything untoward arise. We also appreciate your time and resources are limited. We understand the drastic shortage of people right now in the security sector, which means you need to use your limited resources to the best of your ability and focus on high-value tasks. Automation, too, plays a big part in meeting those needs.

How we help

- We help you detect and manage risks faster, remediate, and automate with the limited resources you have. This enables you to evolve your security posture in line with the outcomes your business wants to achieve.
- Data is key. We gather data from across the entirety of your environment and attribute events to the specific users and assets involved. This allows your team to quickly look throughout your entire environment for all evidence of a discovered compromise, allowing you to react quicker.
- Additionally, we help you adapt to evolving risks in line with the demands of your business so you can adjust your security posture accordingly. In the course of identifying attacker techniques, new behaviour detections are pushed out to automatically match against your data. This means you get the full context on affected users and assets, as well as threat intelligence around adversaries using these techniques.

DevSecOps

Transformation brings about exciting opportunities for innovation and development. As you know, however, building new applications, shifting workloads, and pursuing agility, speed to market, and scalability has to be tempered with security, risk, and compliance. Unless there's cooperation from the very beginning, security can very often be considered an afterthought, bolted onto the latter stages of the development cycle. Security must be embedded from the very start to ensure you're not playing catchup further down the track.

How we help

- We provide you with a simple, convenient, and collaborative way to embed application security testing into the SDLC.
- Our integrations with Jenkins, Azure DevOps, and Atlassian Bamboo facilitate automated scanning in a highly agile environment, where code changes occur frequently.
- We allow security to mature by "shifting left," and identifying code changes that may negatively impact your organisation's security posture.

Cloud Security

If your organisation is like the 87% of enterprises with a hybrid cloud strategy, you'll understand the increasing complexity it brings. As cloud promises to be further utilised[5] in response to the global pandemic, that complexity will only increase further.

While public clouds provide basic protections, they are mainly focused on securing overall computing environments. This can leave your workloads vulnerable. Because of this, deployed cloud environments are at risk of not only account compromises and data breaches, but also resource exploitation due to misconfigurations, lack of visibility, or user error.

How we help

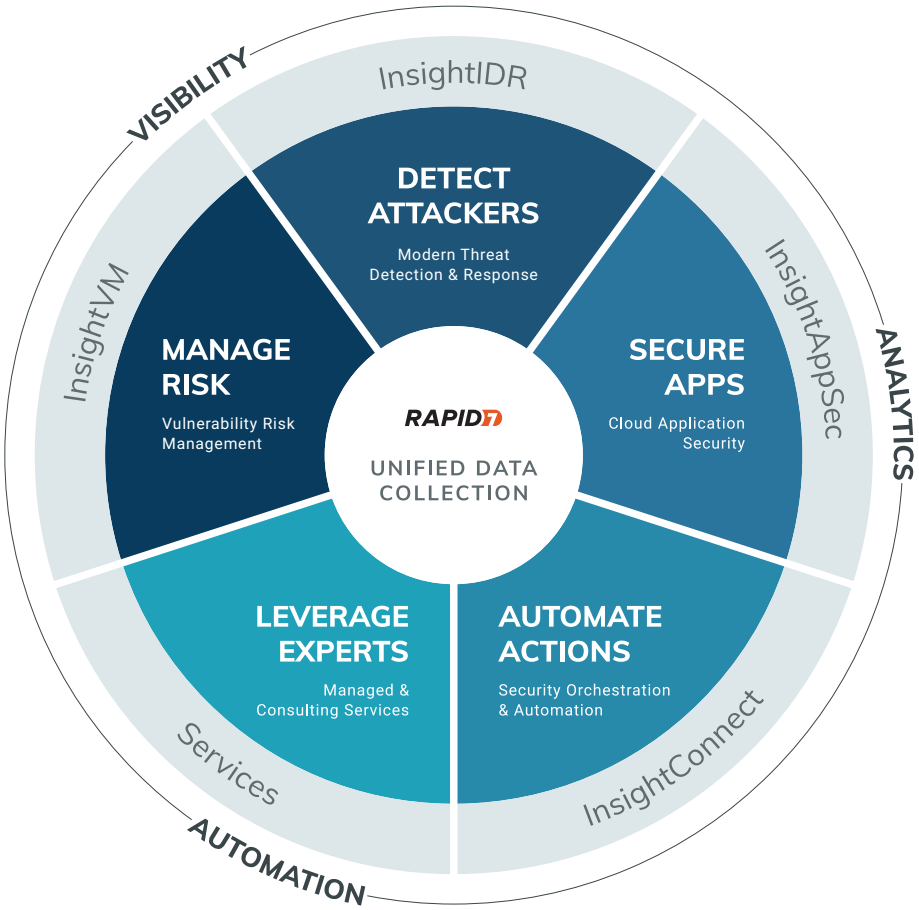
- We help you mitigate attacks by addressing software vulnerabilities and cloud misconfigurations, and utilising cloud identity access management governance strategies and best practices.
- Our highly experienced research and product teams have detailed views of the latest cloud threats, while our cloud-based DAST tool goes much further than the OWASP Top Ten to test for over 95 different attack types and best practices.
- After your developers have remediated for any identified vulnerabilities, Attack Replay gives them autonomy to immediately test their work, quickly close out tickets, and instantly reduce application security risk.

[5] MariaDB, COVID-19's Impact on Cloud Adoption

A holistic approach to your organisation's security

With high digital transformation maturity levels, financial services organisations have complex security requirements. This means considering a more unified approach than juggling simple point solutions.

Visibility is essential in your organisation, drawing in data from what you can see and capture from attacker detection and risk management. You then need the ability to act on that data quickly through advanced **analytics**, then **automate** security processes as part of the DevSecOps role that has become crucial in recent years. This creates the balance between transformative innovation and security.



How we help

The Rapid7 Insight cloud platform equips your organisation with the visibility, analytics, and automation you need to unite your teams, amplify your efficiency, and achieve time to value faster. Learn how our capabilities can help your organisation:

Take a complete approach to your threat detection and response with a cloud SIEM, so you can find and investigate earlier in the attack chain. Learn more here.

- Adapt to evolving threats
- Trip intruders with deception technology
- Find missing puzzle pieces with notable behaviours
- Detect and investigate endpoints in real time
- Determine the scope of cyber-attacks

Understand the vulnerability risk in your modern IT environment, collaborate more efficiently with technical teams, and communicate progress to leadership. Learn more here.

- Gain the visibility to understand and prioritize risk
- Remediate with impact and influence
- Measure and report on the progress that matters most
- Unify your endpoint assessment
- Maximize the value of your tech stack

Leverage leading dynamic application security testing (DAST) technology to mitigate application vulnerability risk and incorporate security into the SDLC. Learn more here.

- Crawl and attack your modern web applications to identify risk
- Empower your developers with Attack Replay and integrations with CI/CD tools
- Understand your compliance posture with pass/fail assessments against common benchmarks

Underpin your approach with security orchestration and automation. This enables your team to accelerate and streamline time-intensive processes, with no code necessary, freeing up time and resources to tackle other challenges and maximize expertise. Learn more here.

- Get more done and respond to security events faster than ever before
- Connect your different security tools and systems
- Gain time and productivity across your security operations

If you'd like to find out more about how Rapid7 can help your organisation, visit our website, or contact us via email.