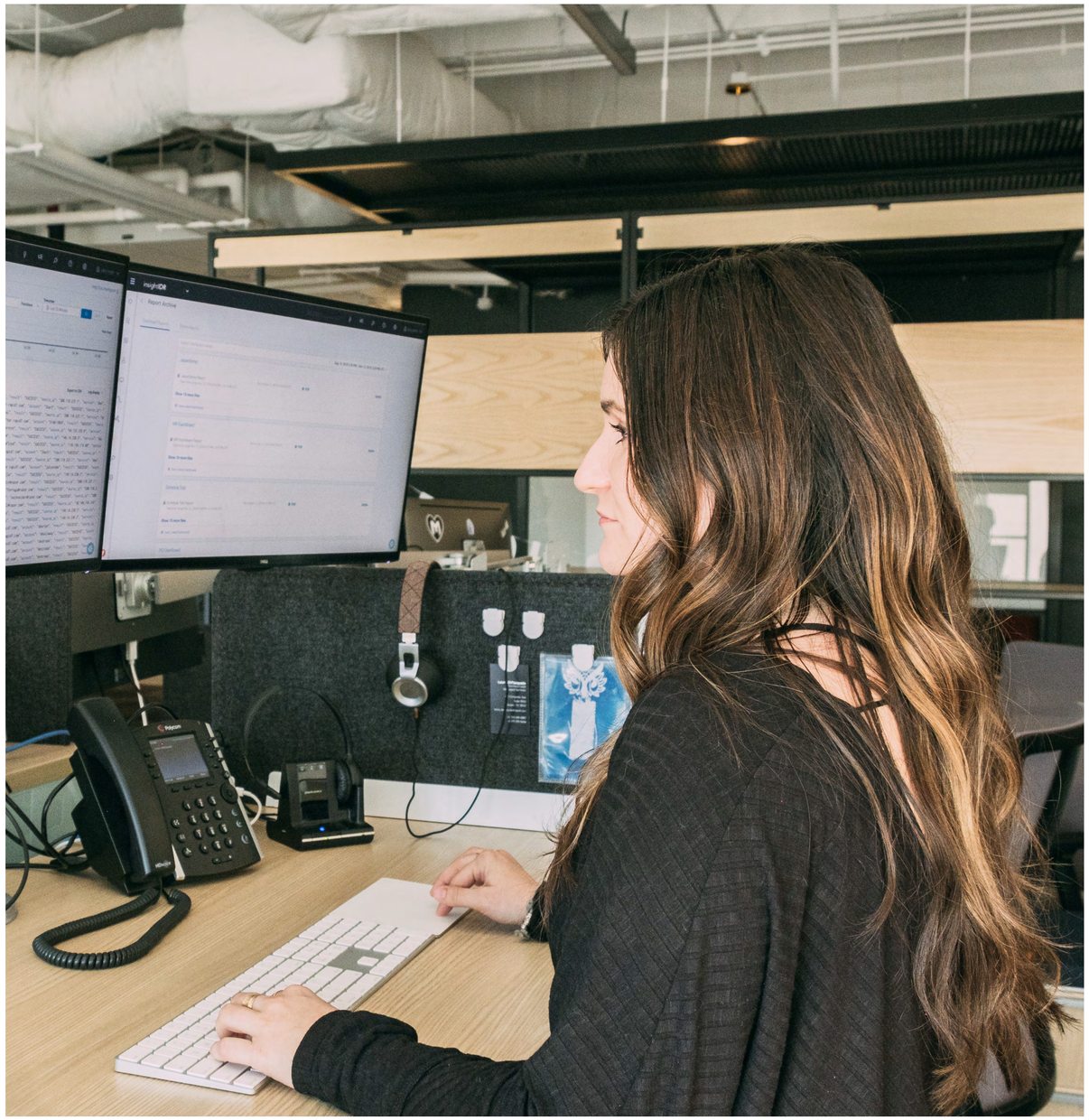
Top 5 Security Concerns in Financial Services

SOLVING THE MOST CRITICAL ISSUES IN THE MOST TARGETED INDUSTRY

Customer trust is the lifeblood of financial services. Guarding your customers' financial and personal data and assets, as well as your company's reputation, is a tremendous responsibility.

And here's the thing: As your organization and environment grow and become more complex, attackers continue to hone their skills. Every day, it gets easier for them to break in, and it's becoming harder and harder to respond to breaches quickly and decisively.



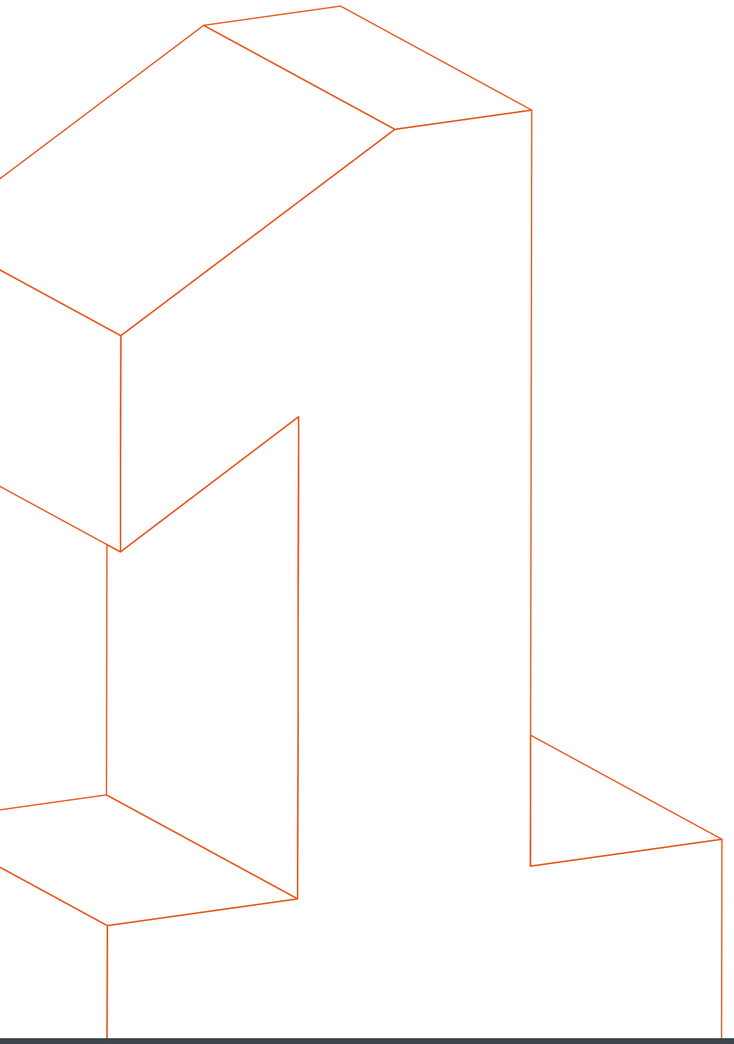
Your success hinges on better visibility into your risk exposure and blind spots, and the ability to detect and respond to threats as they arise.

At the same time, you have other concerns in your headlights, like what new exposures you're facing from digital transformation and moving to cloud. Are you covering all the bases in your work-from-home environment? Are there security risks in your critical web applications? Then there's compliance: Could you do it easier and better?

No matter the size of your security shop or the length of your project list, most finserv companies need the people, process, and technology to stay ahead of known and unknown threats. But who has the time to keep adding new detections, creating threat intelligence, or keeping on top of the latest vulnerability outbreaks?

We've created this guide to show you how financial services companies are partnering with research-informed security experts to successfully address their top five priorities:

01	02	03	04	05
Understanding risk across the attack surface	Securing web applications	Protecting cloud, hybrid, and container solutions	Complying with critical regulations	Finding an experienced security partner



PRIORITY #1

Understanding risk across the attack surface

As your organization continues to scale, move to the cloud, and develop web applications, your attack surface will continue to grow exponentially and create blind spots.

Progressive, forward-thinking financial services organizations need security partners who can help them scale and support their security programs across multiple disciplines.

Legacy solutions were not created to solve modern challenges like working from home or on the road. For this reason, many defenses are now useless, or cover only a small portion of their environment. With hackers inventing new attack vectors and tech all the time, it's tough to secure a laptop on open Wi-Fi provided by an ISP or cable company.

To sleep well at night, you need the answers to these three key questions:

01 Am I vulnerable?

02 Am I compromised?

03 Am I optimized?

Managing your attack surface means staying one step ahead of potential threats. Your resources are finite, so you need to focus on reducing the most amount of risk efficiently and effectively. With the right security partner, you can have the expertise, technology, and insight you need to stay ahead.

HOW RAPID7 RESPONDS

With Rapid7's Insight Platform and Managed SOC Services, you can advance securely with a trusted security partner.

PRIORITY #2

Securing web applications

Web apps are a security exposure in any company, but they continue to be a leading attack vector in financial services. Your web apps should be critical priorities, regardless of how new your organization is to the web or how much it relies on the web for revenue generation.

Websites, web applications, and online services are critical components of any organization these days. They are high-priority targets for attackers because they often contain vulnerabilities and can provide a wealth of sensitive data if exploited. Financial services organizations must be diligent to protect their web applications and services against attacks that can expose customer data.

Web applications and their associated APIs continue to be a target for malicious actors. Why?

01

Their complexity makes them hard to protect. And, because they're usually coded in new languages, legacy scanners struggle to spot vulnerabilities. This makes them the perfect attack vector.

02

It's difficult to use a dynamic application security testing (DAST) tool on them. Not being able to run real-life external security tests against them makes them a bit of an enigma.

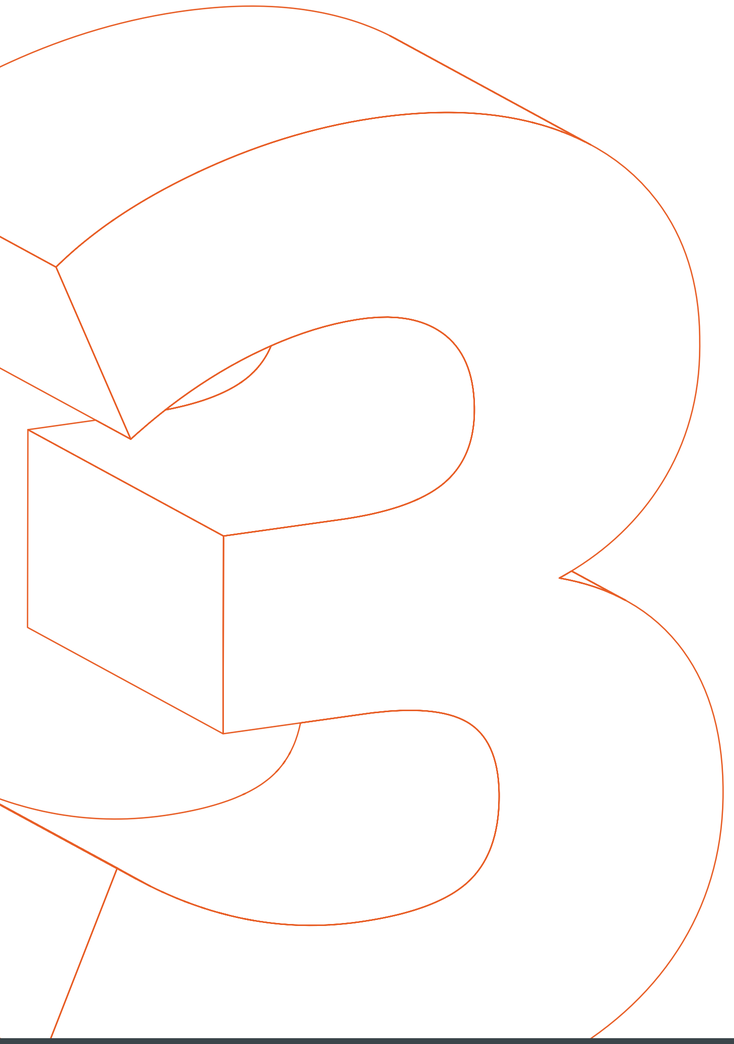
03

They offer high rewards with minimal effort. Hackers can automate their attacks, potentially hitting hundreds of thousands of targets at once and making off with a lot of valuable personal data.

Don't let web applications be a security blind spot. Security experts can help you get visibility into their risks and vulnerabilities, no matter how complex or custom the web app.

HOW RAPID7 RESPONDS

Rapid7 helps you better assess, monitor, and protect against application-based attacks through robust appsec vulnerability management, threat defense, and monitoring and detection. Through runtime application self-protection (RASP) and web application monitoring, you'll be able to enhance your web application security at every level—from browser to server—to identify and block attacks.



PRIORITY #3

Protecting cloud, hybrid, and container solutions

Is digital transformation still on the horizon, or in your rearview mirror? For most, this has meant moving at least part of your system and data to the cloud and, more recently, containerizing application development for reasons of security, cost, and scale.

Global companies providing cloud and containerized systems like Amazon or Azure offer security beyond what most companies can achieve. But in the real world, most organizations have a hybrid solution of cloud or multi-cloud plus on-premises systems.

It's the complexity of that combination that's the rub, and the challenge to cloud security. Is your security story solid for the whole attack surface?

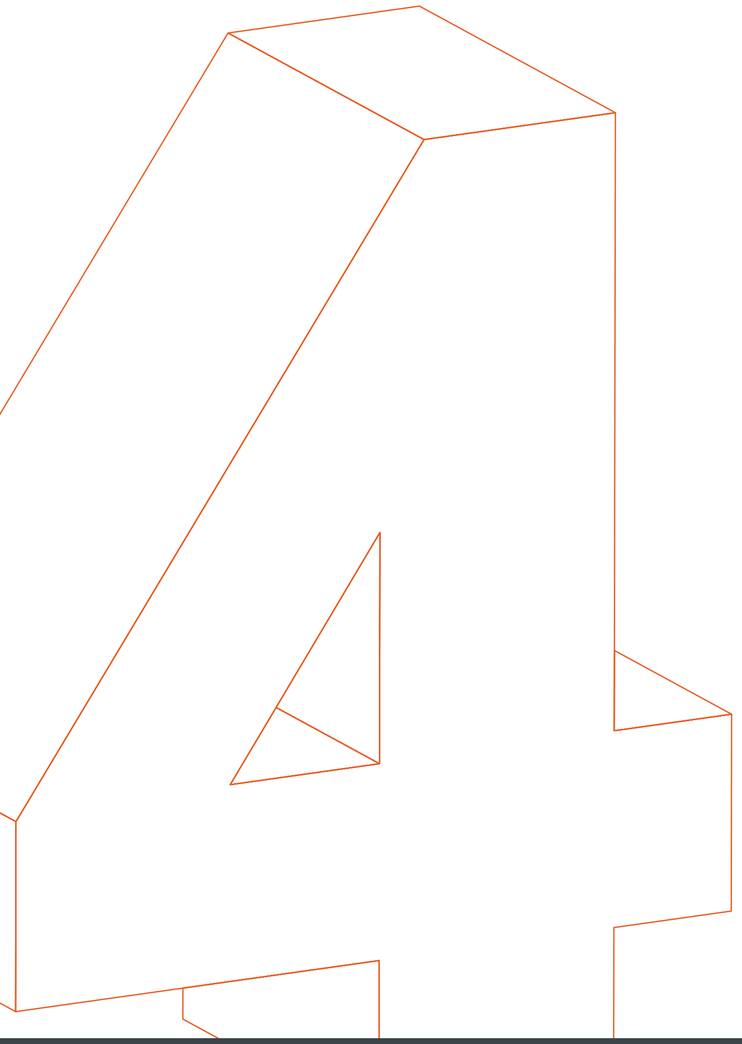
Having a partner that understands cloud security and hybrid solutions is essential. It's critical to be able to constantly monitor and detect vulnerabilities and misconfigurations in cloud networks:

- Finding and checking assets like virtual machines and containers as they are spun up
- Verifying compliance with policies and regulations
- Calculating risk scores to help you prioritize your efforts

Detecting threats in these complex environments can also be tough. A SIEM that can collect and analyze data from on-premises networks, remote endpoints, and cloud platforms will let you break down security information silos and use advanced analytics to respond to incidents.

HOW RAPID7 RESPONDS

Rapid7 can provide security and visibility to even the most complex of environments. Our cloud security solution has become a global leader through development and acquisition of world-class companies, including strong partnerships with AWS, Azure, GCP, and other major cloud providers.



PRIORITY #4

Complying with critical regulations

Financial services providers have to provide clear visibility into compliance with important regulations, and for good reason: You store so much sensitive data that any sort of leak would impair brand trust well into the future.

Regulatory frameworks ensure you have that clear insight into your posture for each control. But could you do it all easier and better as you face down that compliance deadline?

While it's easy to be daunted by the multiple frameworks most financial services companies must conform to, the good news is that most frameworks are spinoffs of basic regulations like CIS, NIST, FFIEC, and GLBA. And what most frameworks are testing is your basic security hygiene.

Common to all frameworks are excellent security practices. To start with, plan your security approach, understand risk, build your roadmap, invest in preventative solutions like firewalls, antivirus, and vulnerability management, and carry out pen testing. To round it out, centralize your security logs and data, and continue to analyze it so you can detect anomalous behaviours and respond to incidents in a timely way.

Yes, it's a lot of work, but take it step by step, because solid security practices line you up perfectly for compliance.

HOW RAPID7 RESPONDS

We treat your security like it's our own, helping your organization grow as we help protect your most valuable assets. If you don't have the people, process, and technology in place to handle compliance without stress, Rapid7 can guide you. Our focus on robust cloud security solutions supports compliance with multiple frameworks.

Rapid7 improves one bank's compliance. Even the auditors are impressed.

> Every year we prepared for our annual state audit, but I don't think we did it well. I'm not even sure we knew what good looked like. So we engaged Rapid7 to improve our security and help us comply with government regulations. Even the out-of-the-box Rapid7 reports helped us answer the audit questions faster and more directly than before."

> When the state came in to evaluate us, they got responses they'd never seen before. Not just: "*Yes, we're doing vulnerability scanning,*" but, "*This is how we prioritize our remediation efforts.*" The auditors were so impressed with the solution that they recommended Rapid7 to the state for their security systems."

PRIORITY #5

Looking for an experienced security partner

Most security shops are great at taking care of day-to-day in-house security needs. But it's tough to run the show while also diving headfirst into the minds of hackers and their latest schemes. It's a specialty that demands constant research, vigilance and a view of cybersecurity across industries, continents, and time.

Many organizations have weighed the cost and effort of taking on these specialty skills internally and decided to engage experts for support. But it's important to find the right partner that understands the risks in financial services and can meet your organization's unique needs.

What qualities should you look for? Your security partner should be:

01 An industry leader in critical solutions like vulnerability management, SIEM, and appsec

02 An active contributor to the security community and up-to-date on the latest threats

03 Involved in research to constantly uncover new attack vectors

04 As passionate about security as you are

HOW RAPID7 RESPONDS

Rapid7 is obsessed with growing, learning, and sharing our experience and industry-leading research to help our customers stay secure.

- We use the findings from more than 1,000 penetration tests every year to help customers.
- We are leaders in vulnerability exposure to help find where you could be exploited.
- We run the 200,000-strong Metasploit community, which powers global security research.
- Metasploit contributors actively add to new types of attacker tools and vulnerabilities.
- We share new threats and better detection techniques with all customers.
- Our SOC solution monitors companies, endpoints, and users around the world.
- We belong to threat intelligence communities like the Cyber Threat Alliance.
- We're plugged into known threats, and hyper-focused on detecting unknown threats.

SECURE BY NATURE

Your ability to protect customer data and resources is critical to your success. To keep ahead of both known and unknown threats, most Finserv companies partner with experts who can integrate with their systems and teams.

Sometimes, this partnership covers a single project to reduce risk, safeguard applications, contain breaches, comply with regulations, or securely modernize their infrastructure. And sometimes, it's to take the lead on all of this critical and cutting-edge work.

Rapid7 innovates through research and analysis of the attacker mindset. Our experience with 9,100 organizations across the world, including over half of the Fortune 1000, helps us look across industries and regions to get a clear and comprehensive global understanding of risk.

Our complete range of security software and services works together to clarify your security strengths and exposures, from users to devices, while letting you dive into more and more granular layers of detail.

Our goal: to give you that inherently secure foundation on which to build customer trust.

Read more at www.rapid7.com