Incident Detection and Response With Rapid7 & Compuquip

compuquip

More than ever, cybersecurity is taking center stage as an essential part of an organization's protection. As cybercriminals find new and innovative ways to exploit vulnerabilities – whether from the gaps found in a remote work environment or outdated infrastructure – organizations need complete data security solutions they can trust to keep them safe and successful.

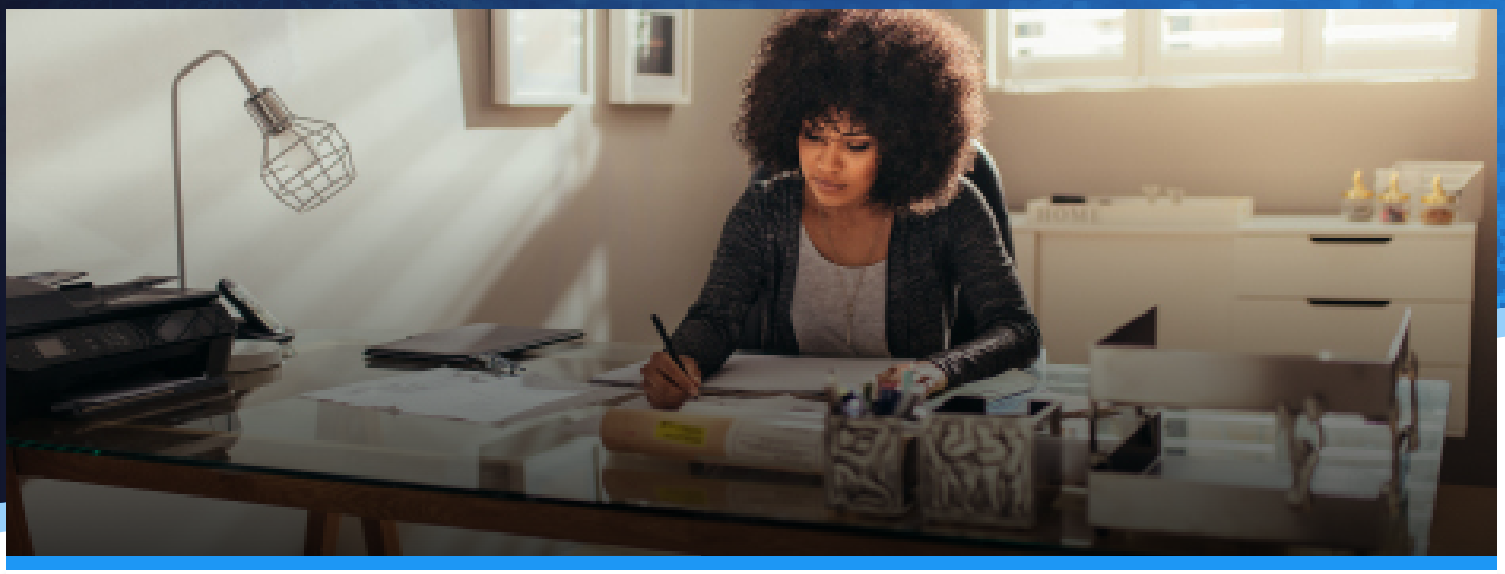
But, with cybersecurity attacks being expected to occur every 11 seconds in 2021, how do you separate the noise from the real threats? Luckily, you don't have to look too far to find your answer. The Rapid7 platform, an all-in-one solution for risk management, can help mitigate risk across your entire connected environment so your company can focus on what matters most!

A leading cybersecurity solutions provider, Rapid7 is on a mission to make security tools and practices accessible to all - and we'd say they've been pretty successful seeing as Rapid7 is trusted by over 9,000+ clients in over 140 countries.

With unrivaled cybersecurity risk management services, Rapid7 can take your threat detection into the new decade – which is why Compuquip is proud to offer Rapid7's managed solutions

This guide is part 2 of 3 about Rapid7's central platform and features the Incident Detection & Response services. Continue to learn more about how Rapid7's data security solutions can provide your organization with the threat detection and risk management services you need to be successful in the 21st century.

> *The Rapid7 platform, an all-in-one solution for risk management, can help mitigate risk across your entire connected environment so your company can focus on what matters most!*



Why Having a Strong Incident Detection and Response Strategy in Place is Essential in Today's Current Business Landscape

Even before the COVID-19 pandemic, cybersecurity risk management solutions have had to adapt quickly to a rapidly changing IT environment. As cybercriminals evolved, by the end of the decade, the cybersecurity threat environment was already progressing dramatically. From a combination of ransomware and other malicious attacks, an estimated two million cyberattacks in 2018 resulted in more than $45 billion in losses alone.

However, the 2020 COVID-19 pandemic, and the ensuing shift to a remote workforce, has resulted in accelerated cyber attacks.

Working remotely poses additional security risks that place remote organizations in vulnerable positions to be taken advantage of by cybercriminals. For instance, hackers may have more access to home internet traffic as compared to an office. Whereas an office environment may have enhanced security on all Wi-Fi networks, a remote employee's home network likely has weaker protocols that can be compromised.

> *The FBI reported that the number of complaints about cyberattacks to their Cyber Division reached as many as 4,000 a day – a 4,000% increase from before the pandemic.*

These vulnerabilities haven't been missed by criminals, either. The FBI reported that the number of complaints about cyberattacks to their Cyber Division reached as many as 4,000 a day – a 4,000% increase from before the pandemic.

The prevalence of cyberattacks is unlikely to go away anytime soon as remote working will continue to be the norm for many in 2021 and beyond.

New data suggests that the total cost of ransomware attacks will top $20 billion globally in 2021 and that a new business will fall victim to a ransomware attack every 11 seconds. This number is down from the 2019 estimate of 25 seconds, which means attacks are becoming more frequent and more sophisticated.

Security breaches can have devastating results on businesses' daily operations, financial bottom line, and reputation that lead to lasting financial consequences. Most small-to-medium businesses are unable to recuperate after devastating attacks. Over 40% of cyberattacks target small businesses, costing them an average of $2.2 million a year. Most never recover; 60% of small businesses that experienced cyberattacks go out of business within six months.

Despite these estimates, a 2019 report found that only 14% are prepared to defend themselves in the case of a disruption. Many business leaders and IT management professionals typically don't have the time in their schedules to focus extensively on day-to-day data security operations.

> *New data suggests that the total cost of ransomware attacks will top $20 billion globally in 2021 and that a new business will fall victim to a ransomware attack every 11 seconds.*

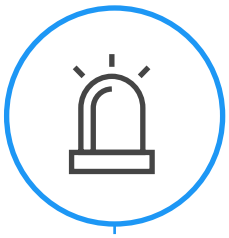
With both the financial security and future of your business on the line, it's critical for organizations of all sizes to have the right cybersecurity risk management solutions in place to monitor suspicious network activity. With Rapid7's Incident Detection & Response technology, businesses can proactively prevent data breaches and malicious attackers before an incident has negatively affected them and their customers.

How Does Rapid7's Incident Detection and Response Solutions Catch Potential Threats?

With so many threats to network security, your organization needs the most comprehensive incident response system available to detect malicious activity before it attacks your system! For comprehensive network visibility and accelerated threat investigation and response, look no further than Rapid7's Incident Detection and Response Solutions.

As part of the Rapid7 risk management platform, the Incident Detection and Response solution is designed to enable organizations to rapidly detect and respond to cybersecurity incidents and breaches across physical, virtual, and cloud assets. Equipped with user behavior analytics (UBA), attacker behavior analytics (ABA), endpoint detection and response (EDR), and deception technology, this managed solution delivers an entirely comprehensive picture of data security - correlating users and assets and giving businesses the visibility needed with speed and efficiency.

As a comprehensive incident detection solution, Rapid7's Incident Detection and Response solutions:



Reduce alert fatigue by delivering more refined results than other incident detection solutions. Constant influxes of data mean lots of "noise" that internal IT teams must sift through to find the real threats. This platform sorts through it all to focus on the legitimate disruptions, meaning your internal IT teams can focus on attaining real results.

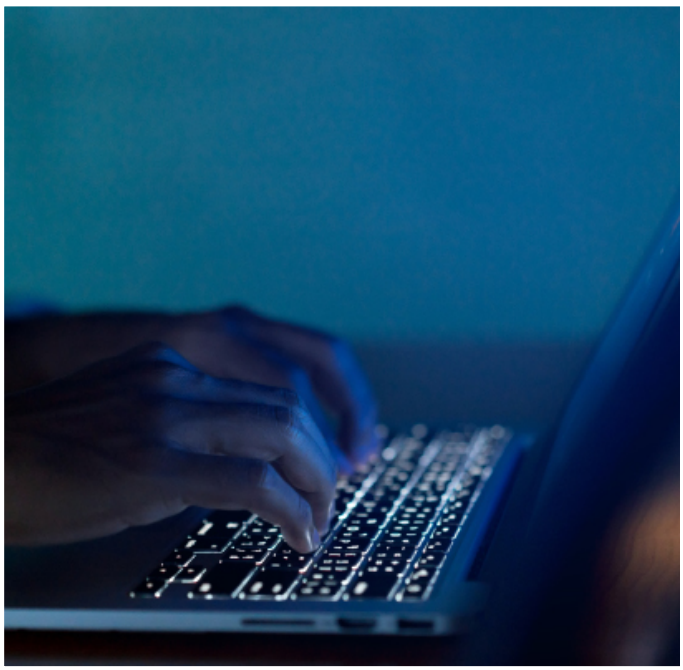
Provide visibility and control across all phases, with actionable data to respond accordingly to an attack. This includes pushing alerts and investigations to give you a faster response time. This combination of refined results and unmatched speed helps to proactively identify threats, meaning internal IT teams can respond quicker and better thwart the spread of threats.

Prevents internal IT teams from wasting time on minimal-risk threats, enabling them to only focus on real threats. This reduces distracting alert fatigue and frees up time to focus on meeting business objectives and achieving goals.

By reducing alert fatigue and sharpening the skill of IT teams, this incident response solution can prevent malicious attacks before they occur. This doesn't just make life easier for your IT team—it creates long-term cost-savings by minimizing risks of data breaches and the costs associated with them, including negative brand reputation, lost consumer trust, and downtime that leads to lost revenue.

What Are Some Tools That Rapid7's Incident Detection & Response Platform Utilizes?

For comprehensive threat detection, the Rapid7 Incident Detection platform utilizes a variety of tools: User Behavior Analytics (UBA), Attacker Behavior Analytics (ABA), Endpoint Detection and Response (EDR), deception technology, and automated workflows. All of these tools are included within the Rapid7 platform to provide the most thorough incident detection solutions.



Automated Workflows

Basic, commonly used workflows are already automated within the platform for fast deployments, such as disabling suspicious accounts and quarantining users with unusual activity. Each Rapid7 solution contains a workflow library so users can choose what automated workflows are the best fit for their organization.

Customers can also build customized workflows within the platform. For example, you can automate responses to disable assets or accounts if there appears to be malicious activity, such as immediately locking suspicious accounts until a further investigation can be conducted.

Attacker Behavior Analytics (ABA)

The ABA tool is programmed to recognize specific tactics and techniques that hackers use so malicious patterns can be quickly identified. Automating this process means that threats can be detected faster as opposed to a member of your IT team having to manually handle these processes!

However, we all know that hackers are continuously changing their techniques to get past the latest security features. No need to worry—as a smart system, the Rapid7 platform will catalog unique attacker behaviors over time and continuously be analyzing data in order to learn and adapt to the latest techniques. Rapid7 evolves with the changing landscape of security; even as hacking techniques evolve and change, the Rapid7 platform evolves and changes as well.

Deception Technology

The Rapid7 Incident Detection platform is installed with deception technology to lure in hackers to dummy systems, deterring them from attacking your real system and exposing them as a threat instead.

As a honeypot concept, the dummy system is designed to interest and deceive a malicious attacker. Once the attackers take the bait, the deception technology fires off an automated investigation workflow to disable them. This tool allows your organization to not only be on the defensive against potential attacks in progress, but be on the offensive when it comes to protection.

User Behavior Analytics (UBA)

Another smart tool, User Behavior Analytics recognizes usual user behavior, such as user time zones and login habits, and detects irregularities that indicate malicious activity. Let's look at a few example situations:

- The platform recognizes that a user who typically logs in to work from Tampa, Florida, is currently logging in from Europe. If the system detects the user working from a different place and time zone, the account will be flagged for suspicious behavior. It will then automatically send an alert and create an investigation for the internal IT team to analyze. The IT team gets the alert, checks the employee's work calendar, and sees that they are on a business trip meeting with a client in Europe. After some investigation, it's clear this is the intended user logging in, and the account is unflagged.

- The platform recognizes that a user logged in from Tampa, Florida at 9:00 AM ET, then the same account logs in again at 10:00 AM ET from Asia. The Rapid7 platform is also programmed to detect impossibilities, and it is clearly not possible for the same person to login from across the world just one hour later. So, the system immediately locks this account and sends an alert for the IT team to investigate further.

All of the platform's incident detection tools can also be automated to produce quick and efficient results that provide comprehensive network visibility and accelerate threat investigation and response. With these smart tools that are constantly evolving to meet the changing security landscape, you can put your confidence in the Rapid7 platform to be the watchdog of your organization into the new decade.

How Does Rapid7 Powered by Compuquip Accelerate Incident Detection and Response Over the Competition?

Rapid7's InsightIDR tool makes it possible to efficiently sift through data so your business can identify and respond to real threats faster. This agile and adaptable SIEM uses machine learning to continuously level up your capabilities as you grow into the platform—if its features are used to their fullest potential. But with so many features and capabilities, it can become difficult for your internal team to maximize InsightIDR's full functionality. The good news? With Compuquip as your cybersecurity partner, you don't have to worry about mastering all the ins and outs of Rapid7 completely on your own.

Compuquip is an InsightVM Certified Specialist, meaning our team of experts have completed extensive hands-on training directly from a Rapid7 Security Consultant and passed the certification exam. Gain peace of mind knowing your business security is in the hands of true masters of the Rapid7 platform!

> *"This unprecedented shift towards a remote work environment caught many organizations off-guard when it came to their cybersecurity—and cybercriminals certainly didn't waste any time capitalizing on those vulnerabilities."*

What Makes Rapid7 Incident Detection Essential for Remote Workforce Security?

Having peace of mind about your network security is more essential than ever with the rapid shift to remote work due to the COVID-19 pandemic. This sudden shift to remote work has increased vital business systems' exposure to malicious attackers.

Prior to the COVID-pandemic, only 7% of the American workforce had the option of remote work. Currently, that number has jumped to 66% of all employees that are participating in a work-from-home situation, whether partially or entirely. This unprecedented shift towards a remote work environment caught many organizations off-guard when it came to their cybersecurity—and cybercriminals certainly didn't waste any time capitalizing on those vulnerabilities.

Since the start of the pandemic, the FBI has witnessed a 400% increase in reports of cyberattacks, with increasingly more amounts of ransomware targeting small-to-medium businesses. A recent Tanium survey found that 90% of participating CXOs reported a 90% increase of cybersecurity attacks while working remotely, with 98% of them reporting security issues spikes within just the first two months of the pandemic.

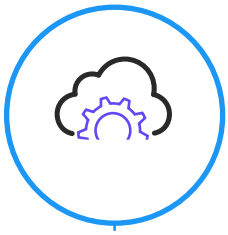
> *The FBI has witnessed a 400% increase in reports of cyberattacks, with increasingly more amounts of ransomware targeting small-to-medium businesses.*

The dramatic increase in cyberattacks can be attributed to the precarious position of many remote work employees. Virtual private networks, or VPNs, are relied on by many businesses as critical infrastructure, but many home networks are compromised or infected with malware that can easily be exploited by hackers. Much of the security systems in place at an office are unable to be extended into every employee's home network, leaving them relying on their easily accessible home Wi-Fi network systems on unreliable public networks at coffee shops or co-working spaces.

Instead of sitting back allowing the shift to a remote work environment to become a catalyst for cyberattacks, make the proactive decision to keep your business safe with incident detection software for the remote workforce. With the Rapid7 Incident Detection and Response platform, your organization can be equipped with the next-level threat detection you need for security and success.

Increased Visibility

No matter where your employees are working from, the Rapid7 platform provides visibility into user behaviors at the endpoint level so your organization has the eyes it needs to detect threats before they attack.



Secure Data

Data is encrypted through Rapid7, sent through the cloud, AND accessible 24/7, 365. The platform can even secure and encrypt your employee's data, no matter what location or device they're working from.

Reduce Fatigue

The Incident Detection platform is designed to empower your internal IT team and free up their time for more important tasks by eliminating minimal-risk threats that are distracting and cause "alert fatigue."

With the comprehensive network visibility and accelerated threat detection and investigation with Rapid7, you can have peace of mind through these turbulent times when you should be focusing on your business needs and goals – not your security.

Why Managing Rapid7 Through Compuquip Can Add Additional Value for Your Business!

By leveraging Rapid7's Incident Detection and Response through Compuquip, your organization can reap a host of benefits! Besides the numerous awards and recognition that the Rapid7 platform has earned, Compuquip has chosen to partner with the managed risk platform due to its powerful solutions for helping organizations of all sizes, regardless of their industry, manage their vulnerabilities through these unpredictable times and beyond.

So, why choose Compuquip to be your Rapid7 partner?

Certified & Experienced

Compuquip is no stranger to working with incident detection and response; we've helped both large enterprises and small businesses deploy and manage solutions since 1980! Plus, our cybersecurity team has years of experience working with Rapid7 products and services specifically. In fact, we are one of only three Rapid7 partners in the United States with exclusive Professional Services rights for projects from Rapid7 and a Rapid7 Gold Partner, which means Compuquip has certified and trained engineers on the platform with the expertise to help customers.

Competitive Pricing

Due to our Rapid7 Gold Partner membership, Compuquip can offer the Rapid7 suite at a competitive price and provide enhanced management services. In fact, Compuquip's price is more competitive than Rapid7's managed solution! Since the implementation of Rapid7's managed solution is our primary focus, Compuquip can focus on your needs as a customer so you can receive the most out of the platform.

Expert Industry Knowledge

Partnering with Compuquip gives you unique, valuable access to the expertise of industry experts. The team at Compuquip bring their expertise to help you not only leverage the Rapid7 platform, but also to unpack the data gathered from these solutions so you can make more informed decisions and realize a greater ROI.

What Other Services Does Compuquip Provide to Enhance the Benefits of The Incident Detection and Response

By choosing Compuquip as your Rapid7 platform partner you receive way more than just the Incident Detection and Response solution itself - you also receive the ongoing support and management services you need to fully realize the platform's potential for supercharging your security impact!

A Co-Managed Solution for Increased Security

The Incident Detection platform is a co-managed solution, so both the user and Compuquip's team will receive any initial alerts and investigations. By putting our heads together, we collaborate together to find the best-fit solution for your unique needs. When a valid security issue is detected, you can choose to fix the issue with your own internal IT team or can use Compuquip's experienced experts. No matter the security threat, Compuquip is there to help you through it along every step of the way!

Additionally, Compuquip offers a variety of services and provides training and support from our team of certified Rapid7 experts.

Continuous Support & Assistance

Compuquip assists your organization throughout its entire experience of Rapid7. By leveraging the platform through Compuquip, our team manages everything from start to finish – from configuration to management to added value to offboarding.

Custom Training

Our certified Rapid7 experts conduct custom training sessions for customers on everything from products, new features, how to utilize Rapid7 – or anything cybersecurity-related in general! Compuquip is with you from start to finish offering guidance throughout your entire Rapid7 journey.

With the unrivaled threat detection of Rapid7 and co-managing support of Compuquip's industry experts, your organization can experience the visibility and expert guidance you need to drive your security forward in unprecedented times.

In a world with increasingly more sophisticated security threats, detecting threats before they occur is essential for success. With Compuquip and Rapid7, you can cut the noise to focus on the threats that matter.

This guide is part two of three in a series about the Rapid7 cybersecurity risk management platform. Check out our next guide for an in-depth understanding of Rapid7's Application Security solutions. For more information about Rapid7, check out our blogs below:

- Why Compuquip is Your Florida Rapid7 Partner
- Empowering Cybersecurity Through Rapid7 & Compuquip

Or, feel free to reach out to the Compuquip team with any additional questions you may have! Our experts would be happy to answer any questions you may have about managing the Rapid7 platform through Compuquip or any of our other data security services.

About Compuquip

Since 1980, Compuquip has operated as a family-owned advanced technology solutions partner for businesses throughout Florida and beyond. We have grown into a trusted provider of cybersecurity products and services that help our enterprise partners address their network infrastructure and security architecture needs in an ever-changing security landscape.

With a full-in house team of qualified and experienced cybersecurity engineers, solution architects, and IT specialists, Compuquip has everything Florida businesses of any size, in any industry, need to efficiently mitigate and manage cybersecurity risks.

Email: info@compuquip.com

Phone: 789-641-5437

Address: 2121 Ponce De Leon Blvd. Suite 530

Coral Gables, FL 33134

Follow us on: