Are you Compliant or Secure?

A Financial Services Guide to Cybersecurity

CRITICALSTART®
They're good. We're better.

What is compliance?

Whether it's Payment Card Industry (PCI) compliance or meeting DFS Standards, compliance boils down to a regulatory framework to raise the bar on cybersecurity. But when financial services organizations comply with these standards, are they merely checking boxes, or are they making the investment and effort to actually be more secure?

Compliance should always be the byproduct of a strong cybersecurity program—not the other way around. Meeting standards doesn't necessarily equal effective security, but a comprehensive framework for security alignments can achieve standards while actually protecting a business from harm.

238%

increase in cyberattacks targeting financial institutions in 2020.

$5.72

The average cost of a data breach in the financial sector in 2021 was $5.72 million.

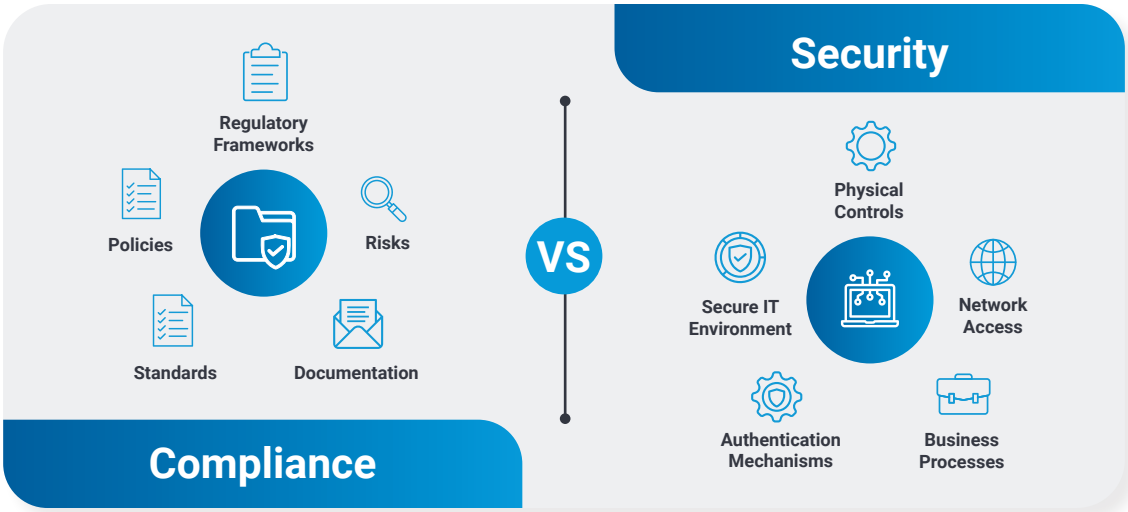
The first half of 2020 saw a **238% increase in cyberattacks** targeting financial institutions, and **the average cost of a data breach in the financial sector in 2021 was $5.72 million.** Consider this your guide to preventing such an attack on your own organization. You'll learn the steps necessary to deploy an effective cybersecurity platform that moves from checking boxes to stopping attacks. You'll learn the importance of integrating MDR into this platform and you'll discover how to evaluate your security partners to ensure you're getting the comprehensive and dynamic approach to cyberprotection that you deserve.

Compliance Versus Security: How to Unify Your Security Posture Under a Comprehensive Banner of Protection

Let's be clear: It's important that your cyberprotection is compliant with industry standards. Radius Financial Group recently had the private data of 16,000 customers accessed when they fell short of PCI DSS standards. But being compliant only takes an organization part of the way on their cybersecurity journey.

Effective cybersecurity is an all or nothing game where the companies that make the full effort have a real security-in-depth strategy, while the ones that put a partially effective program in place are the ones that cyberattackers will target when they discover vulnerabilities. After all, it's easier to go after the low-hanging fruit than attempting to penetrate a business that has their potential points of entry locked down and a response plan in place to prevent a breach from being able to move throughout their system.

When done properly, the difference between a compliant organization and one that's truly secure can be striking:



What are the 18 CIS Security Controls?

There are 18 critical security controls that every financial services organization needs to deploy at a minimum to protect against sensitive data breaches. A company that's compliant might have 12 of these controls in place in order to maintain that compliance.
But this is not a game of horseshoes. Close isn't good enough.

A secure organization needs to have all 18 critical security controls in place—no exceptions. Known as the 18 CIS Critical Security Controls, these controls include:

1. Inventory and Control of Enterprise Assets
2. The Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

For more information, read our blog on the topic!

Ok, but how do I do all of this?

We get it. Cybersecurity can be a difficult and complicated process. You might have a gut reaction to try and staff up to internally build out the cybersecurity resources you need to meet the complexity of addressing today's threats. But according to the ISC2 2020 Cybersecurity Workforce Study, 56% of organizations say that they are at risk due to the current cybersecurity staff shortage. Not to mention the cost of trying to build up the right resources yourself.

Calculating the Cost of Digital Security

Need to determine the cost of security analysts to protect your infrastructure? Consider the following:

- **+ An average endpoint generates 5000 security alerts per year**
- **+ 2000 endpoints generate 10,000,000 alerts annually**
- **+ A security analyst takes an average 15-30 minutes to investigate one alert**
- **+ Investigating only the alerts classified as "high" or "critical" would require hiring 21-22 analysts**
- **= An average analyst's salary is $35/hr., so those 21-22 analysts would require an investment of over $1.5 million annually.**

For more information on calculating the cost on your own SOC, review our Total Cost of Ownership eBook.

You also need to see around corners to find the threats you know are out there, but that's tough when your security products are locked up in silos and not communicating. You're not alone, as nearly 30% of organizations use more than 50 separate security solutions and technologies. But the same study providing this data indicates that companies with more than 50 tools rank 8% lower in the ability to detect a cyberattack and rank 7% lower in the ability to respond to an attack compared to companies using less than 50 tools.

Make no mistake, this is a dangerous situation. The volume and severity of cyberattacks is increasing through multiple cyber-attack vectors such as compromised credentials and email, phishing, and cloud misconfiguration. And security teams are missing the attacks sliding through these openings. Companies with 1500-5000+ employees admit they're ignoring 53% of alerts and it typically takes a team 27-30 minutes to investigate an actionable alert—and it also takes 26-32 minutes to investigate a false positive.

Quite frankly, it's a situation that sucks. But the good news is you don't have to take it anymore. You can take what seems like a monumentally complex challenge and simplify it down to clearly view threats and take direct action. But it will take a bold team, bold technology, and a badass service model to move the cybersecurity needle back in the direction of simplicity and peace of mind.

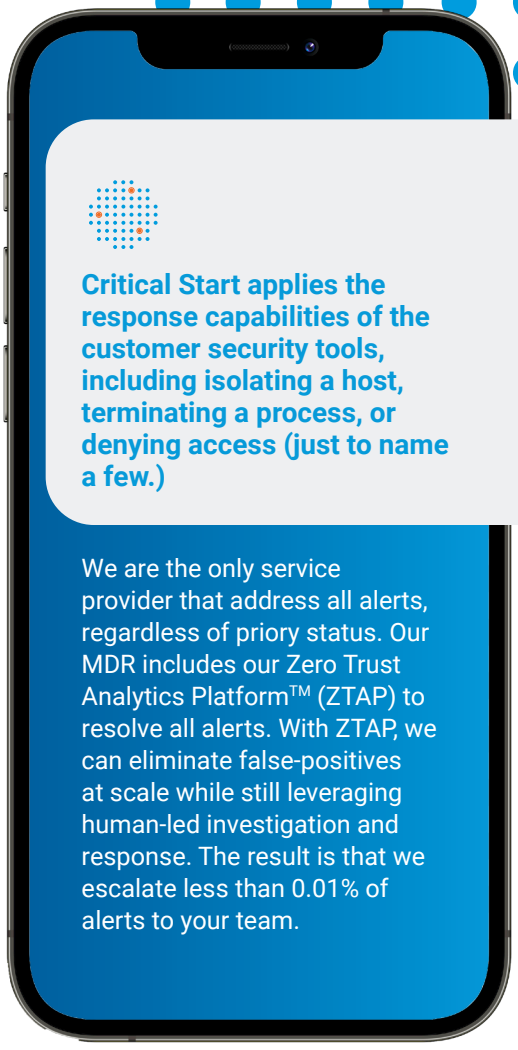
How to simplify the complex with MDR

Enterprises have a serious need to be able to extend their defenses to find, respond and mitigate threats. But building out a comprehensive approach to developing this capability internally can present a nearly insurmountable burden to enterprises that have other pressing business priorities than dealing with the complexity of cyber defense. Bringing the wide swath of technologies, services, and human capital together to blend both human and machine into a complete, actionable security ecosystem—is not something for the faint of heart.

MDR should work to create an enterprise SOC that strongly encompasses all of these elements to give its clients confidence that they have a highly collaborative partner to handle the critical security functions required to match up against the advanced cyberthreats they face. What does MDR for the enterprise look like? These are some of the critical components:

- ✓ It should outperform the traditional one-size-fits-all approach by adapting to the unique differences of each customer.
- ✓ It should simplify security and shrink risk with continuous monitoring/ threat detection and response coverage. Solutions and services should integrate with existing industry leading SIEM, EDR/EPP and XDR tools with the goal of building visibility, reducing complexity and collapsing attacker dwell time.
- ✓ Onboarding and implementation should take into the account the organization's unique environment and existing security tools and processes.
- ✓ MDR should automate areas such as automatic resolution of false-positives and include automated response actions to improve your SOC effectiveness and reduce attacker dwell time.

There should also be a mobile component (iOS and Android compatible) for on-the-go threat detection and response. Security analysts should not be chained to a desk, because when they can collaborate with their MDR partner and respond to threats from anywhere, attacker dwell time and risk are reduced, and SOC coordination and effectiveness are improved.



But here's the critical part:

Detections and Indicators of Compromise (IOCs) should be infused directly into the tools used by the MDR team. The goal is to create a high-fidelity threat detection and validation platform that uses specific detection logic customized to your environment. Threat intelligence should include a curation of original and third-party data to derive new detections and IOCs with everything mapped to the MITRE ATT&CK® framework to reduce complexity and improve SOC effectiveness.

The MDR response to threats should be guided by agreed upon rules of engagement. You want a team that will respond to an alert on your behalf with the core capability including remote response mitigation, investigation and containment activities far beyond traditional alerting and notification. This team should be able to scale to accelerate your journey while constantly focusing on the mission of protecting your business, not just chasing a revenue stream.

Finally, an MDR partner should have badass performance and be able to prove it. That means contractual SLAs that enable the client to hold them accountable to objective, irrefutable outcomes.

Critical Start Client SLAs include 1-hour time to detect and median time to resolution.

We also provide an incident response retainer: If we already know the client's network topology, it reinforces agility to our response during a crisis.

MDR Stops Threats Before Severe Damage Occurs

One particularly virulent ransomware affecting the financial services industry is Quack-bot (Q-bot). Q-bot defeats most endpoint protection technologies and steals credentials, account numbers, and other sensitive banking for export to cyber thieves. Q-bot has been evolving since 2007 to stay ahead of security technologies, making it a sophisticated and dynamic threat.

MDR is effective at countering Q-bot since security analysts can use playbooks to identify the seemingly unrelated alerts of Q-bot and connect them to the broader picture of an incoming attack. This provides the capability to stop this type of ransomware before it can do significant damage.

Build Versus Buy: Bottom line advantages to MDR

Utilizing MDR provides many distinct and serious cost advantages over trying to develop security capabilities in-house. MDR providers can help you take advantage of economies of scale to shrink total cost of ownership while increasing the expertise and resources you have at your disposal. The MDR provider will also already have the real estate, technology and expertise to integrate efficiently with your current environment. Software license costs can be significantly reduced, since the MDR provider can purchase licenses at scale, distributed across their entire client base.

Human Costs

On average, a single endpoint will generate 5,000 alerts annually. If a hypothetical business has 2,000 endpoints, it will translate into 10,000,000 alerts per year that security analysts will need to investigate. Here's what that looks like :

Critical-Priority Alerts
.1% of total events
2-3 analysts
$175,000/year

High-Priority Alerts
.9% of total events
21-22 analysts
$1,575,000/year

Medium-Priority Alerts
29% of total events
697-698 analysts
$50,750,000/year

Low-Priority Alerts
70% of total events
1682-1683 analysts
$122,500,000/year

SOC Total Cost of Ownership: Internal Versus MDR

Total Cost of SOC Ownership	Internal	MDR
SOC Analysts	$750k to $100,000,000+ based on number of alerts processed	Included
Alerts Processed	Typically critical/high only	All alerts resolved
Technology cost	$500k-$1,000,000	Included
Real-estate cost	$25-$85 per square foot	Included
Level of expertise	Varies	Very High, spanning multiple industries, security environments and threat scenarios
Level of protection	Varies	Extremely high

How to Build the Most Effective MDR for Financial Services

Resolving all alerts is a critical issue

Disruptive new thinking is needed to stay ahead of the shifting tactics of a human attacker. Recent insight on this need is provided from IDC. Their study found that for large enterprises with over 5,000 employees, it was taking more time (32 minutes) to investigate false positive alerts than the time it would take (30 minutes) to investigate an actionable alert that could indicate a threat. According to the study, a better state to address this trend should include: "Alerts are fully triaged and investigated by seasoned cyber professionals whose core focus is on detecting, stopping, and when necessary, responding to threats while using the latest technology…Statistics, like mean time to detect (MTTD) or mean time to respond (MTTR), are readily discussed at board meetings, without repercussions, because the trend line is toward reducing times."

Use XDR to limit attacker dwell time

One of the latest tools that MDR analysts can use is the next evolution in the security space is known as XDR. XDR unifies data including identity, email, cloud platforms and other networks to tell a story that analysts can use to more clearly identify true threats. Tim Junio, SVP of Products, Cortex at Palo Alto Networks explains the difference between XDR and legacy security approaches this way: "Protection, prevention and detection requires joining endpoint data with other data," he shared. "Basically, if you're dependent on only one source of information at a time for security, you're going to miss sophisticated attacks." Tim believes that combining endpoint data with network security data is an essential place to start. "If you look at the prior era of endpoint protection, which is where you started to have behavioral analysis and looking at things happening locally on a machine," he said. "And that obviously was a huge leap in technology that was efficacious for a while, but then adversaries adapted and started doing a better job of obfuscation. We needed a new approach and joining endpoint data with network data gave us new kinds of visibility. If you're looking across different data sets your odds dramatically improve that the attacker is unable to obfuscate across everything."

When considering the value of MDR and XDR working together, it's also a good idea to consider the cost of inaction. The reality is that very few attacks hit instantly. An attacker needs to gain access, examine the environment, get the right credentials, and then deploy Ransomware. This process can take hours or days. If XDR identifies a low or medium incident indicating a breach that is not routed to someone who will mount an effective response—let's say for 12 hours after the initial alerts—that is 12 hours a potential attack has to work within your environment.

How to Select an MDR Partner

The essential key in selecting an MDR vendor is to realize that not all are created equal.

Consider asking a potential vendor these questions as indicators of how they will perform when your organization is facing a threat:

- **How long does your team take to respond to alerts? Are there contractual obligations around this?**
- **Will my company have access to your SOC as needed or is that an additional charge?**
- **Is there any hardware associated with this tool?**
- **If my company grows quickly can the MDR tool you're using scale quickly?**
- **Can this tool help me respond to both SIEM and EDR from one console?**
- **Can we investigate and respond to alerts natively from our phones?**

Key Takeaway

The last two questions are particularly important, as they can determine what kind of control and visibility you will have in determining the direction of your new security environment. Information on alerts needs to be accessible from one device and one platform, and it should be accessible at any time and place to ensure critical threat and response information is always available as it happens.

Is it Really MDR?

As you're evaluating solutions, it's important to determine if what you're evaluating is a Managed Security Service Provider (MSSP) or true MDR. An MSSP takes incident and event data and monitors it 24 x 7. But an MSSP can be overly broad and does not dive deeply into the underlying causes of alerts. MDRs use their own SOC, security processes and infrastructure to really absorb alert information and uncover the hidden reasons behind them. Effective MDRs also have a much deeper and more sophisticated response plan in place to identify both vulnerabilities and threats, and then they take a dynamic response to resolving those issues.

Do They Treat Every Alert as Critical?

This means that every alert collected must be treated equally. In a legacy environment, with thousands of alerts pouring in from EDR and SIEM tools, many vendors will actually disable detection logic to prevent alerts they feel do not require attention.

The problem is that attackers are increasingly being detected through medium, low and even informational alerts. A top-down approach to dealing with alerts is simply not sufficient in today's threat environment.

A far more effective strategy is to use a trust-oriented approach to handling alerts at scale. An MDR vendor should work with their client to build a Trusted Behavior Registry to determine which alerts indicate normal behavior and can be trusted. Resources can then focus on the alerts outside of this registry.

Best-in-class threat prevention should mean:

- ✓ Complete visibility, detection, and response across network, endpoint, and cloud assets.
- ✓ Expert threat hunting and forensic specialists who will reduce your mean time to detect (MTTD) and mean time to respond (MTTR).
- ✓ In-depth security experience to help you properly tune and manage dedicated infrastructure.

You partner should be able to scale at the pace of your growth. Traditional approaches consistently require the addition of security analysts, technology, and operational process to stay ahead of new risks. But the right MDR partners should be simply able to look at your latest employee count and expand their services to keep risk in check.

Why Accept Risk?

Critical Start MDR is driven by ZTAP, featuring the Trusted Behavior Registry™ (TBR). This is the largest registry of known good alerts (false positives), which can deliver the scalability to resolve every alert.

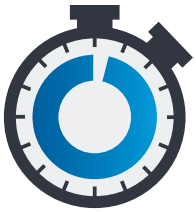
We take every relevant alert from your EDR, XDR or SIEM into ZTAP and match it against known good alerts in the TBR. If there is a match, the alert is automatically resolved. If there is no match, the Critical Start Security Operations Center (SOC) investigates the alert.

Are they willing to put it in writing?

This one question is particularly critical to not only building a good working relationship, but also ensuring that the vendor you're considering is ready to deliver on their promise.

While it's common for an MDR vendor to provide a Service Level Objective (SLO), that's not going far enough and here's why:

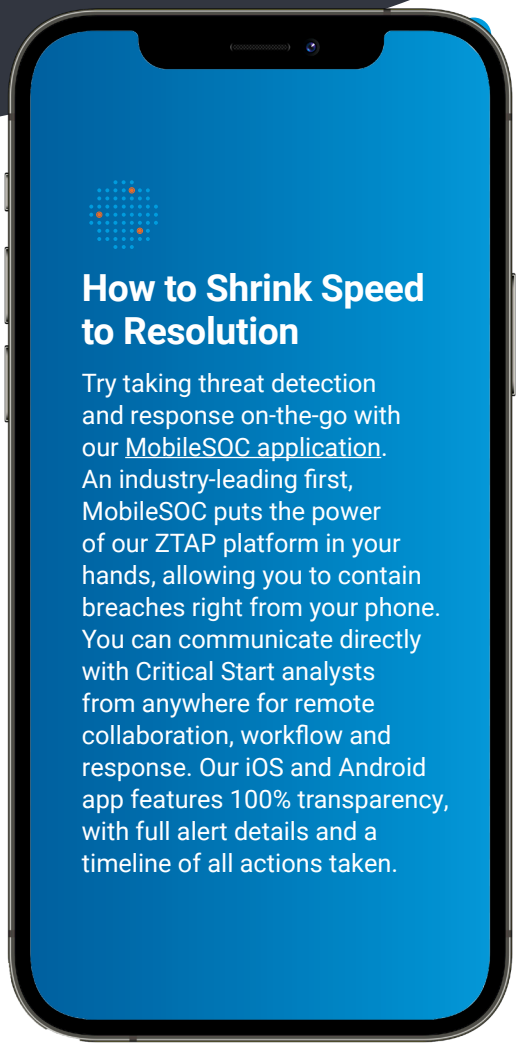
- An SLO is not committing to a median time to resolution.
- An SLO is not outlining any penalties if service level objectives are not met.
- An SLO is not defining a level of transparency to understand if a vendor is really measuring up to their promises.



At Critical Start, we provide a Service Level Agreement (SLA). In our SLA, we clearly define Time to Detect (TTD) and Median Time to Resolution (MTTR). Our guarantee is that we will triage every alert in minutes with a 1-hour SLA.

Our customer portal is also built around transparency. There's no "black box," as our ZTAP dashboard allows you to see what our analysts see. Working with Critical Start, you have complete visibility and access to every alert with full investigation details and every action taken. Everything can be audited and reports can be generated.

Beyond visibility into the service, you will have visibility across your security ecosystem. You can better understand how your security tools are performing and validate their return on investments, as well as gaining a clear understanding of the true value of your MDR service.



Why Critical Start is the Right MDR Choice for Financial Services

To simplify, we first embrace the complex

When we first started our MDR service, we said there must be a more challenging way to solve for the problems security teams are facing with detection and response. You read that correctly. We said **more challenging.** Every other security technology vendor and service provider in the market focuses on finding the outlier—the bad. But the problem with this approach is that there will always be too many different things to go look for—that's the very definition of complexity. How do security teams scale to keep up with threats? They **can't.**

Critical Start is the only managed detection and response services provider on the market today who chose to approach the problem differently. And may we dare even further by saying we approached it a better way. While others are focused on finding bad, we focus on finding good. While others prioritize or suppress alerts, we say, bring it on! Bring us every alert because we developed the industry's only Trusted Behavior Registry (TBR) within our Zero-Trust Analytics Platform (ZTAP) purpose-built to resolve all alerts.

Combine this exclusive technology with collaborative, well-trained, seasoned security experts--experts who will deeply understand your environment to adapt and scale with your organization's needs and partner with you to detect, investigate and respond to threats specific to your organization—and the result is a collaborative team, at your side, at your service. That's how we define simple for our customers.

24x7x365

Critical Start's 24x7x365 human-led investigation and response is performed by highly skilled analysts who work in a U.S.-based SOC 2 Type 2 certified Security Operations Center. Every analyst completes 200 hours of training during onboarding and another 40-80 hours annually.

There's no denying that cybersecurity is hard. But it doesn't have to be for you.

At Critical Start, our MDR business is simplifying your business. We deliver managed detection and response that flexes to your business objectives and cybersecurity vision, regardless of the complexity.

We offer unique benefits to enterprise customers who are building and optimizing security operations to be extremely effective and better at stopping breaches.

Turmoil to tranquility. Our services integrate with industry-leading security tools and our security experts tamp down the noise and push them to be more effective at detecting and stopping threats.

X – tended MDR. Over 40% of our existing customer base relies on us for threat detection and response that leverages multiple endpoint security tools. Our services also expand beyond endpoint to SIEM, identity and cloud.

Don't build a SOC, buy one. Our in-house SOC experts tailor our service to your unique needs and become an extension of your team, seeking to deeply understand your environment, helping you make faster, more accurate decisions on which actions to take.

Simple security, sped up time to value. Security teams will never scale to keep up with threats. So, we said let's approach the problem differently. We developed the industry's only Trusted Behavior Registry (TBR) within our Zero-Trust Analytics Platform (ZTAP) purpose-built to resolve all alerts. We simplify your life by reducing your volume of alerts by more than 99 percent. We escalate only less than 0.1% of alerts, and never send you the same alert twice. In fact, you can see an 80% reduction in false positives on the first day of production monitoring.

Life is mobile. Security operations should be, too.
We simplify your security team's lives with the power to triage and contain alerts from anywhere. Our mobile application, MobileSOC, provides you with easy, quick interaction with your Critical Start security team.

Bewilderment to clarity. Our service is an open book, and we give you the tools to inspect it. From your detection coverage aligned to industry frameworks, to full alert details with enhanced context, and a dashboard proving our contractual service licensing agreements for time to detect (TTD) and median time to resolution (MTTR)—we operate with precision and *everything* is visible in ZTAP and MobileSOC.

Tools change, but your service doesn't have to. We are on the journey with you as you continuously optimize your program. As you make decisions about the security tools you leverage, we'll be there at your side, scaling with you, still stopping breaches.

Conclusion

Financial Services has enough complexity without the threat of a cyber breach. Critical Start can help identify the gaps in your security coverage and put together the team, processes and technology to close the books on uncertainty and free your internal teams to focus on the strategic tasks that grow your bottom line.

To see how we can help, contact us at criticalstart.com/contact