ITSpecialist eSENTIRE

WHITE PAPER

Make the Business Case for Managed Detection & Response (MDR)

A Security Leader's Guide to Demonstrating the Value of Investing in MDR

Executive Summary

The state of cybersecurity is troubling for many security leaders. Threats continue to rise, with no signs of slowing down. Ransomware, for instance, is up 13% over the past year, which is more than the rate of the past five years combined, **finds Verizon**.

Meanwhile, organizations are expected to take on more cyber responsibility, such as compliance with evolving regulatory frameworks, cyber insurance requirements, and third-party vendor risk management. At the same time, rising costs and the threat of a recession are causing many businesses to reduce headcount, while reprioritizing their spend and increasing due diligence on their cybersecurity programs.

Unfortunately, cost-cutting measures like reducing headcount or budget cuts aren't as easy to make for business-critical areas like cybersecurity.

As it stands, IT teams are often overstretched due to the continuing cybersecurity skills gap, making true 24/7 security coverage unsustainable. And as cybersecurity threats grow, businesses of all sizes face an increased risk of cyberattacks resulting in downtime and revenue disruption, loss of reputation, customer trust, legal fines, and more.

So, how can chief information security officers (CISOs) and other security leaders manage increased cyber risk without overloading employees or spending recklessly? **The answer lies in tying cyber risk and business risk together.**

Comparing the cost of your cybersecurity measures in relation to business risk reduction, e.g., reducing the risk of downtime and revenue disruption, can help Security and Finance teams see eye to eye on where to make security investments that keep their business up and running.

To improve overall cybersecurity ROI, your Finance and Security teams should align on what business disruption means to your company from a dollars and cents perspective. Preventing said disruption means ensuring 24/7 threat detection, investigation, containment, and threat response capabilities to reduce threat dwell time and stop spread across your environment will be critical. How this is achieved can vary depending on your organization's resources and maturity.

One option is building out your own 24/7 Security Operations Center (SOC) so your team can use forensic tools and threat intelligence to hunt, investigate, and respond to threats in real-time. However, it's often a non-starter for many businesses, considering the investments in security tools, staffing, and operational expenses it takes to effectively build out an in-house SOC.

A second more proactive solution that is 80% more cost effective involves outsourcing your Security Operations to a trusted Managed Detection and Response (MDR) provider who can identify, isolate, respond to, and remediate known and unknown cyber threats 24/7 on your behalf, rather than only delivering security alerts that your team struggles to manage.

As this report examines, making the business case for MDR can be easier than you think, as long as you're armed with the right tools and strategies for building alignment with your organization's Finance leaders.

Challenges IT & Security Teams Face in the Current Economic Environment

While many companies are taking cybersecurity more seriously than ever before, staying ahead of cyber threats can feel like running in a hamster wheel. It's not a question of if, but when cyber threats will bypass traditional cybersecurity controls. Security leaders need to provide 24/7 coverage globally, avoid alert overload, and detect, investigate, respond to, and contain threats - which is frequently not possible for smaller in-house resources that wear multiple hats.

So, instead of making progress, you're running in circles without feeling like you have the right protections in place.

That's due to challenges such as:

- **Limited budget:** Most security teams don't have the luxury to add new cybersecurity tools whenever they want or to hire more staff to monitor and remediate threats in real-time. They often have to make do with limited budgets and fight for every dollar, especially in this era of rising costs and recession risk.

  "Every department is competing for budget, and there's only so much money to go around," says Greg Crowley, CISO at eSentire, and former VP, Cybersecurity & Network Infrastructure at WWE.

- **Constrained resources:** Time and employee bandwidth also have limitations. A big contributor to this problem is that existing security providers simply pass on any alerts they identify to your team, without doing a thorough threat investigation and taking response on your behalf, let alone prevent them from happening again.

That leaves in-house employees overwhelmed with alert fatigue and often a backlog of additional work needed to secure the organization, which can lead to employees burning out. At some point, there's simply not enough resources to manage everything, especially with companies often having a shortage of employees with cybersecurity-specific skills.

"We've been hearing about it for years. There's a skills shortage. There's a cybersecurity personnel shortage and inflation is driving up salaries. There's burnout. All those are real, and they are definitely felt amongst security teams," says Crowley.

In addition, businesses are also facing a growing scope of cybersecurity responsibilities:

- **Expanding threat landscape:** Increased digitalization, remote work, and cloud migration expand the attack surface. It's not just a matter of dealing with a higher quantity of threats. This expanding attack surface also requires expertise in threat hunting, containment, and remediation.

- **Increased cyber oversight:** Regulators and/or supply chain partners are increasingly asking companies to provide more transparency on their cybersecurity practices, and they're holding companies accountable for cyber protocols. Organizations with boards also see increased cyber responsibilities put on their directors.

- **Meeting cyber insurance requirements:** Underwriters at cyber insurance providers are looking to reduce policyholder risk and many times require that policyholder organizations develop and implement strong cybersecurity controls and governance including 24/7 security monitoring and incident response capabilities.

- **Proving the cost-effectiveness of cybersecurity investments:** Amidst budget constraints, business leaders want to see that they're getting their money's worth from cybersecurity investments. They also want cyber tools and services to deliver quick time to value for their investments.

  "To get the most value out of cybersecurity spend, Finance wants to see reporting on what cyber threats look like and what cybersecurity investments are doing to block those threats," notes Anthony Lam, CFO at eSentire, who's held several CFO roles throughout his career, including at publicly traded companies.

  To build alignment between the two teams, this reporting should speak in business terms, e.g., showing how a cybersecurity investment prevented an attack that could have caused two weeks of business interruption.

With all these challenges converging, security leaders can't sit back and see what happens. They need to act by coordinating to optimize cybersecurity spend and minimize risk.

Getting the Finance on Board: 5 Steps to Build the Alignment

While many business leaders understand the importance of investing in cybersecurity, they might not be fully aware of what the threat landscape looks like. To find the type alignment that leads to more effective cybersecurity investments, Security leaders need to closely consider the perspective of Finance, who think primarily about risk and finances, and elevate the sense of urgency by highlighting the financial risk of not taking cybersecurity investment action - now.

"Understand the overall business plans, initiatives, and goals, and then align your security spend with those, making sure that security is enabling business success," advises Crowley.

To build that alignment, here's what Security leaders should be ready with to get Finance on board:

1. **Present cyber risk as a financial risk:** Discuss specifically what cyber incidents could cost your company.

   "Security leaders need to articulate cyber risk in business terms, which usually means dollars and cents," says Tia Hopkins, Field CTO and Chief Cyber Risk Strategist at eSentire.

   "But even though they can expect to get more resources and support from senior leaders, there will be a bit more scrutiny on their program spend, and so they'll have to come up with meaningful KPIs and metrics to demonstrate the effectiveness of their cybersecurity investments," adds Hopkins.

   One of the biggest financial risks is downtime, such as from ransomware, which leads directly to lost revenue from interrupting the normal flow of businesses.

   Ransomware remains the biggest threat from an organizational, financial, and brand perspective, causing an average of 22 days of business interruption — meaning less than 100% productivity —according to Coveware. Plus, you need to account for the cost of remediation.

The average daily cost of downtime could be far more expensive than cybersecurity investments. **In many cases, the resulting downtime alone can cost organizations upwards of $225K per day, which drives many security leaders to pay the ransom, adding to the financial hit to the organization.**

Mean Daily Downtime Cost Per Industry (in USD)

Healthcare

$244,267

Finance

$228,589

BioPharma

$225,552

Technology

$224,837

Energy

$223,810

Legal

$223,586

Industrial

$221,979

Transportation

$219,790

Entertainment

$220,013

Retail

$217,646

Hospitality

$216,574

Source: eSentire analysis based on IBM Annual Cost of Data Breach report and IDC market intelligence

2. **Adopt a risk-based approach:** "Presenting cyber risk as financial risk only tells part of the story. Finance leaders want to adopt a risk-based approach," says Lam, "with the goal being to direct budget according to risk priority areas."

   So, aligning cybersecurity investments based on critical areas that are most at risk of contributing to business disruption will help you make that case for sufficient budget.

   Also, keep in mind that average downtime costs only tell part of the story. Discussing additional risks, which might have different priority levels within your organization, such as:

   - **Legal/compliance costs**, e.g., regulatory fines for mishandling sensitive data
   - **Communication costs**, e.g., for notifying customers of attacks and remediation steps
   - **Potential reputational damage**, which can lead to long-term revenue losses, such as if customers lose trust in your business

   Focusing on these costs helps Finance leaders understand that even though all risk can't be eliminated, strengthening cybersecurity can deliver ROI based on these potential costs.

3. **Speak the same language:** Building alignment also requires communicating via terminology and core concepts that everyone understands.

   That could include getting technologists involved to help non-technical leaders understand cyber technology the role it plays in reducing risk. Doing so could also help articulate the total number of points of risks overall.

   However, be mindful of technology speak. There's a fine line between getting the stakeholders to understand technology risks and opportunities vs. losing them in the details. So, always tie these conversations back to finance.

   "It's important for the technologists to really try and talk in terms of what key financial stakeholders understand, which is risk in dollars," says Lam.

4. **Offer options:** Finance often wants to see what good, better and best options look like so they can weigh the costs and benefits.

   If you can make the case side-by-side as to how more robust investments can alleviate existing constraints and provide strong value, you can avoid the situations where investments get delayed quarter after quarter.

   For example, outsourced MDR services might appear more expensive, but if finance leaders can see how that upfront expense can reduce the cost of security tools, security operations and hiring staff, they might be convinced to pull budget from upcoming quarters forward.

> As a CFO, I would want to see a decision matrix, like what does adding a solution from Company A give us vs. adding one from Company B, and what the price differential is.
>
> At the end of the day, Finance teams are more interested in the value we get for the dollar we pay. So, if it makes sense to spend a little bit more because you're getting elements of extra value, that could be worth paying for.
>
> *- Anthony Lam, CFO, eSentire*

5. **Demonstrate program improvement with reporting:** Building alignment isn't limited to situations where you need to ask for budget for new investments. Security teams should also get on the same page as their Finance team through ongoing reporting of existing cyber investments, whether that's to show shortcomings or prove the ROI of past investments.

   In general, provide at least quarterly reporting for what your security solutions are doing and how they're protecting the organization. Still, remember to not get too bogged down in technical details, especially as this reporting might be presented to other senior leaders and boards.

   "You don't want to go in talking to senior leaders and boards in terms of, say, 20% of events are coming from this initial attack vector, for example," says Hopkins. "You do want to tell a story to tie back to business risk. There's a bit of an art to that."

   Keep the focus on the business impact, avoid downtime leading to revenue disruption and reducing the risk of compliance/legal issues stemming from a data breach.

Key Metrics to Track Overall Security Program Improvement

- Avoiding Downtime, Leading to Revenue Disruption
- Reducing Risk of Compliance & Legal Issues
- Mean Time to Detect
- Mean Time to Contain
- Average Incident Handling Time
- Threats Prevented Through Automated Blocking
- Exploitable Vulnerabilities Addressed
- Comparable Industry-Specific Asset and Overall Risk Scores

Presenting Finance With Options to Reduce Risk & The Threat of Downtime

While you might have a wide range of conservations with Finance, building a cybersecurity defense framework generally boils down to one of two approaches — building out your own SOC or leveraging an MDR provider.

Keep in mind that the goal is to build cyber resilience, rather than the unrealistic goal of eliminating cyber risk. According to the National Institute of Standards and Technology (NIST), cyber resilience is your "ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources".

Although building cyber resilience doesn't guarantee keeping every single adversary out of your environment, it does prepare your organization to defend against advanced cyberattacks and the latest tactics, techniques, and procedures (TTPs) attackers rely on.

These common security approaches can vary in terms of the expense and effectiveness in building cyber resilience. So, present a cost/benefit analyses for these options:

1. **DIY SOC Approach**

   To defend against modern ransomware threats in real-time, you can't rely on outdated, traditional cybersecurity solutions in the name of prevention – you need 24/7 threat detection, investigation, and response capabilities. A Security Operations Center (SOC) helps protect an organization from known and unknown cyber threats that can bypass traditional security technologies.

   The do-it-yourself approach, where you fully build out your own in-house SOC that meets your needs, is often cost-prohibitive. In addition to committing years to designing the facility, your cybersecurity team must consider the financial investment required to arm them with the best people, processes, and technology.

   To sufficiently staff a SOC, you'd generally spend far more than you would by leveraging an external provider. DIY can also be costly and/or create security gaps given the constant technology upkeep needed to meet new cyber threats and cyber oversight obligations.

   By a conservative estimate, the costs associated with building a SOC in the first year alone for 100 employees can be upwards of $800,000.

   Plus, a DIY approach can exacerbate issues like IT staff being overstretched. Asking existing staff to take provide 24/7 coverage globally for managing security threats generally isn't feasible unless you significantly ramp up hiring.

   "You can't ask your staff to always be on call," says Crowley.

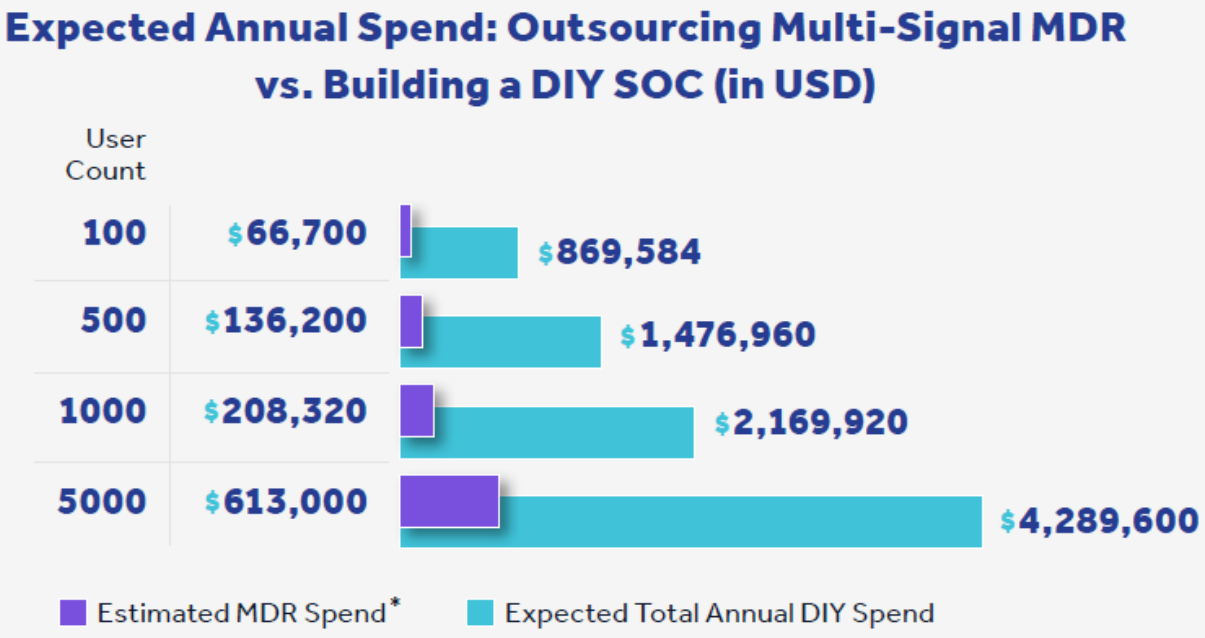
   But without 24/7 coverage, it's hard to be resilient in the face of accidents, threats, and attacks.

2. **Multi-Signal MDR Approach**

A multi-signal MDR provider tends to be more cost-effective and risk-effective than building out your own SOC or continuing with a partner who only delivers alerts. Not only does MDR often cost significantly less than hiring your own threat intelligence staff and licensing cybersecurity tools, but it can also help you get the most out of existing IT/security investments because many providers offer BYOL options that leverage your existing security tools.

Strong MDR providers can respond to threats on your behalf. They also provide technical knowledge based on experience gained across a wider range of businesses. Plus, if they have a large customer base, they can apply any detection engineering or runbooks created from other customer environments similar to yours through Security Network Effects. So you can learn from others without having to go through the pain yourself.

> When you think about the cost of cybersecurity professionals to bring them in-house and weigh that against the value of an outsourced MDR provider being able to bring a suite of services together under one hat, there's a strong value proposition in going with an MDR provider," says Lam.



* The multi-signal MDR cost displayed is an estimate. For an accurate quote on eSentire MDR, please fill out our Request A Quote Form

The Value of MDR Is an Easy Sell

A strong MDR provider can strengthen your security while costing less than many other solutions. Compared to the cost of downtime, it's clear that MDR makes financial sense if you're serious about reducing financial risk, reputational risk, and compliance risk.

If you can frame the value of MDR in terms Finance understands, then it's often an easy ask, especially if you want to stay ahead of risk.

"Don't wait until something happens to allocate budget to it," advises Crowley. "Make the budget part of every business goal and initiative and understand that security needs to be 24/7/365. You need that quick response and 15-minute mean time to contain that MDR provides."

However, not all MDR providers are the same. In fact, when it comes to doing more with less, seek out a partner who truly "Owns the R in MDR" and prioritizes complete threat response. An effective MDR provider should offer:

- **Multi-signal ingestion:** Ingestion, normalization, and correlation of data across network, endpoint, email, identity, log, cloud, and other sources so you have full visibility across

your attack surface.

- **Access to a world-class team of 24/7 SOC Cyber Analysts and threat intelligence & threat hunting experts:** Your MDR provider should have a team of Elite Threat Hunters that support their 24/7 SOC Cyber Analysts with building detection models, conducting proactive global threat hunts, and curating original threat intelligence research.
- **Security network effects:** An MDR with a global customer base can apply findings from incidents that may have impacted other customers to help you proactively avoid the same threats should they impact your organization.
- **Peace of mind and reduced in-house resources required due to Response expertise:** You don't just want alerts; you want the security of knowing the MDR provider has the expertise, experience, and context to take action on your behalf to eliminate threats from your environment effectively. They should also be able to manage incident response on your behalf to not overwhelm or distract your existing team members.
- **Interoperability:** Your MDR provider should easily integrate with your existing tech stack vs. forcing you to onboard their specific tech/tools.

Case Study: VENERABLE®

Venerable is a leading US-based organization holding organization within the insurance annuity sector that focuses on building and growing insurance businesses with long-term capital.

Venerable's small but mighty security team needed a trusted security partner that could cover in-house security expertise gaps to mitigate cyber risks and address multi-cloud security by:

- Evolving at the same speed with which cloud technologies are evolving,
- Prioritizing a security strategy that encapsulates the necessary toolsets, resources, and cyber expertise that can support their security roadmap and outpace their business technology requirements, and
- Having the security expertise to ensure that their multi-cloud environment was protected against misconfigurations and vulnerabilities.

Read this case study to learn why Venerable chose eSentire and how they benefit from 24/7 threat detection and response as well as cloud security posture management to secure their multi-cloud environment.

Download Now

Turn Alignment into Savings and Security

There's no doubt that companies face significant challenges from both security and economic perspectives. Security leaders need to build resilience in the face of increased cyber risk, yet they often seem to lack the resources to optimally do so.

But even though budgets may be too tight to increase investments, it's often possible to improve cybersecurity effectiveness with the right solutions and save money in the long run. For example, reducing ransomware risks can reduce the costs of downtime, so it could make financial sense to increase budget for a cyber program.

To make these investments IT & Security teams need to be able to make a business case to Finance.

However, doing so means building alignment. To get on the same page, frame cybersecurity risk as a business risk. By looking at the pros and cons of different security approaches in financial terms, rather than just technical ones, you can come to a win-win agreement.

In many cases, Security and Finance both conclude that outsourcing MDR capabilities to a high-quality provider is more cost-effective in the long run compared with the cost of downtime or building a SOC in-house.

MDR can save you upwards of 80% compared to a DIY approach. And everyone in your company benefits when you can save money while strengthening security.

Not all MDR is Equal: What Sets eSentire Apart

eSentire is recognized globally as the Authority in Managed Detection and Response because they hunt, investigate, and stop known and unknown cyber threats before they become business disrupting events. eSentire was founded in 2001 to secure the environments of the world's most targeted industry—financial services. Over the last two decades, they have scaled cybersecurity services offering to hunt and disrupt threats across every industry on a global scale.

With two 24/7 Security Operations Centers (SOCs), hundreds of cyber experts, and 1750+ customers across 80+ countries, eSentire has scaled to deliver cybersecurity services with a proven track record of success in securing businesses across global industries.

eSentire, goes beyond the market's capability in threat response, helping organizations of all sizes build resilience and prevent disruption. eSentire's multi-signal MDR approach ingests endpoint, network, log, cloud, asset and vulnerability data to enable complete attack surface visibility. Enriched detections from the eSentire Threat Response Unit (TRU) are applied to captured data identifying known & unknown threats including suspicious activity and zero-day attacks.

eSentire's Cyber Resilience Team, comprised of our SOC Cyber Analysts, Elite Threat Hunters, Threat Response Unit experts act as an extension of your customers' team from Day 1. Powered by their industry-leading XDR cloud platform and unique threat intelligence, eSentire can detect and respond to cybersecurity threats with a Mean Time to Contain of 15 minutes.

eSentire MDR features include:

- ✓ 24/7 Always-on Monitoring
- ✓ 24/7 Live SOC Cyber Analyst Support
- ✓ 24/7 Threat Hunting
- ✓ 24/7 Threat Disruption and Containment Support
- ✓ Mean Time to Contain: 15 minutes
- ✓ Machine Learning XDR Cloud Platform
- ✓ Multi-signal Coverage and Visibility
- ✓ Automated Detections with Signatures, IOCs, and IPs
- ✓ Security Network Effects
- ✓ Detections Mapped to MITRE ATT&CK Framework
- ✓ 5 Machine Learning Patents for Threat Detection and Data Transfer
- ✓ Detection of Unknown Attacks Using Behavioral Analytics
- ✓ Rapid Human-led Investigations
- ✓ Threat Containment and Remediation
- ✓ Detailed Escalations with Analysis and Security Recommendations
- ✓ eSentire Insight Portal Access and Real-time Visualizations
- ✓ Threat Advisories, Threat Research, and Thought Leadership
- ✓ Operational Reporting and Peer Coverage Comparisons
- ✓ Business Reviews and Strategic Continuous Improvement Planning

Our Difference	Your Results
Full Threat Visibility & Investigation	See the complete picture of your attack surface with multi-signal intelligence enabling deeper correlation and investigation capabilities, proven to contain threats faster.
24/7 Threat Hunting & Disruption	Be confident you're continuously protected by our SOC Cyber Analysts and Elite Threat Hunters who rapidly investigate, contain and close down threats when an automated response isn't possible.
eSentire XDR Cloud Platform	Stay ahead of new and emerging threats with high fidelity detection and automated real-time threat disruption powered by unique intelligence from across our global customer community.
Rapid, Robust Response	See even the most advanced threats disrupted, isolated, and stopped with a Mean Time to Contain of less than 15 minutes. We detect in seconds and contain in minutes, so your business is never disrupted.
Original Threat Intelligence	Add world-class threat researchers to your team to hunt the most advanced undetected threats. Our Threat Response Unit (TRU) delivers original research, curates threat intelligence and builds new detection models to ensure you stay ahead of attackers.

Want to Learn More?