deepwatch

Managing Security Risk: Cybersecurity Solutions for Mid-Sized Businesses

A SCALABLE APPROACH TO STOPPING CYBERSECURITY THREATS

Introduction

There is a new security reality facing mid-sized business leaders and security professionals today.

With breaches costing small to mid-sized businesses an average of $3M in 2021[1] the stakes are higher than ever.

Three factors are driving security leaders to meet with their boards of directors and business leaders to address these increasing risks to the company's bottom line:

1. **Changing business models** including modernization, cloud adoption, and a shift to remote work are expanding the attack surface
2. **Ransomware and phishing attacks** are now advanced persistent threats
3. **Attacks on security vulnerabilities** are on the rise

In this guide, you'll find answers to these challenges and how an MDR solution can help you efficiently maximize security investments and effectively manage security risks to your business.

Growing the Business in **Changing Times**

Security leaders and business owners share a common goal – both want to grow the company securely while meeting revenue goals. In the past, security was seen as an administrative cost center, only loosely tied to business operations. Today, with technology often a required component of business, these goals are no longer mutually exclusive.

In recent years, an organization's survival has come to depend on its ability to rapidly modernize, causing many organizations to accelerate their modernization plans in response to the events from 2020-21. Unfortunately, this race to adapt introduced more cybersecurity risks for businesses to manage than ever before. In the past two years, we have seen skyrocketing growth in security attacks using a combination of old and new tactics, techniques, and procedures.

Remote Work and the Rise in Ransomware

In early 2020, remote work went from a rare opportunity for workers around the world to a global business norm almost overnight.

While business and IT teams raced to modernize operations, bad actors took advantage of the situation. The most ominous trend over the past two years has been the steep increase in ransomware attacks with exorbitant extortion demands. On the dark web, criminal gangs have monetized ransomware to increase their profits with multi-pronged business schemes such as ransomware-as-a-service and double- and triple-extortion demands, posting stolen credentials for auction if the victim doesn't pay. These ransomware attacks have created nightmares for businesses worldwide.

Many ransomware attacks are never mentioned in the media. A 2021 survey[2] of ransomware victims revealed:

- **60% of respondents experienced** revenue loss after the ransomware attack
- **53% stated their brands** were damaged as a result
- **42% of the respondents with cybersecurity insurance** found their policy only covered a small percentage of damages
- **Multiple factors increase the risk** of a crippling ransomware attack, including unmonitored networks, inadequate threat detection, unsecured email systems, compromised passwords, spear phishing emails, and employees who click on phishing emails.

Raising the Table Stakes: New Security Requirements

No wonder organizations are struggling to manage cybersecurity risks while running their businesses. In today's marketplace, three new areas for the security leader have emerged as the top critical risks to keeping the business in operation while meeting revenue goals.

Cybersecurity Understaffing Causes Security Risks

For over a decade, the demand for skilled and experienced cybersecurity talent has far outstripped the supply. In The Life and Times of Cybersecurity Professionals (2021), 95% of respondents noted the industry's skills shortage has not improved and is getting worse. Citing higher workload from unfilled positions or unprepared new hires, respondents said they're burnt out and leaving jobs as a result. With 70% of respondents saying they're constantly recruited for new positions, it's not surprising these are now critical problems for IT and InfoSec leadership to fix.

Finding the right security talent is hard. In the same survey, 78% of respondents noted they found recruiting cybersecurity talent difficult. The recruiting challenge is worse for mid-sized businesses that need cybersecurity generalists, which is at odds with the industry trend toward specialization, driving compensation higher and higher to levels that mid-sized businesses cannot sustain.

WHEN SECURITY STAFF LEAVE, NEW CHALLENGES ARISE

When a SecOps job is not filled immediately following the departure of an experienced security analyst, security threats and overall business risks increase. If critical security duties, like network monitoring or threat hunting, are missed on any given day or night, the risk of a devastating breach is much higher for the business.

Difficult-to-Manage Cybersecurity Technologies

Many organizations are playing catch-up to secure the new virtual perimeter, pouring large dollar amounts into costly technologies hosted in multi-cloud and hybrid security environments. These technologies require specialized expertise to ensure they are properly deployed to effectively secure the internet-facing perimeter. They also require expert management for users to realize the full benefits of the technology. Hiring and retaining the right expertise in an already tight labor market is untenable for mid-sized companies with smaller security teams and limited budgets.

Lack of “Common Ground” with the C-Suite

A survey of security leaders revealed a startling finding: only 16 percent of respondents say IT security and lines of business are fully aligned with respect to preserving cybersecurity during the digital transformation process. Security leaders tasked with managing cybersecurity risks also need to educate their business leadership about cybersecurity and demonstrate the ROI of security investments.

OTHER SECOPS CONSIDERATIONS

- **Regulatory Compliance**
  (PCI-DSS, HIPAA, ISO/IEC 27001)
- **Data Privacy Laws**
  (GDPR, CCPA, HIPAA)
- **Third-Party Security**
- **Supply Chain Security**

Modernizing the SOC & the Fast Track to SecOps Maturity

Best practices for mature security operations include 24/7 security monitoring of internet-facing systems, advanced email security, Security Information and Event Management (SIEM) alert management, and specialized human expertise. To achieve "good enough," a cybersecurity program requires a customized application of best practices mapped to a security framework, like the NIST Cybersecurity Framework (CSF). The framework can then be connected to the business goals and desired security outcomes, providing a source of truth for executive alignment on risk tolerance while maintaining good cybersecurity hygiene.

CYBERSECURITY HYGIENE BEST PRACTICES

- **Multi-Factor Authentication**
- **Email Security and Phishing Prevention**
- **Security and Event Information Management (SIEM)**
- **Vulnerability Scanning and Patch Management**
- **Endpoint Detection and Response**
- **Next-Generation Firewall Technology**

Source: Deepwatch 2022 Threat Intel Report

Three Strategies to Solve SecOps Challenges

Maturing Security Operations can be difficult if resources are limitied, staff are hard-to-hire, and critical technology may not be properly deployed, or exist at all. To address these common issues faced by security leaders today, these three areas can be prioritized in SecOps.

24/2/365 Security Alert and SIEM Management

Security teams cannot rapidly detect and respond to threats if they lack visibility of activity in the environment. Deploying a SIEM system to maximize the value of their existing security investments is a best practice. A properly managed SIEM ingests log sources from preventative technologies, like antivirus, intrusion detection systems, vulnerability scanners, and critical netflow from connected systems throughout the company environment.

However, not all SIEMs are the same, and not all organizations can afford a best-in-class SIEM. In addition, SIEM management expertise is needed to properly deploy, manage, and tune the SIEM.

Implement Security Controls for the Remote Workforce

With migration to remote work, both the use of personal (BYO) devices and the rate of employee churn have increased. Staff turnover and BYO devices introduce the risks of improperly secured endpoints and put the business in danger. The repercussions of data breaches related to remote work are also more severe, costing $1.07M more on average.[1]

This has changed the value of many security tools. On-premise network monitoring tools are now less valuable than endpoint tools, DNS filtering, email security, and remote proxy solutions for protecting workstations and users. New employees, remote employees, and staff attrition are risks because new employees have a higher likelihood of clicking on phishing emails that download malware or links that trick them into entering their credentials on fake websites.

Even with security awareness training, employees still make mistakes. The security team has to catch those mistakes before threat actors gain a foothold in the network.

Extend the In-House Team with Expert Support

Outsourcing is a good way to address immediate staffing pressures and associated security risks. Instead of wasting time trying to hire in-demand experts at astronomic salaries, outsourcing aspects of security operations to a security vendor that can augment the in-house resources.

Shoring Up Security Defenses **in a Rising Tide**

There is no such thing as a 100% preventative solution in cybersecurity. Effective cybersecurity requires a defense-in-depth strategy that combines an in-house security team with third-party managed security services that provide fast time-to-value on security investments. To level up their security operations fast, companies are choosing either a managed security services provider (MSSP) for basic security services, or a Managed Detection and Response (MDR) provider for 24/7/365 security monitoring, advanced threat monitoring, and complete customer service.

Raising the Table Stakes on Security

Shoring up detection and response capabilities is the most effective way to reduce cyber risk. Doing so requires around-the-clock monitoring with visibility across the entire environment. Traditional MSSPs can't deliver the necessary level of detection and response. This is where the right Managed Detection and Response partner comes in–to mitigate the risks and support improved outcomes.

Leveling Up the SOC with MDR Now

A SOC is the gold standard for effective security, yet building and operating a SOC requires a level of investment that is out of reach for most companies. The right MDR vendor can provide the benefits of an expert-managed SOC at a price that fits the security budget of a mid-sized company.

MDR has become the go-to choice, with analyst firm Gartner Research predicting 50% of businesses will have some type of MDR in place by 2025. Business and security leaders need to align the security program with desired business outcomes to invest in the right type of MDR partnership for long-term success.

The first step in finding the ideal MDR service is to establish the baseline security requirements of the environment. Then, the core attributes of different vendors can be evaluated to determine if the necessary detection and response functionality is provided.

CORE FEATURES SHOULD INCLUDE:

- **Analyst-recognized MDR service provider**
- **24/7/365 security monitoring** managed by trained, U.S.-based security analysts
- **Hosted in a secure**, closed platform and engineered to perform advanced threat detection and rapid response
- **Visibility across the environment** delivered through a SIEM that is tuned for critical data ingestion and high-fidelity alerting
- **A methodical approach** to achieving a modern Security Operations Center that scales with evolving business needs and can be measured with a SecOps maturity model while allowing your team to focus on strategic initiatives
- **Historical data portability**

Winning C-Suite Support

An advanced MDR provider allows organizations to realize the full benefits of comprehensive security operations, including a SOC, at a significantly lower cost. An MDR can provide the customer service that traditional MSSPs do not. Investing in an MDR service returns an almost immediate ROI and risk reduction due to improved visibility and 24/7/365 security monitoring. Demonstrating the following benefits of working with an MDR vendor helps the C-Suite understand the full value of a trusted MDR partner, both in securing the business today and helping it grow securely over time:

Extend the security team — Outsourcing monitoring to an MDR provider can ensure fully staffed security and optimized and maximized technology.

Scalability — An MDR service provider can help optimize current and planned security investments and operationalized threat intelligence across their customer verticals.

Reduce Security Management Complexity — Outsourcing ensures organizations don't have to worry about the cost, time, and expertise of having to staff and maintain a SOC on premise.

Reduced Staffing Costs — Optimize investments needed in people to build and manage an effective SOC.

Improved Work-Life Balance for In-House Staff — With the confidence that security events are monitored and prioritized 24/7/365, internal security staff can enjoy dinner, watch TV, and take time off.

Risk Management — MDR experts can help build and maintain SecOps risk management frameworks, including frameworks specific to SOC environments.

Long-term Growth — With pressure off the security team, security leaders can focus on tasks to support business growth, which they previously could not get to.

Business Continuity — Working with an MDR partner provides much-needed stability, reducing the loss of continuity due to the cybersecurity staffing revolving door.

The challenges faced in Security Operations are not going away, and companies are making the shift to managed detection and response faster than ever before. The right MDR provider can support CISOs, CTOs, and IT security leaders with world-class SecOps services, establishing secure and sustainable business operations that pave the way for optimal growth in the future.

How Deepwatch Can Help

Deepwatch secures businesses via its highly automated, cloud-based SOC platform backed by a world class team of experts that protect your network and digital assets 24/7/365. Deepwatch extends your team and proactively improves your cybersecurity posture via our proprietary maturity model. Deepwatch's managed security services are trusted by leading global organizations.

Deepwatch is an analyst-recognized MDR, proven to deliver advanced threat detection and rapid response, with the expertise and technology to provide 24/7/365 customer support for escalated, coordinated incident response.

- **Get Time Back for the In-House Team:** Relieve understaffed in-house IT and security teams from complex security burdens that inevitably cause staff burnout.
- **Proactive Security:** Reduce risk with increased visibility across the network, including email security to stop phishing and mitigate the risk of ransomware.
- **24/7/365 Monitoring:** Expert analysts quickly detect and respond to threats, reducing the likelihood of a catastrophic breach.

To learn more about how Deepwatch Managed Detection and Response can help, visit **www.deepwatch.com.**

deepwatch

ABOUT DEEPWATCH'S MANAGED DETECTION & RESPONSE SERVICES

Deepwatch is a trusted security leader, offering professional and innovative managed security to help support security operations and stop breaches and attacks. Deepwatch's managed detection and response services include 24/7/365 threat monitoring, alerting, validation, and proactive threat hunting, with accelerated detection of malware, botnets, and ransomware behavior aided by industry's most comprehensive and fastest platform built with machine learning and content libraries. At Deepwatch, organizations work with a named squad—an assigned team of experts that includes detection and response analysts and threat hunters who take time to understand a business's unique environment.

From economies of scale, network effect and technology, and personnel savings, with Deepwatch's MDR solution, customers have realized greater than 450% ROI per year on average. Moreover, through real-time squad collaboration and engineering refinements, customers' environments have seen 40%+ improvements in security maturity every year.

Visit www.deepwatch.com or reach out to us at sales@deepwatch.com.

SOURCES

[1] IBM Cost of a Data Breach Report 2021:
https://www.ibm.com/downloads/cas/OJDVQGRY

[2] Ransomware: the True Cost to Business, Cybereason:
https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

ESG Research Report: The Life and Times of Cybersecurity Professionals 2021, Volume V, A Cooperative Research Project by ESG and ISSA; https://www.issa.org/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

(ISC)^2 Cybersecurity Workforce Study, 2021: A Resilient Cybersecurity Profession Charts the Path Forward; https://www.isc2.org/Research/Workforce-Study#

Ponemon Digital Transformation & Cyber Risks study;
https://ponemonsullivanreport.com/2020/07/digital-transformation-cyber-risk-what you-need-to-know-to-stay-safe/

Bussa, Toby et. al., "Market Guide for Managed Detection and Response Services," Gartner, August 26, 2020 - ID G00722909:
https://www.gartner.com/en/documents/3989507/market-guide-for-managed-detection-and-response-services