A CyberTheory Research Report:

The Convergence of Compliance and MSSP/MDR results in a New Service Category: Managed Cybersecurity and Compliance Provider (MCCP)

Published: 15 November 2020 – CT0725740

Advisory Analysts: Chuck Brooks, Kim Green, Don Cox, CISM, Steve King, CISM, CISSP, Kiren Chaudry, Jeff Spivey, CRISC

The Convergence of Compliance and MSSP/MDR results in a New Service Category: Managed Cybersecurity and Compliance Provider (MCCP)

A CyberTheory Trend Insight Report

Published: 15 November 2020 – CT0725740

Advisory Analysts: Chuck Brooks, Kim Green, Don Cox, CISM, Steve King, CISM, CISSP, Kiren Chaudry, Jeff Spivey, CRISC

In an era of increased complexity, advancing threats and technologies, new remote work realities, the dawn of a 5G, 100 times faster network delivery backbone and expanding compliance requirements, CIOs of small and medium businesses should look to MSSP/MDR firms to help them monitor, detect, respond and recover from cyberattacks, while taking advantage of their compliance knowledge and certification capabilities.

Overview.

Two unusual and apparently unrelated trends have emerged during this pandemic:

1) The rapid growth of the MSS (Managed Security Services) market

2) An increased demand for complex compliance

The former has been accelerated by the complexity of today's cybersecurity landscape, the expanding skills gap and increased compliance requirements. The latter comes from the increased compliance load that is now required of every business, regardless of size, to prove that they are in line with a higher levels of cybersecurity capability maturity than in the past.

Companies in every industry sector are now required either by state or federal government decree, or by their customers to demonstrate their ability to defend against cyber-threats and protect their custodial data.

At the same time, most of these businesses, whether SMBs or Mid-cap and Enterprise companies have determined that they cannot or do not wish to manage that process themselves and have turned to external support.

By doing so, they save money, time and avoid delays in contract execution.

A third trend that is beginning to emerge is a new category of managed security known as MCCP for Managed Cybersecurity and Compliance Provider.

An MCCP completes the security puzzle for SMB and Mid-cap companies by adding full compliance to monitoring, cyber threat detection, SOC, forensics and incident response.

Context.

Managed Detection and Response (MDR) has been a hot-growth cybersecurity market for several years now and MDR revenues continued to grow in Q2 this year in spite of some headwinds from the pandemic.

Prior to the pandemic, the global MDR solutions market was projected to expand at a red hot compound annual growth rate (CAGR) of 16.4 percent between 2020 and 2024, with revenues expected to reach US$1.9 billion by 2024.

According to Markets and Markets, the global Managed Security Services market is projected to grow from US$31.6 billion in 2020 to US$46.4 billion by 2025. That’s a compound annual growth rate (CAGR) of 8.0% during the forecast period.

MSSP Alert reports that the overall market will grow roughly 12% to 15% annually through 2025. Near term, the Top 250 MSSPs are expected to grow roughly 15% from 2019 through the end of 2020, according to their research findings published in September 2020.

Whichever report you believe, the market for outsourced security services is going to continue to expand and grow at a fairly robust CAGR of between 8% on the low end to as high as 16% on the upper guidance.

At the same time, the more traditional managed IT services provider (MSP) market serving SMB customers will continue its growth as well, topping 10% CAGR according to ChannelE2E insights.

What does this all mean?

Compounding Complexity.

We believe that the compounding complexity in managing data and cybersecurity has become impossible for all but the best staffed and resourced companies, whether large or small.

According to RSA research, the average number of cybersecurity tools small organizations are using ranges between 15 and 20 tools, medium-sized businesses are using 50 to 60, and large organizations or enterprises are using over 130 tools on average.

We believe that the proliferation of tools inside organizations' cybersecurity environments owes itself to the decades-old Lockheed Martin Cyber Kill Chain, the well-known framework for identifying and preventing attacks.

While it had been a useful tool at one time, it set in motion the prevent and defend cycle that most cybersecurity teams organize around today, giving them too much to manage, and leading them to create discrete, siloed teams and seek technology solutions for each part of the kill chain.

But it's not just about the number of tools organizations have. It's also about each tool's hidden costs, which include the sticker price; the cost for someone to manage it and to make sense of the data coming from it; and the cost for a security operations center, or SOC, to tie it all together.

These three things added together make up the actual cost of product or the total cost of ownership, and are well beyond the reach of most SMBs and even Mid-caps.

Even if they could afford to layer in that many point protections, most companies can neither afford to hire security analysts to chase down all of those alerts, nor attract the kind of talent the market demands at this level.

Modern Cybersecurity Challenges.

For an effective cybersecurity program, an organization needs to coordinate its efforts across the entire information and threat landscape, and in this era, doing so presents an almost impossible challenge for most companies.

Elements of this requirement encompass all of the following:

Network Security: The process of protecting the network from unwanted users, attacks and intrusions. In the COVID-19 world, working from anywhere and being supported by a 'new' software-defined network that casts the Internet as the outward boundary and includes every point of presence in the computing environment, creates broad new challenges for even the most sophisticated networking operations.

Application Security: Apps require constant updates and testing to ensure these programs are secure from attacks. Application security changes constantly.

New threats and attack vectors emerge, and new regulations ramp up compliance requirements. Testing and prevention strategies need to keep up with those changes.

Legacy systems are rarely examined for vulnerabilities, yet all of these were created pre-internet and decades earlier. Long before cybersecurity became a reality.

Attackers like to exploit vulnerabilities in legacy code. When developers reuse code that has been in circulation for decades, they likely and unwittingly inherit its technical debt, which includes security bugs and flaws.

Endpoint Security: Remote access is a necessary part of business, but it is also a weak point for data, now further exaggerated by WFH requirements and expanded threat networks through home routers and insecure applications.

To compound the problem, a multitude of new endpoint devices are accessing the network every day, from Internet of Things (IoT) equipment, printers, smart displays, and sophisticated peripherals, to a variety of Bring Your Own Devices (BYOD) with different operating systems and authentication capabilities.

This landscape is expanding quicker than most data security personnel can respond. In monitored environments, threat alerts are creating response fatigue as reports of incidents are often false positives while false negatives frequently go undetected.

In today's average business environment, the level of security analyst required to manage incident response is simply unavailable.

Data Security: Inside of networks and applications resides data. Protecting company and customer information is a separate layer of security. And in most cases, the challenge is to identify those information assets that need protection, where they reside and how they are protected. The sudden shift to WFH, has created a broad array of opportunities for hackers.

What has not changed, however, is an organization's responsibility to protect data and secure systems to reduce the risk of a breach or unauthorized access to information. The regulatory requirements, and other state and industry standards for protecting information, are as critical as the day they were implemented, if not more so. GDPR, CCPA, NYDFS, PCI DSS, CFIUS, HIPAA, HITRUST, SOX, and so on – still need to be adhered to.

Compliance is an enormous task for even well-resourced organizations and the average Mid-cap or SMB company simply cannot keep up with the requirement.

Identity Management: Essentially, this is a process of understanding the access every individual has in an organization. IT organizations everywhere, from SMBs to Fortune 500 companies, are moving from on-premises software to on-demand, cloud-based services.

As enterprise IT makes this transition to a new hybrid on-demand/on-premises configuration, controlling who is granted access to which applications becomes increasingly important. This presents CIOs and their teams with a whole new set of identity management challenges. In addition, users must keep track of multiple URLs, user names, and passwords to get access to their applications.

Managing Identity challenges is complicated for even the best-managed security teams.

Database and Infrastructure Security: Database security means protecting and securing a database, the database management system software, and the devices upon which they reside from illegitimate use and malicious cyber threats and attacks.

Protecting these devices is critical in the expanded threat environment and smaller businesses cannot keep track of all of their devices and do not know how to defend against newer sophisticated attacks.

Database security procedures are aimed at protecting not just the data from intrusion, misuse of data, and damage, but also protecting the database management system and all the applications that access it.

This requires a multitude of processes, tools and methodologies that are rarely found in the SMB, Mid-cap environment.

Cloud Security: Today's organizations desire the accessibility and flexibility of the cloud, yet these benefits ultimately mean little if the operation is not secure. Protecting data in a 100% online environment presents a number of challenges. And these require sophisticated security teams to assure that servers are configured properly, access rules are applied consistently and a zero-trust mental framework is underlying every consideration.

Support for the big 3 cloud service providers is essential in today's crowded markets and a firm understanding of the shared responsibility model is crucial to getting it right.

Mobile Security: Today, many companies integrate their corporate processes with mobile platforms that support enterprise apps. It is part of the modern remote mobile world. Securing mobile applications and other digital communication channels is imperative, yet most businesses know little about modern security standards and requirements for protecting these devices and their operating systems.

The combination of inadequate or poorly secured Wi-Fi networks and a wide range of vulnerabilities in the connected home, make mobile devices a target for entry points to the corporate system.

More sophistication and complexity yields greater challenges for all.

Incident Response/Disaster Recovery/Business Continuity: In the event of a security incident, businesses must revert to an incident response plan. That plan is a set of instructions to help IT staff detect, respond to, and recover from security incidents and address issues like cybercrime, data loss and service outages that threaten daily work.

IR plans need to be tested throughout the year as if a live event had occurred. This requires time, money and depth of understanding that can create attack scenarios that mimic real life.

Very few businesses of any size have the capability, motivation or discipline to follow this guidance and as a result, when a breach occurs, they are unprepared to recover.

Security Awareness Education: Assuring that a culture of cybersecurity awareness exists in any company is a very difficult process to pull off.

Treating cybersecurity threats as existential requires some tangible evidence that end users can wrap their minds around and because these threats operate in an unseen space, it is difficult for employees and customers alike to recognize the signs of inbound threats like phishing attempts as they occur.

Training employees to recognize the indicators and modify their behavior requires an extensive commitment to awareness training from the top of company leadership on down, and it is rarely accomplished even under this rapidly threatening environment.

Steep Challenge.

The most difficult challenge in cybersecurity is the continually evolving nature of specific security risks themselves. Traditionally, organizations have focused most of their cybersecurity resources on perimeter security to protect their most crucial system components and defend against known threats.

This approach no longer works, as the threats advance and change more quickly than organizations can manage. To combat the threats, advisory organizations promote more proactive and adaptive approaches to cybersecurity.

And, the National Institute of Standards and Technology (NIST) has issued guidelines in its risk assessment framework that encourage a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.

The conundrum is that while this free advice is available to everyone, implementing it requires time, money and trained human resources. The ability to connect the dots between business goals and cybersecurity investment does not exist for most.

Cybersecurity Capability Maturity.

And for the millions of businesses who find themselves somewhere along the supply chain for government contracts, November 30th looms as the deadline to prove compliance with the Department of Defense (DOD) interim rule to strengthen the defense contractor supply chain through implementation of the Cybersecurity Maturity Model Certification (CMMC) framework which will determine the contractors' cybersecurity maturity.

This rule applies to anyone at any level in the supply chain, not just the 300,000 primes, but the millions of sub-primes in 2nd, 3rd and 4th position as well.

The interim rule defines each of the five cybersecurity levels for which contractors may obtain third-party certification, with each level building on the one before.

This requires that contractors must maintain the requisite CMMC level for the duration of the contract; ensure that their subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments; and include the requirements of the CMMC clause in all subcontracts or other contractual instruments.

States Follow Suit.

By October 1, 2025, the DOD will include the CMMC clause in all solicitations above the micro-purchase threshold (including those for task and delivery orders and those for commercial items) except solicitations that are exclusively for commercially available off-the-shelf (COTS) items.

This has broad implications for all businesses, as it essentially sets the first commercial requirement (vs. a guideline) for cybersecurity maturity.

If businesses can't achieve it, they will be prevented from participation. And as recent history demonstrates, commercial standards will follow.

Witness California's adoption of most of the meat from the GDPR regulation along with steeper requirements of their own.

At least 43 states and Puerto Rico introduced or considered close to 300 bills or resolutions that deal significantly with cybersecurity last year. Some of the key areas of legislative activity include:

- Requiring government agencies or businesses to implement training or specific types of security policies and practices
- Creating task forces or commissions
- Restructuring government for improved security
- Studying the use of blockchain for cybersecurity
- Providing for the security of utilities and critical infrastructure
- Exempting cybersecurity operations information from public records laws
- Addressing the security of connected devices
- Regulating cybersecurity within the insurance industry
- Providing funding for improved security measures
- Addressing cybersecurity threats to elections

New Assessment Methodology.

As the DOD phases in the CMMC, contractors subject to DFARS 252.204-7012 will need to obtain a cybersecurity assessment under the newly announced "Assessment Methodology."

This new methodology requires an assessment of the contractor’s implementation and compliance with NIST SP 800-171 at three different levels: Basic, Medium, and High.

A Basic Assessment is based on a contractor’s self-representation of compliance. For both the Medium and High Assessments, the DOD will review the contractor’s system security plan description of how each NIST SP 800–171 requirement is met. Under a High Assessment, the DOD will require a contractor to demonstrate its system security plan.

Demonstrating one’s system cybersecurity plan will be difficult for most. It requires sophisticated attack simulations and penetration testing, combat between red and blue teams, and an ability to immediately restore and recover.

The impact on all businesses is huge. Funding, planning and putting those abilities in place is highly complex, expensive and a C-suite time-sink. Without the recognition of an existential threat, business has refused to acknowledge both the breach realities and the risk.

Convergence of Compliance and MSSP/MDR.

With the increased complexity and cost combined with a concrete requirement to achieve certain levels of cybersecurity maturity, it is easy to see why the market growth in compliance-centric MDR companies has skyrocketed.

In analyzing the components required by a strong provider in this space, MDR and MSSP actors must go beyond the standard functionality of managed security, SOC, detection, and response that characterizes the current market place.

We believe that a new category of definition is required. This new category must demonstrate capabilities in Managed Compliance along with threat defense and protection, and provide those services on a reliable 24/7 clock.

The new category is called MCCP, which stands for Managed Cybersecurity and Compliance Provider.

Representative Vendors.

In examining the providers in today's market, we found ten representative vendors who offer a complete set of industry agreed upon MSSP, MDR and Compliance services.

While not intended to be a list of all the providers in the MCCP services market, many of the market leaders in the SMB and Mid-cap space are represented. This indicates a definite shift toward the inclusion of compliance capabilities.

Abacode

Abacode is a next-generation Managed Cybersecurity & Compliance Provider (MCCP). Leveraging a unified suite of capabilities, their Cyber-Lorica platform delivers a holistic, framework-based MDR/SOC/Compliance cybersecurity program and managed risk. Their unified services platform is designed for ongoing assessment and compliance changes and updates along with continuous cybersecurity monitoring and management.

Alert Logic

Alert Logic's proprietary managed detection and response (MDR) platform and team of security experts deliver outcome-based security by collecting network traffic and more than 60 billion log messages each day, providing coverage across vulnerabilities and attacks by bringing together asset visibility and security analytics for networks, applications, and endpoints in on-premises, hybrid, and cloud environments, and providing compliance services for CMMC.

Arctic Wolf

Arctic Wolf® Managed Detection and Response (MDR) solution provides 24×7 monitoring of customer networks, endpoints, and cloud environments to help detect, respond, and recover from modern cyberattacks, in addition to providing compliance advisory services across a broad spectrum of regulatory frameworks.

Armor

Armor Anywhere delivers audit-ready compliance and cost-effective security and protection through threat detection and response capabilities by integrating and streamlining best-of-breed security tools and processes with cybersecurity expertise. Armor is certified by HITRUST whose framework is designed to simplify HIPAA compliance requirements by providing prescriptive compliance guidelines.

BlackPoint

Blackpoint's MDR service leverages their patented security operations and incident response platform SNAP-Defense, combining network visualization, insider threat monitoring, anti-malware, traffic analysis and endpoint security in one rapidly deployed service that also supports compliance adherence as well as audits and assessments including NIST 800-171, HIPAA, PCI-DSS, NYCRR-500, and ISO/IEC-27001.

Cysiv

Cysiv SOC-as-a-Service is a managed detection and response (MDR) service that also complements an extended detection and response (XDR) solution. In addition, their compliance services extend to SOC 2 Type II and ISO 27001 certification, helping to ensure compliance with key regulations and standards, including GLBA, PCI, HIPAA, CCPA, FedRAMP, and HITRUST.

eSecurity Solutions

eSecurity Solutions provides an end-to-end security solution including risk assessments, regulatory compliance, enterprise-level security products and managed security with MDR. Their solution addresses the top customer problems of compliance, threat detection and response, alongside expert security guidance and support.

eSentire

eSentire's Managed Detection and Response (MDR) service is delivered from their cloud-native XDR platform. It uses patented artificial intelligence to understand the massive volume of real-time security signals coming from their clients' diverse data sources. This unique technology has overcome the data challenge of modern cybersecurity and detects what other solutions miss. Combining this understanding with asset and vulnerability data enables the delivery of protection customized to their customers’ business needs, and they provide compliance consulting services for all regulations.

RSI Security

RSI Security provides a host of managed SOC, threat detection and response services, and as a seasoned QSA (Qualified Security Assessor), ASV (Approved Scanning Vendor), and authorized HITRUST CSF Assessor, their compliance services extend beyond HIPAA, PCS/DSI, FINRA, NYDFS, GDPR and HITECH to include NIST 800-171 and DFARS along with CMMC certification.

Secureworks

Secureworks offers a unique combination of cloud-native, SaaS security platform, intelligence-driven MDR security solutions and compliance advisory through adversarial security testing services for assessments that address logical, physical, technical and non-technical threats, expose gaps, and meet compliance mandates while reducing risk and improving overall security posture.

Recommendations.

As we have outlined above, the market for MDR and Compliance services is expanding rapidly as even larger cap businesses find themselves unable to independently support a myriad of new regulations, often tied to particular industry sectors in addition to imposition at the state and federal government levels.

But companies need to accept the fact that working with an MCCP is not a substitute for owning the foundations of incident response policies and procedures. Many internal functions still need to own their share of these plans which include HR and legal and may not be a part of the MCCP offering.

As we learned from the Capital-One breach, companies should insist upon an incident response retainer, either from their MCCP provider or another third party, for investigations and breaches that go beyond what the MCCP contractually provides. In the case of Capital-One, the Magistrate Judge's order reflects at least one key lesson for companies facing cyber incidents.

To shield a forensic report as a work product, a company must demonstrate that the report would not have been created in essentially the same form absent litigation. This burden is more difficult to meet where the company has a pre-existing relationship with the cybersecurity vendor that prepares the report.

If a company has unique data residency and specific privacy requirements, not all MCCPs at this stage of their evolution may have the compliance skills to support all regulations. Instead of selecting an MCCP on the basis of regulation compliance alone, selecting a provider with a data collection architecture that adheres to specific data residency requirements is the key to a successful choice.

Many SMBs and Mid-Cap companies looking to outsource their cybersecurity management want assurances that the Google Cloud Platform is supported by their managed provider. Based on pricing and foundational security, many smaller companies have chosen GCP over AWS and Azure. Taking advantage of the lower-cost Google cloud security infrastructure makes perfect sense when the investment Google has committed to security is considered.

Google's global scale technical infrastructure is designed to provide security through the entire information processing lifecycle and provides the secure deployment of services, secure storage of data with end-user privacy safeguards, secure communications between services, secure and private communication with customers over the internet, and safe operation by administrators.

Google uses this infrastructure to build its internet services, including both consumer services such as Search, Gmail, and Photos, and enterprise services such as G Suite and Google Cloud Platform.

The security of the infrastructure is designed in progressive layers starting from the physical security of data centers, continuing on to the security of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support operational security.

Google invests heavily in securing its infrastructure with over 500 security engineers dedicated to the GCP, including many who are recognized industry authorities.

It relies on cryptographic authentication and authorization at the application layer for inter-service communication and strong access control at an abstraction level and granularity unprecedented in public cloud platforms.

While we were not able to extend our analysis of the providers we reviewed to determine GCP support, we recommend that managed security service provider evaluations include this capability in the future.

This report reflects the opinions of CyberTheory's research team, and may or may not be interpreted to be statements of fact. The information in this publication has been obtained from reliable sources. CyberTheory disclaims all warranties to the accuracy or completeness of the information. In addition, CyberTheory does not provide legal or investment advice and its research should not be construed or used for those purposes. CyberTheory's research is produced without input or influence from any third party vendors. All contributions to this reporting are voluntary and reflect the opinions and experience of the contributing analysts.