The Best Managed Security providers in the US

When it comes to managed service providers, there is a wide range of services that a company can provide. Typically, smaller companies will specialize in two or three key areas, rather than being stretched too thin. The larger firms will be able to provide services across multiple disciplines. In this article, we will start by reviewing managed service providers that are some of the tops in the industry. These vendors may provide multiple services but not all provide the same types of services. The article will delve into managed detection and response, cloud, and security operations, and then round out some good value vendors that are worth reviewing.

**SecureWorks**

The majority owned by Dell, SecureWorks offers a strong set of services for end clients. With security management, security monitoring, and vulnerability management, SecureWorks has built a strong set of offerings. One caveat to keep in mind is that some of the services will require their tools to be able to provide the service, unlike IBM or Optiv. Even with this, they bring a strong track record of providing high-quality services for organizations across the globe. With some of the largest customers in the world, SecureWorks can be considered a reliable partner to engage for your project.

**Mandiant**

Mandiant was recently purchased by Google which will allow them to continue to grow, not that they really needed help with that. Mandiant comes into the managed services to augment its large portfolio of security offerings. They are known for highly technical services like penetration testing, incident response, and forensic investigations. This has allowed them to build a wide range of security-managed services that can assist their clients with their needs. Like a few of the vendors on this list, Mandiant will have preferred or required technology for services like security operations, endpoint detection, or other services that are reliant upon software to provide the service.

**Optiv**

As one of the largest US-based security companies, Optiv has grown over the years organically and through acquisition and mergers, which has allowed them to build a very robust set of services. Optiv has been able to provide managed services for an extended period, and in many cases, for longer than some companies on this list. Something to keep in mind when working with Optiv is that some of their managed services will require the utilization of a defined set of technology to make it work but not all are this way. For instance, they can do security operations across multiple vendor solutions.

**IBM**

IBM has been around technology for about as long as technology has existed. Well, maybe not that long, but they are the true gray hairs of the industry. Love or hate IBM hardware, software, or security services, there is no denying that IBM possesses a deep experienced pool of consultants to provide services. This allows them to offer a large range of managed services to end customers and, in many cases, at a very high level. Whether your organization utilizes IBM hardware or software, IBM can support your security programs in the areas you may need.

The Best International Managed Security providers

**Darktrace**

Darktrace is based out of the United Kingdom and is one of the youngest companies on this list. They have grown up in the age of cloud-based systems, which has allowed them to build a strong security offering around security detection and response. With their AI-based system that can augment human eyes on glass, Darktrace has been able to build a solution that is affordable and more than capable to detect anomalous activities across your infrastructure and users. While they are more focused on detection, response, and security operations, they are still a strong company to consider outside of the US or within the US.

**Accenture**

Almost everyone knows Accenture for the very broad set of services that they offer. They landed on the international list, as opposed to the US-based list, because they are one of the largest international companies providing consultancy services. This allows Accenture to build a service that meets the client’s needs, regardless of location. While there may be better specialty service providers, the benefit of Accenture is the ability to provide strong services in security or outside of security to help a company potentially gain economy-of-scale discounts.

**Wipro**

With the core of its physical presence in India, Wipro is known for providing security services globally to clients of varying sizes. Wipro provides services that range from managed services for full security programs to individual specialty managed services (like security operations). One of the bigger differentiators for Wipro is its ability to seamlessly integrate into a business and operate in such a way that internal and external contacts are not aware that a third-party is being utilized.

**NTT Data**

NTT is known for providing technical consultants to its clients. While they may not have as broad a portfolio as Optiv, Mandiant, Wipro, or IBM, they do offer deep experience across vulnerability management, threat detection, security operations, and endpoint-managed detection and response. With the ability to support companies that operate in the APAC region, NTT Data is a strong solution provider for a globally positioned or APAC regionally positioned company. With the support of a large company, they also provide stability to their security services for the long term.

Best Managed Detection & Response (MDR) Providers

When it comes to managed detection and response providers, it is important to understand that it is likely that any provider will have a single vendor for the tools with whom they work. This may seem frustrating or not a good business case, but it is advantageous for your business. Having a deep understanding of the tool, the alerts, and the good and bad of the provider allows them to provide strong services and efficient services.

**Sophos**

Like nearly all the providers on this list, Sophos offers a product that is required to be installed on endpoints and the environment to provide their managed service. While this may be the case, they are willing and able to work with existing tools in the environment to help with managing costs, both operational and contract. Add that they offer MDR solutions across email, cloud, network, and endpoints, and they have a robust solution offering that can dramatically increase a company’s security controls.

**Crowdstrike**

Crowdstrike may be best known for being one of the pioneers in the EDR (endpoint detection and response) software space. However, they have transitioned to offering strong MDR and incident response services, due to the capabilities that their tool offers. They may not be the cheapest. In fact, they are often one of the most expensive MDR providers on this list, but they do offer a strong solution that can work regardless of the OS of the system. They can offer cloud, endpoint, service security detection, and response solutions. Add in their strong partner network that can integrate with their software to pull insight, and it truly makes them a leading provider in this space.

**Red Canary**

Red Canary is known for publishing reliable indicators of compromise, open-source tools, and other security knowledge. This helps bring additional clout to their capabilities in providing MDR solutions. With the ability to provide a full enterprise solution that consists of detection, investigation, and response, Red Canary is a company worth evaluating when looking for an MDR solution provider. Like SentinelOne and Crowdstrike, Red Canary brings their software solutions to assist with providing services to your organization, so it is important to engage as part of the EDR tool evaluation exercise.

**SentinelOne**

SentinelOne is very similar to Crowdstrike. Both started out with EDR software and have transitioned into providing MDR solutions. Keep in mind the SentinelOne tends to be a cheaper option than Crowdstrike Falcon, but this does not mean that is lower quality. Testing shows both are very similar in their capabilities. With a strong software solution that will be required to be installed as part of the managed service, SentinelOne is on par with any of the solution providers on this list. One benefit when comparing to some of the other providers on this list is that the SentinelOne agent tends to be a favored software solution for other MDR solution providers that do not have their own tool built. This will provide some flexibility to move your MDR solution provider to another company, if you so choose.

Best Managed Cloud Security Providers

When it comes to reviewing managed service providers for cloud security, it is critical to understand the vendor, which is the core competency of the provider. Not all vendors are able to provide security services across all cloud platforms. Further, it is important to understand how the vendor will be assisting your organization in securing the platform. Is the vendor simply providing services related to security, like architecture review, tool management, or configuration? Or are they providing full cloud management with an eye toward security? Either is valid approach when it comes to cloud security.

**Logicworks**

Logicworks is a cloud consulting company that can provide security services and cloud management services. In many cases, they take on the management of your cloud platform to assist with securing, but that is not the only service that they provide. Logicworks is primarily focused on AWS and Azure cloud service providers, which may limit their ability to help a company with a larger multi-cloud deployment.

**Capgemini**

Capgemini is much like Logicworks and TCS, in that they provide cloud security services that include cloud transition or existing customers. As part of their offerings, they have security assessments, security advisory, and secure cloud configuration. Further, they also offer a 24x7 cloud security operation offering that can quickly mature an organization’s detection and response capabilities.

**HCL Technologies**

HCL offers a broad range of security services but, like all the other vendors on this list, also offers up services to help with transformation projects to the cloud. They not only provide the ability to plan and complete the transformation project in a secure fashion but also offer additional services that can further secure the cloud implementation: from offerings that are focused on architecture, gap assessments, and project management to offerings that will help with vulnerability management and detection. Some of their more mature managed service offerings are related to security operations for cloud and secure infrastructure management services.

**Tata Consultancy Services**

TCS is capable of providing services across Azure, Oracle, and AWS, with some abilities in GCP and IBM cloud. They are extremely experienced with managing cloud deployments and migrations for customers, which includes taking on security for the new tenant. They have a strong offering around build zero-trust rust cloud deployments, specifically in AWS. While they are globally positioned, TCS tends to focus on US and Europe-based organizations.

Best Security Operations Center (SOC) Providers

While many of the vendors that have been discussed previously offer security operation-managed services, the below are some of the best in the space for companies. In many cases, the vendors in this space will require the installation of their tools and services to further help with the detection and response to security events. While this may be frustrating, this allows the company to be deep in its tech stack and allows for better processes and procedures for all clients.

**CyDeres**

Recently purchased by the Herjavec Group, CyDeres offers up a security operations center that is built on top of Google’s Chronicle SIEM solution. Leveraging a modern cloud native SIEM has allowed CyDeres to build a strong service that drastically extends the capabilities of the platform through custom-built detections and response plans. Fully located in the United States, CyDeres offers 24x7 services and extremely quick response times, per contract. Not only do they offer detection services but offer additional services to take on remediation of events for their end clients.

**Artic Wolf**

Artic Wolf, like CyDeres, has a preferred technology stack for its security operations managed services. Not only do they require logs to be pulled into their platform, but they also prefer their clients to run their EDR tool. They are also US based and offer up 24x7 monitoring services and the ability to add on remediation services, as well. To extend their solution out, they offer services that can cover your O365, SaaS, and cloud solutions, which allows for a robust, more holistic approach to your security operations managed service provider.

**Expel**

Expel, like the other two on this list, requires the utilization of their SIEM solution, as part of the service. They do offer the ability to augment internal logging systems with their detection capabilities, but all logs must be exported to Expel. Leveraging a machine learning platform, along with eyes on glass approach, allows Expel to have quick response times and increase the accuracy of detection. Where they excel, like Artic Wolf and CyDeres, is in the ability to help cut down on the amount of false positive alerts in your environment. While they offer up some remediation services, they can be limited compared to what Artic Wolf or CyDeres offer.

The Best Value Managed Security providers

When it comes to best value providers, there are a lot of managed service providers that may come in quite a bit cheaper than the providers on this list. That can leave your organization wondering why they are so much cheaper, which is a valid question. In many cases, you get what you pay for, and for budget security or detection vendors, what you most likely will get is a vendor that throws alerts to your team to triage and remediate. If all your organization is looking for is a tier-one support company, this may be sufficient. However, f you need more, proceed with caution on any vendor that is offering significantly cheaper services.

**SolCyber**

SolCyber lands on this list because of the value add that they provide. SolCyber is truly focused on providing a holistic managed service, with tools included, for startups or small companies. While this has been their primary approach, this does not preclude larger companies from utilizing their services. Their primary focus in helping with managing detection, response, and email security to help meet security requirements related to ISO27001 and SOC2. Further, they have worked a partnership with cyber insurance providers to offer up lower premiums, if their full solution is implemented.

**Huntress**

Huntress offers up a suite of services that range from MDR to threat hunting to security awareness training. While they may not be the cheapest in value providers, they make up for that in their ability to offer great services at an affordable price. With internally built tools layered with highly technical consultants, Huntress is a great partner in further building out an organization’s security capabilities.

**Alert Logic**

Much like Huntress, Alert Logic offers up MDR solutions that are built on top of their internal tools. Offering 24/7 security operation services that is staffed with highly technical experts, Alert Logic is capable of handling billions of log messages per day. They provide the option to engage in security reviews as part of their security operation center to further increase the overall security posture of your organization.