ARTICLE

Top Five Evaluation Criteria for Selecting a Cloud MSSP

SecureWorks®

You've made the decision to move to the public cloud. Congratulations on transforming your organization to become more agile and competitive. After evaluating the bench strength and cloud expertise of your IT and security staff, you also identify the need for third-party expertise to augment your current skills. What evaluation criteria should you consider when selecting a Managed Security Services Provider (MSSP) for the cloud? You need to consider criteria not only today, but also into the future as your cloud transition progresses over time. Use this criteria to select a short list of well-qualified cloud candidates.

Selecting a MSSP for the cloud requires you to assess your current environment and needs, as well as conduct firsthand research about viable alternatives. Many firms have popped up who have rebranded themselves as MSSPs and even cloud-centric MSSPs in order to compensate for the commoditization of hardware and low profit margins. How can you evaluate not only which cloud MSSP is right for your firm, but also ensure that you are putting your trust in the right relationship and team with a proven track record? You can't make the decision lightly regarding business-critical functions like managing your valuable applications, infrastructure and sensitive data.

Organizations large and small have a mix of on-premises infrastructure in their own data centers or server closets plus public cloud workloads. You may be looking for a cloud MSSP that can support such a hybrid IT environment with a seamless experience that simplifies your security. If you've already been using a third-party MSSP, it may be time to evaluate the ROI of your past approach and consider revamping your relationship as you move to the cloud. Cloud computing is about transformation and that includes enhancing your security posture as well.

Here are the top five criteria to consider when selecting a MSSP to manage and monitor your public cloud data and applications.

To evaluate which Managed Security Services Provider is right for your organization, look for the correct balance of security and cloud expertise, grounded in threat intelligence, along with a firm with a proven track record.

Select a Pure Play Cloud MSSP

When evaluating potential MSSPs, look for one whose sole focus is security with a standard offering for managed cloud security. Those who offer security services as a secondary business to their hardware operation, for example, may not have the focus or strategic investment to enhance their MSSP solutions over time or recruit hard-to-find threat experts. You will want to look for a cloud MSSP with a proven track record of at least 10 to 15 years, as well as advanced analytics and large-scale data collection in order to enhance the ability to detect and prevent evasive and persistent attacks. As more and more business-critical data moves to the public cloud, it increases the chance that threat actors will target your cloud workloads.

How many MSSP clients do they protect globally? The larger the client base, the more threat intelligence that can be harnessed to understand the attackers, their motives and their methods. Your cloud MSSP should also be vendor agnostic regarding software applications and virtual servers monitored in the cloud. What customer support and onboarding capabilities are offered?

Select the optimal cloud Managed Security Services Provider that augments your capabilities. This allows your teams to redeploy their time to concentrate on your core business operations and customers.

Financial Stability of the Vendor

You should evaluate the financial strength of all your IT and security vendors, including MSSP providers for cloud. How long have they been in business? If they are a publicly held company, what is their company revenue and profitability? Do you have confidence that they will be in business for many years? Does the cloud MSSP own and manage all of their back-office functions in house?

The last thing you need is a third-party provider with financial difficulties, which could increase your business risk instead of reduce it. Look at the financials of the MSSP function alone if the vendor is not a pure play firm. Evaluate their ability to continue investing and innovating in new services, customer support and tools for their client base.

Financial instability can lead to staff turnover, which can create potential knowledge and service gaps, as well as introduce third-party insider threats.

Advanced Analytics Expertise

Some MSSPs have their own in-house research function that uses advanced analytics to identify patterns and emerging threats from the vast log sources across their global client base. Elite threat researchers then synthesize and turn this data into actionable, predictive intelligence. The objective of advanced analytics and threat intelligence is to provide an early warning on cyber threats to clients.

When evaluating a cloud MSSP, look for an organization that integrates deep threat intelligence into its security platform and processes. Do they have a threat intelligence team? How many people work on it? Do they maintain their own threat intelligence platform, or do they purchase the insights from other firms? MSSPs that leverage their own proprietary technology and analytics can incorporate emerging threat data more rapidly.

A Seamless Experience On-site and in the Cloud

Threat monitoring should be anytime, anywhere with real-time insights and reporting. When evaluating a potential cloud MSSP, consider a managed security solution with a consistent interface for on-premises infrastructure as well as cloud environments. An integrated online client portal provides visibility that reduces complexity with fewer systems and vendors to manage. This “single pane of glass” capability also minimizes the likelihood that you will overlook a threat correlation and provides the ability to detect threats at the earliest stage possible.

When protecting your organization’s sensitive information, you need a solution that mirrors the security of your current environment and takes it to the next level of maturity. Ask a potential cloud MSSP about control and visibility across your own infrastructure and in the cloud that provides comprehensive security. Is the client portal focused on ease-of-use? Does it include compliance reports that can streamline your audits?

Broad Portfolio, Including Remediation

The optimal cloud MSSP should not only offer its own proven security solutions and tools, but also be able to help mitigate any threats that are detected. This remediation capability helps you get back up and running faster in the event of a breach; do not wait until you are in the midst of a data breach to seek out incident response expertise. An end-to-end cloud security portfolio can also grow with you and can help future proof your security investment.

When assessing a potential cloud MSSP, ask about the depth and breadth of solutions offered. Do they offer consulting and professional services capabilities such as the development of a Cybersecurity Incident Response Plan (CIRP)? Do they offer proactive and reactive incident response services in the cloud? Security industry experts now recommend that organizations balance detection with prevention in order to minimize the impact of a breach.

Conclusion

These five objective criteria enable you to evaluate the cloud MSSP that best augments your staff and skills, simplifies your security compliance and protects business-critical information and applications in the cloud. Working with a cloud MSSP isn't just about solving your internal resource challenge; it's a way to optimize your security effectiveness and move to the public cloud with confidence.

For more information, call **877-838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com/cloud