MSSP Buyer’s Guide for Healthcare

CLEARDATA®

Introduction

As a healthcare organization managing sensitive data in the cloud, it's not enough to choose a Managed Security Service Provider (MSSP) that can help you identify cloud risks, vulnerabities, and cyber threats. You need a partner that can step in and remediate them ***for you***.

This guide is designed to help you choose the right MSSP. We'll show you how to secure stakeholder buy-in and budget, develop a selection process, evaluate MSSPs against key criteria, and set KPIs to ensure your selected MSSP partner demonstrates their full value and executes on their goals.

Here's your MSSP buyer's guide for healthcare, complete with the guidance you need to make this critical selection.

TABLE OF CONTENTS

Secure Stakeholder Buy-In & Budget

To secure stakeholder buy-in at all levels, first underscore the current reality of healthcare cyber threats. Tie this context into the importance of selecting an MSSP that not only identifies vulnerabilities, but remediates them, taking this responsibility off of your company's plate. Highlight how this proactive approach minimizes operational disruptions, avoids compliance pitfalls, and reduces long-term costs compared to traditional monitoring-only services.

Understand the Threat Landscape in Healthcare

Healthcare organizations face unique challenges, including ransomware attacks, data breaches, and stringent compliance demands. These risks require an MSSP with the capability to not only identify threats but also resolve them in real-time.

80%

80% of healthcare breaches can be traced back to misconfigurations, reflecting a need for expertise in order to avoid costly errors.

67%

67% of healthcare organizations were hit by ransomware in 2024.

#1

Healthcare is the #1 sector for third-party data breaches, accounting for 58% of data breaches in 2023.

136%

Healthcare cyberattacks surged by 136% in the last year alone.

Source: https://www.prnewswire.com/news-releases/xm-cyber-report-finds-80-of-security-exposures-are-fueled-by-misconfigurations-302136164.html

Know the Value of Choosing the Right MSSP

The ideal MSSP for healthcare will become your proactive partner for managing security operations, offering services that go beyond monitoring to include complete resolution of incidents on your behalf.

An MSSP acts as an extension of your team—one that identifies threats and handles remediation directly, ensuring your internal focus stays on delivering quality healthcare. A best-fit MSSP simplifies your cybersecurity while empowering your team to focus on mission-critical goals.

MSSPs are particularly valuable for healthcare organizations because they provide continuous protection, advanced threat detection, and incident response—all while ensuring compliance with strict regulations like HIPAA and HITRUST.

Not all MSSPs are built the same, though. Healthcare-specific MSSPs understand the unique demands of the industry. From securing electronic health records (EHR) to ensuring compliance with the latest healthcare regulations, they specialize in both preventive and responsive measures that help keep your organization safe.

A skilled MSSP can handle the day-to-day cybersecurity needs of your organization, working both proactively to prevent threats and reactively to resolve incidents. As a result, your internal team is freed from time-consuming security tasks, allowing them to focus on core business objectives. This reduces the need for additional in-house staffing and helps boost productivity across departments, as your internal teams can direct their efforts toward patient care and other mission-critical tasks.

Healthcare-Specific MSSP Services:

- ✓ **Threat Detection:** Around-the-clock monitoring to detect suspicious activity before it becomes a problem.
- ✓ **Incident Remediation:** Rapid action to contain and remediate threats, ensuring that your systems remain secure.
- ✓ **Compliance Support:** Simplified auditing and continuous compliance with healthcare regulations like HIPAA, HITRUST, and GDPR.

Addressing Common Pushback from Stakeholders

When discussing MSSPs with internal stakeholders who may still have hesitations about engaging a new technology partner, here are some common concerns and how you can address them effectively:

- **"Isn't it better to handle cybersecurity in-house?"**
  While in-house teams are beneficial, managing around-the-clock cybersecurity in an industry as high-risk as healthcare requires a highly specialized skill set, extensive resources, constant monitoring, and the ability to swiftly remediate threats. MSSPs provide this level of focus and expertise, which may be challenging to maintain internally without significantly increasing costs and staffing.

- **"What about the cost?"**
  It's understandable to weigh the costs of any new technology partner. However, the cost of MSSP services is often lower than the financial and reputational losses associated with a breach. MSSPs bring long-term value by reducing breach risk, managing compliance, and increasing operational efficiency.

- **"How can we trust an external partner with sensitive data?"**
  MSSPs specializing in healthcare have strict data security protocols and healthcare-specific certifications, like HITRUST and HIPAA, that meet the highest standards of patient data protection.

MSSPs free your internal teams to focus on core healthcare missions, reducing burnout and enhancing productivity.

What Could Happen Without an MSSP?

Failing to partner with an MSSP that offers comprehensive remediation puts your organization at risk of catastrophic consequences. Operational downtime can stretch from hours to months. Compliance gaps may become costly to fix retroactively. Because internal teams are ill-equipped to handle evolving threats without an MSSP that remediates incidents immediately, preventing long-term damage.

The average cost of a data breach in healthcare is $9.77M: These expenses are a result of recovery efforts, regulatory fines, and reputational damage.

+ + =

$9.77M

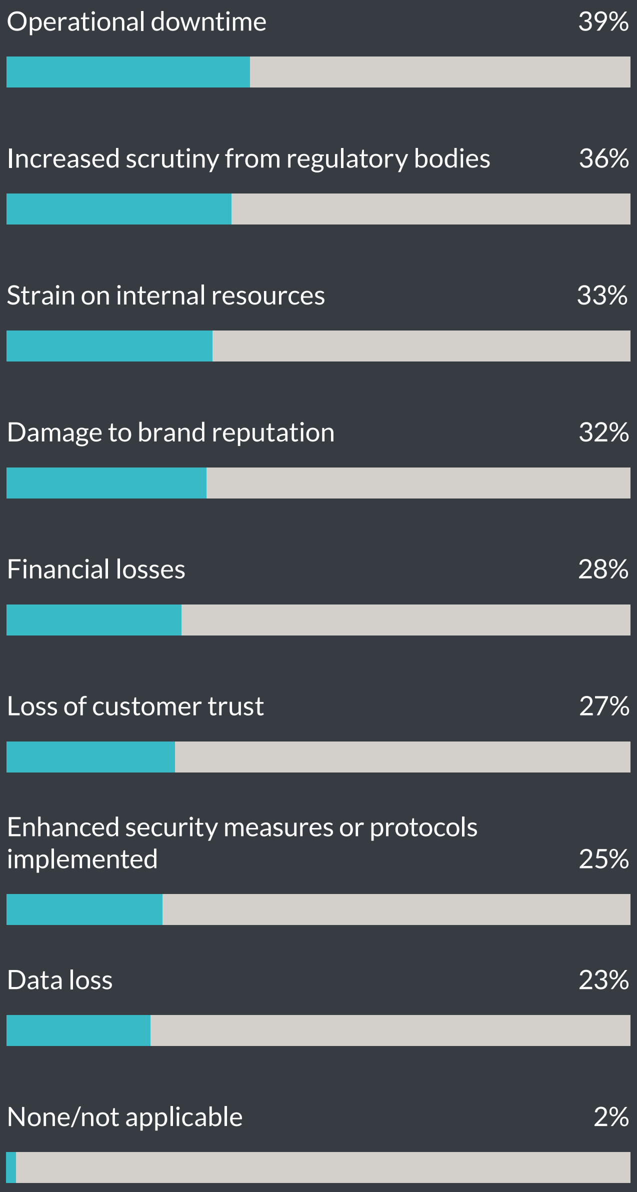
Breaches can also cause long-term disruptions to operations: In many cases, recovering from a breach takes months of resource-intensive work. When these incidents involve patient data, the stakes are even higher. For example, in a worst-case scenario, a hospital could be locked out of its system during a ransomware attack, forcing it to turn away patients or revert to paper-based processes.

When a breach occurs, patient safety is immediately at risk: Hospitals may be forced to revert to manual operations, delaying critical care and increasing the likelihood of errors. In a sector where every second counts, healthcare organizations need a partner who can identify threats early and take action fast.

Managing cybersecurity in-house can strain internal teams: Managing cybersecurity in-house, particularly within healthcare, requires constant vigilance, specialized skills, and a considerable time investment. Internal teams can quickly become overwhelmed, leading to productivity loss and, over time, even burnout.

The Value Lost Without an MSSP

What were the most significant impacts your organization experienced due to cloud misconfigurations?



Base: Respondents with cloud misconfigurations (n=142). Multiple answers allowed.

The longer you wait to secure your organization, the greater the risk. Protecting your infrastructure with an MSSP ensures that you avoid these crippling costs and maintain the trust of your patients.

Spell Out the Benefits MSSPs Provide

The right MSSP doesn't just monitor threats; it eliminates them at the source. Benefits of engaging an MSSP with strong remediation capabilities include:

1 **Proactive Threat Detection & Resolution**
One of the biggest benefits of working with an MSSP is the ability to detect, mitigate, and respond to threats before they escalate. Sophisticated security teams use the latest tools to monitor your systems 24/7, providing real-time insights that help stop attacks in their tracks. And, the right MSSP will act quickly to remediate them on your behalf.

2 **Continuous Compliance and Audit Readiness**
With constantly changing regulations, staying compliant can feel like an uphill battle. MSSPs automate compliance processes, providing audit readiness at all times. ClearDATA's platform, for example, simplifies compliance with built-in safeguards for HIPAA, HITRUST, and GDPR, so that your organization will always have a pulse on compliance and what needs to be done in the case that you're no longer compliant.

3 **Scalability**
As your organization grows, so do your security needs. MSSPs provide the ability to scale security measures quickly and efficiently, ensuring that your protection grows along with your infrastructure.

4 **Reduced Operational Overhead**
Rather than investing in an expensive in-house security team, MSSPs offer access to specialized healthcare security experts at a fraction of the cost. This means that your internal IT team can focus on improving operations, while the MSSP handles the complex, evolving world of security.

Present the Financial Incentives of Using an MSSP

Investing in an MSSP with remediation expertise translates into significant financial savings and operational resilience. Highlight that the cost of breach recovery—including downtime, fines, and reputational damage—far exceeds the expense of partnering with a remediation-focused MSSP.

Additionally, MSSPs can optimize IT budgets by consolidating redundant subscriptions or systems while preventing the costs of staffing in-house remediation teams.

Below is some of the financial information you should include in your presentation:

Long-term Savings

When pitching an MSSP to stakeholders, it's essential to frame the investment as a strategic move that offers significant financial benefits over time. To do this effectively, follow these actionable tips:

- **Highlight the Cost of Inaction:** Start by presenting data on the financial impact of potential cybersecurity incidents. Use industry statistics or case studies to show the average cost of data breaches, regulatory fines, and downtime. Emphasize that the expense of not investing in an MSSP far exceeds the cost of the service itself. This approach helps stakeholders see the investment as a necessary measure to avoid larger financial losses.

- **Calculate Potential ROI:** Make your case stronger by providing a rough estimate of the expected return on investment (ROI). Illustrate how an MSSP could lead to savings on remediation, compliance management, and liability insurance premiums. If possible, show examples of organizations that achieved significant cost reductions after implementing an MSSP, to demonstrate tangible results.

- **Present Value Beyond Security:** Emphasize that an MSSP offers more than just security protection—it also frees up internal resources. Quantify the value of time saved for your IT and security teams, which can then be redirected towards projects that drive revenue or innovation. This way, the investment isn't just seen as a cost but as a way to enable growth and productivity.

Allocating the Budget for an MSSP

Even if leadership recognizes the value, budget constraints can still pose a barrier. Here's how to frame the conversation around reallocating funds to make room for an MSSP:

- **Reevaluate Existing Tools and Subscriptions:** Conduct an audit of your current tech stack to identify underused or redundant tools that can be phased out or consolidated. Present a plan to reallocate these savings toward the MSSP, demonstrating a commitment to optimizing the budget. This approach shows stakeholders you're not just asking for more funds but actively finding ways to finance the investment.

- **Leverage Existing Budget Lines:** Sometimes, the funds can be found within existing budget lines. For instance, if there are separate allocations for compliance, risk management, or IT consulting, consider how these could be consolidated under the MSSP's broader umbrella. Show how this shift in allocation could actually streamline spending, while still covering essential needs.

- **Consider Staffing Adjustments:** If your organization currently employs a full-time security team, explore the potential cost benefits of supplementing or even partially replacing these roles with managed services. While this might be a sensitive topic, positioning the MSSP as a way to enhance—not eliminate—the internal team can help you make the case. It may free your team to work on more strategic initiatives, thereby maximizing the existing investment in staff.

What to Look for in an MSSP

Alignment on your vendor selection process is a key step in choosing an MSSP partner. The following sections provide actionable tips on aligning evaluation criteria, choosing the right process for assessing MSSPs, and creating a comprehensive evaluation checklist.

Align on Criteria

Before beginning the evaluation process, align your team on the priority of selecting an MSSP equipped with remediation expertise. Identify shared goals, such as reducing downtime or ensuring compliance, and develop a unified understanding of what "success" means in an MSSP partnership.

Security and Remediation Capabilities

- ✓ Advanced threat detection and incident response
- ✓ Automated threat remediation
- ✓ Comprehensive response protocols
- ✓ Endpoint protection and network monitoring
- ✓ Vulnerability management and regular security assessments
- ✓ Data encryption and secure backup solutions

Compliance and Regulatory Support

- ✓ Familiarity with industry-specific regulations (e.g., HIPAA, GDPR, CCPA)
- ✓ Ability to support audits and provide necessary compliance documentation
- ✓ Regular updates on compliance changes and regulatory requirements

Service Level Agreements (SLAs)

- ✓ Guaranteed response times for various levels of incidents (e.g., critical, high, medium)
- ✓ Uptime guarantees and system availability
- ✓ Specific resolution time commitments

Reporting and Visibility

- ✓ Access to real-time monitoring and alerts
- ✓ Comprehensive monthly or quarterly security reports
- ✓ Customizable dashboards to track key metrics

Scalability and Flexibility

- ✓ Service packages that can expand as the organization grows
- ✓ Ability to customize services based on specific needs
- ✓ Options for both short-term projects and long-term engagements

Customer Support and Account Management

- ✓ 24/7 support availability and clear escalation paths
- ✓ Dedicated account management
- ✓ Support for onboarding and training internal teams

Reputation and Industry Experience

- ✓ Positive case studies and customer testimonials
- ✓ Recognition from industry analysts or third-party cybersecurity firms
- ✓ Proven managed security services experience

Healthcare-Specific Expertise

- ✓ Extensive experience in healthcare security and compliance
- ✓ In-depth understanding of healthcare-specific threats and vulnerabilities

Proactive Security Measures

- ✓ Emphasis on threat prevention through continuous monitoring and threat intelligence
- ✓ Implementation of advanced security protocols to detect and neutralize threats early

Integration with Existing Systems

- ✓ Seamless integration with current infrastructure
- ✓ Minimal disruption to operations during implementation

MTTI (Mean Time to Identify) and MTTR (Mean Time to Respond)

- ✓ Rapid identification of threats to minimize potential damage
- ✓ Fast containment and resolution of incidents
- ✓ Continuous improvement of response times through automation and expert analysis

Choose Your Evaluation Process

Selecting the right process for evaluating MSSPs will streamline your decision-making.

Request for Proposals (RFP)

An RFP can help you gather detailed information from multiple MSSPs. Include specific questions that address your key criteria (like the list above).

Interviews

Prepare a list of essential questions, such as:

Automated Threat Remediation

Describe your automated processes for identifying and remediating threats?

How quickly can your automated tools neutralize threats once detected?

Incident Response and Recovery

Can you describe your process for incident remediation from detection to recovery?

How do you ensure minimal operational disruption during remediation efforts?

Comprehensive Threat Intelligence

What threat intelligence tools or strategies do you use to anticipate potential risks?

How do you incorporate external risk data (e.g., industry-wide threats) into remediation strategies?

Compliance Gap Remediation

How do your services address compliance gaps that arise during audits or assessments?

What support do you offer to ensure regulatory requirements like HIPAA or HITRUST are met?

Real-Time Vulnerability Patching

How quickly can you identify and patch vulnerabilities once they are discovered?

How do you prioritize vulnerabilities that pose the highest risk to a healthcare organization?

Testing and Validation

Do you conduct regular penetration testing or vulnerability assessments to validate your remediation efforts?

How do you ensure that the issues you resolve stay remediated and do not recur due to systemic flaws?

Case Studies and Customer Testimonials

Look for case studies that highlight similar industries or challenges to your own. This can provide insight into how the MSSP performs in real-world scenarios and the outcomes you can expect. Customer testimonials and third-party reviews can also add valuable perspective.

Evaluate MSSPs

Use this checklist template to make sure the MSSPs you're evaluating have advanced threat detection, protection, and response and remediation capabilities.

Security Capabilities

- ✓ Advanced threat detection
- ✓ Incident response and automated remediation
- ✓ Endpoint protection
- ✓ Network monitoring

Compliance and Regulatory Support

- ✓ Familiarity with industry-specific regulations (e.g., HIPAA, GDPR)
- ✓ Audit support
- ✓ Compliance documentation

Service Level Agreements (SLAs)

- ✓ Guaranteed response times
- ✓ Uptime commitments
- ✓ Resolution time standards

Reporting and Visibility

- ✓ Real-time monitoring
- ✓ Customizable dashboards
- ✓ Comprehensive security reports

Scalability and Flexibility

- ✓ Service packages that accommodate growth and offer customization options

Customer Support and Account Management

- ✓ 24/7 availability
- ✓ Dedicated account management
- ✓ Onboarding support

Reputation and Industry Experience

- ✓ Positive case studies
- ✓ Industry recognition, such as inclusion in Gartner's Magic Quadrant
- ✓ Expertise in managed security services, such as the AWS MSSP Competency

Cost and Pricing Structure

- ✓ Ensure the provider outlines all costs upfront, including any variable fees or package options, to fit your organization's needs and budget.

Healthcare-Specific Expertise

- ✓ Experience in healthcare security and compliance
- ✓ Understanding of healthcare threats

Proactive Security Measures

- ✓ Threat prevention through continuous monitoring

Integration with Existing Systems

- ✓ Can seamlessly integrate with current infrastructure
- ✓ Minimal disruption to operations during implementation
- ✓ Compatibility with existing tools and platforms

MTTI and MTTR

- ✓ Rapid threat identification (ideally within minutes or hours, at most)
- ✓ Fast incident containment and resolution (typically targeting containment within hours and full resolution within 24 to 48 hours)
- ✓ Continually improving response times

For healthcare organizations, rapid response is critical. Look for MSSPs with industry-standard MTTI (minutes) and MTTR (hours to 24 hours) times.

Create MSSP Partner Success Metrics

To ensure your MSSP investment delivers ongoing value, it's essential to track relevant KPIs, build comprehensive reports, and regularly communicate the results to stakeholders. Below, we've laid out the steps for how you can properly show the value of your MSSP investment.

Know What KPIs to Track

Monitoring the right KPIs helps measure the performance and impact of your MSSP. Here are some key metrics to focus on:

Incident Response Times

Track the average time taken to detect, respond to, and resolve security incidents. Faster response times indicate a more effective MSSP.

Number of Security Incidents Prevented or Remediated

Measure how many incidents have been prevented due to proactive monitoring or how many incidents have been remediated before causing significant damage.

Compliance Metrics

Monitor compliance status across relevant regulations (e.g., HIPAA, GDPR) and measure the MSSP's role in ensuring that compliance requirements are consistently met.

Cost Savings from Incident Prevention

Estimate the potential costs saved by avoiding breaches, fines, or downtime. This can be done by comparing the number of incidents and their severity before and after engaging the MSSP.

Uptime and System Availability

Track the percentage of uptime and any disruptions that may have been prevented or minimized by the MSSP.

User Satisfaction Scores

Collect feedback from internal users regarding the MSSP's performance and the ease of working with them.

Build a Report of Your KPIs

Creating a clear, comprehensive report allows stakeholders to see the value of the MSSP investment. Follow these steps to build an effective report:

Organize KPIs by Category

Group your KPIs under categories such as "Incident Response," "Compliance," and "Cost Savings" to make the report easier to follow.

Include Both Quantitative and Qualitative Data

Combine hard numbers with real-world examples or case studies. For instance, if a rapid incident response prevented a potential breach, include the details to highlight the MSSP's impact.

Use Visuals for Clarity

Add charts, graphs, and tables to represent trends and compare before-and-after scenarios. Visuals make the data more digestible and emphasize key takeaways.

Track Progress Over Time

Show trends by including data from multiple time periods (e.g., quarterly, annually). Tracking progress over time helps stakeholders see whether the MSSP is driving consistent improvement.

Provide Actionable Insights

Highlight areas where the MSSP is performing well and identify opportunities for further improvement. Offer recommendations on optimizing or expanding services based on the data.

Report Back on the Success of the MSSP Investment

Regularly communicating the results of your MSSP investment helps justify its continuation and secure ongoing stakeholder support. Here's how to do it effectively:

Schedule Regular Review Meetings

Present the KPI report to stakeholders at regular intervals (e.g., quarterly or bi-annually). Use these meetings to review performance, discuss challenges, and address any concerns.

Tie Results to Business Goals

Link the MSSP's impact directly to broader business objectives, such as reducing costs, ensuring compliance, or protecting customer data. This helps demonstrate the MSSP's strategic value.

Address Any Performance Gaps

If certain KPIs are falling short, explain the underlying causes and outline a plan for improvement. This shows stakeholders that you're proactive in addressing issues and maintaining the investment's effectiveness.

Reinforce the Case for Continued Investment

Use the report's findings to reiterate the value of the MSSP. Emphasize cost savings, reduced risks, and improvements in compliance to demonstrate why ongoing investment is necessary for the organization's security and growth.

An ideal MSSP for healthcare will showcase clear results and in-depth reporting, from the number of threats remediated to root cause analysis and tailored intelligence, helping prevent future incidents.

Take the Next Step: Invest in Your MSSP Partner for Healthcare

As the only healthcare-specific cloud provider with an AWS MSSP Level 1 Competency, ClearDATA is the trusted MSSP for healthcare's advanced threat protection, detection, and response and remediation. We're here to take healthcare cloud security and compliance off of your plate. Unlike MSSPs who just offer security advice, we take prioritized actions for you—and you'll always know what we're doing and when.

So now that you're armed and ready to choose an MSSP for your healthcare organization, take the next step.

Meet with our MSSP team today for tailored recommendations and a look inside our CyberHealth™ Platform and managed security services.

Why exhaust your in-house team with prevention, detection, and response when you can count on the experts.

Set up a time and we'll discuss what our MSSP services can do for you.

LET'S TALK

As a healthcare-specialized MSSP, ClearDATA provides:

- ✓ Proactive Threat Management: Through 24/7 monitoring and detection, ClearDATA's team helps prevent breaches before they happen.
- ✓ Threats Remediated & Neutralized: Respond and recover from cyber threats up to five times faster compared to doing it on your own.
- ✓ Continuous Cloud Compliance: ClearDATA ensures that your organization remains compliant with healthcare regulations at all times.
- ✓ Multi-Cloud Expertise: Whether you're using AWS, Azure, or Google Cloud, ClearDATA manages your security so you can focus on delivering patient care.

CLEARDATA®