MSP vs. MSSP

Understanding the Difference — and Why You Need Both

CloudWave

Healthcare organizations face a dual mandate: keep clinical systems running smoothly and defend them against increasingly sophisticated cyber threats. A Managed Service Provider (MSP) and a Managed Security Service Provider (MSSP) each bring distinct, essential capabilities to the table. When they work together, they create a unified technology environment that is both operationally efficient and security-hardened.

WHAT IS AN MSP?

A Managed Service Provider (MSP) is your technology operations partner. MSPs take ownership of day-to-day IT infrastructure management, ensuring that networks stay connected, systems stay updated, and end users stay productive. They serve as your outsourced IT department — or an extension of your existing one.

Typical MSP services include: help desk and end-user support, server and workstation management, network administration, cloud infrastructure management, backup and disaster recovery, software licensing and procurement, and patch management.

For healthcare organizations, MSPs are the team that keeps your EHR accessible, your clinical workstations running, and your staff connected across every department and facility.

WHAT IS AN MSSP?

A Managed Security Service Provider (MSSP) is your cybersecurity operations partner. MSSPs focus exclusively on protecting your organization from threats, managing your security technology stack, and ensuring your defenses evolve as the threat landscape changes.

Typical MSSP services include: 24/7 Security Operations Center (SOC) monitoring, SIEM management and log analysis, Endpoint Detection and Response (EDR/MDR), vulnerability management and penetration testing, incident response and forensic investigation, security risk assessments and compliance advisory, and virtual CISO (vCISO) strategic guidance.

For healthcare organizations, MSSPs are the team that detects ransomware before it encrypts your systems, ensures your HIPAA security posture is audit-ready, and responds to incidents with an understanding that patient safety is always the top priority.

SIDE-BY-SIDE COMPARISON

Capability	MSP	MSSP
Primary Focus	IT infrastructure uptime, performance, and end-user productivity	Threat detection, incident response, and security posture management
Core Services	Help desk, network management, patching, backup & disaster recovery	SIEM/SOC, EDR/MDR, vulnerability management, penetration testing
Monitoring	System health, availability, and performance metrics	Security events, threat intelligence, anomalous behavior
Staffing Expertise	Network engineers, sysadmins, cloud architects	Security analysts, threat hunters, incident responders, compliance specialists
Compliance Role	Supports IT controls and documentation	Leads security risk assessments, audit preparation, and regulatory alignment
Incident Response	Break/fix, system restoration, disaster recovery	Threat containment, forensic investigation, remediation guidance
Operational Hours	Typically business hours with on-call support	24/7/365 security monitoring and alerting

THE KEY DISTINCTION

An **MSP** asks: "Is the system up and performing?" An **MSSP** asks: "Is the system secure and defended?"
Both questions must be answered "yes" for a healthcare organization to deliver safe, uninterrupted patient care.

WHY HEALTHCARE ORGANIZATIONS NEED BOTH

Many healthcare organizations assume their MSP handles security, or that their MSSP will keep systems running. In reality, these are fundamentally different disciplines requiring different tools, processes, and expertise. Here's why a combined approach matters:

Uptime without security is a liability. A perfectly running network with no security monitoring is an open invitation to threat actors. Healthcare data is among the most valuable on the dark web, and unmonitored systems are low-hanging fruit for attackers.

Security without operational context creates blind spots. An MSSP that doesn't understand your IT environment — your network topology, your clinical applications, your change management processes — will generate excessive false positives, miss contextual threats, and struggle to respond effectively during incidents.

Compliance demands both. Regulatory frameworks like HIPAA, HITRUST, and state-level privacy laws require both operational controls (backup, access management, system hardening) and security controls (monitoring, risk assessment, incident response). Neither an MSP nor an MSSP alone can cover the full spectrum.

Incident response requires coordinated action. When a ransomware attack hits, the MSSP leads the investigation and containment while the MSP handles system isolation, backup restoration, and infrastructure rebuilding. Without both partners working in concert, recovery time extends from days to weeks.

THE PARTNERSHIP MODEL: HOW MSPS AND MSSPS WORK TOGETHER

The most effective approach treats the MSP and MSSP as complementary partners with clearly defined roles and integrated workflows. Here's how responsibilities typically align:

Domain	MSP Responsibility	MSSP Responsibility
Endpoint Protection	Deploys and manages endpoint agents across all devices	Monitors EDR/MDR telemetry, investigates alerts, and drives threat response
Patch Management	Tests and deploys patches on schedule; manages reboots and rollbacks	Identifies critical vulnerabilities requiring emergency patching; validates remediation
Network Security	Configures and maintains firewalls, VPNs, and network segmentation	Analyzes network traffic for threats; tunes firewall rules based on threat intel
Identity & Access	Manages Active Directory, SSO, MFA deployment, and user provisioning	Monitors for compromised credentials, privilege escalation, and access anomalies
Incident Response	Isolates affected systems, restores from backup, rebuilds infrastructure	Leads investigation, performs forensics, coordinates containment and eradication
Compliance	Implements technical controls and maintains IT documentation	Conducts risk assessments, maps controls to regulatory frameworks, prepares for audits

WHAT TO LOOK FOR IN AN MSSP PARTNER

Not all MSSPs are created equal — especially when it comes to healthcare. When evaluating an MSSP to complement your MSP, prioritize the following:

Healthcare specialization. Your MSSP should understand clinical workflows, medical device ecosystems, EHR environments, and the regulatory landscape specific to healthcare. Generic cybersecurity firms often lack the context needed to protect patient care environments without disrupting operations.

Proven MSP collaboration model. Ask how the MSSP works with existing IT teams and MSPs. Look for defined integration points, shared escalation procedures, and a willingness to operate as a true partner rather than a siloed vendor.

24/7 SOC with healthcare context. Round-the-clock monitoring is table stakes. What matters is whether the analysts behind the screens understand the difference between a normal HL7 interface spike and a genuine data exfiltration attempt.

Remediation, not just detection. Many MSSPs will tell you there's a problem. The best ones help you fix it — with remediation services that account for clinical system dependencies and patient safety considerations.

Advisory depth. Beyond day-to-day monitoring, your MSSP should offer strategic services like vCISO guidance, board-level reporting, tabletop exercises, and long-term security roadmap development.

THE BOTTOM LINE

Your **MSP** keeps your technology running. Your **MSSP** keeps it safe. Together, they form a complete technology partnership that protects both your operations and your patients. In healthcare, you can't afford to choose just one.