SECNAP
NETWORK SECURITY

The MSP's Guide:

Successfully Securing the Small to Mid-Sized Market

Offer affordable cybersecurity services that are effectively securing client data while helping to facilitate compliance.

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM/PARTNERS

Recent Changes to Cybersecurity Landscape for SMBs

Cloud computing has created many new opportunities for small and medium-sized businesses (SMBs), but it also left the door open to the same highly sophisticated, targeted cyberattacks that once plagued only large enterprises.[1] The COVID-19 pandemic greatly accelerated this trend.

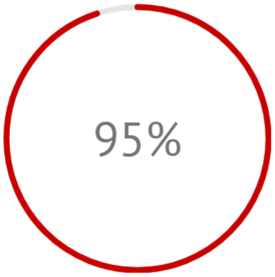
Since the pandemic began, U.S. SMBs have reported:

- **63%** increase in phishing/social engineering attacks
- **52%** saw more cases of credential theft
- **50%** reported an increase in account takeover attacks[2]

Providing Technology Services to SMBs

Cybercriminals also have been infiltrating managed service providers (MSPs) and using those footholds to leverage access to the MSP's customers, with potentially dangerous results for both the MSP and their customer base.[3] Large enterprises are able to maintain robust and expensive cybersecurity defenses that are highly effective at preventing breaches and other cyberattacks.

In contrast, many SMBs have only basic cybersecurity defenses in place, such as antivirus software, identity access management (IAM) solutions, and firewalls. Some SMBs lack even these basics. As a result, MSPs that serve these "middle market" clients are under increasing pressure to provide more robust cybersecurity solutions and expertise. Ninety-five percent of MSPs now have clients requesting help with their cybersecurity, and two-thirds of MSPs have clients requesting assistance with compliance.[4]



Ninety-five percent of MSPs now have clients requesting help with their cybersecurity.

[1] https://www.zdnet.com/article/smbs-see-cyberattacks-that-rhyme-with-large-enterprises-due-to-cloud-shift/
[2] https://www.keepersecurity.com/en_GB/ponemon2020.html
[3] https://assets.documentcloud.org/documents/6980788/US-Secret-Service-PIN-on-MSP-attacks.pdf

Protect Your Business to Protect Your Clients

In addition to handling their clients' security issues, MSPs are struggling to manage their own. By the nature of their business, MSPs have high-level remote IT access privileges to multiple organizations. Thus by breaching just one MSP, cybercriminals gain access to dozens, even hundreds of other companies. For this reason, cybercriminals are increasingly targeting MSPs directly. Based on security assessments performed by our Security Operations Center (SOC), we are seeing that organizations are more vulnerable to high and critical vulnerabilities than they were a year ago. In 2019, at least 13 MSPs were used to deploy ransomware on their clients' systems.[4]

Managing Multiple Security Vendors

As MSPs who serve small and mid-market enterprises pivot towards offering enhanced security services, many attempt to build comprehensive security stacks. Unfortunately, this means purchasing multiple solutions from disparate vendors whose products are not designed to integrate with each other. In a typical scenario, the MSP adds new vendors to satisfy the needs of only one or two clients and quickly ends up managing five to seven different security vendors.

Pricing of cybersecurity services and maintaining reasonable profit margins becomes extremely difficult due to involving multiple vendors with too many unknowns. The MSP quickly becomes mired in an unsustainable situation where it is suffering alert fatigue from tracking outputs from many different security products. Lacking a single pane of glass for easy viewing of event and log data from multiple devices in one place, the MSP must monitor solutions from multiple different vendors, all with separate user interfaces, adding to the number of tickets and systems the MSP's team needs to track and be responsible for.

Piecemealing together a security solution from different vendors can be difficult to manage and therefore ineffective.

SIEM Monitoring Alert Fatigue

MSPs often attempt to mitigate alert fatigue by sending logs from multiple security devices into a SIEM. As technology providers implement SIEM services on multiple clients, it becomes complex and expensive. Profit margins decrease when SIEM management requires higher skilled engineers to perform 24/7 monitoring.

Outsourced Monitoring Only

Another common avenue MSPs take would be to outsource the SIEM monitoring to third-party SOC adding additional expense. Many vendors who provide SOC monitoring often outsource to offshore call-centers in order to keep their margins profitable thus raising the possibility of regulatory issues for you and your clients.

[4] https://www.zdnet.com/article/at-least-13-managed-service-providers-were-used-to-push-ransomware-this-year/

When Solutions Cause Problems

MSPs must also contend with the aftermath of supply-chain attacks on their security vendors, such as the coordinated zero-day attack on network device manufacturer SonicWall, disclosed in early 2021. Notably, SonicWall was at least the fifth large company to report a sophisticated attack on its systems within a relatively short time frame. The other targets included Microsoft, network management tool provider SolarWinds, FireEye, and Malwarebytes.

When a supply chain breach occurs, the MSP's vendors may point fingers at each other and pass the buck to the MSP. Since the MSP is responsible for the direct business relationship with the client, the MSP's reputation will be damaged in any event.

MSPs need a unified, integrated, multi-layered security stack that is fully managed yet affordable to clients of any size.

CloudJacketX Empowers Technology Providers

SECNAP understands the unique challenges MSPs are encountering as they adjust their business models to include cybersecurity services in response to changing client demand. Our CloudJacketX security platform was built on the premise that comprehensive security solutions need to be available to SMBs and middle-market companies for a reasonable price. SECNAP offers service pricing that scales with the size of your clients and allows SMBs and mid-market companies to afford an industry-leading enterprise security solution.

SECNAP's patent and patent pending technology is developed in-house by our US based development team which keeps our costs down. This allows for tight integration between our developers and security analysts, resulting in rapid and ongoing service enhancements and improvements. Our partners enjoy a higher recurring revenue stream with no upfront investment or minimum sales requirement.

Intrusion Prevention System

Intrusion Detection System

Security Information and Event Management

Internal Threat Detection

Lateral Threat Detection*

Vulnerability Management

Endpoint Detection

Data Loss Prevention

Managed 24/7 by
Security Operations Center

Managed Cybersecurity Layers

MDR services that include an intrusion detection system (IDS), intrusion prevention system (IPS), internal threat detection (ITD), lateral threat detection (LTD), and data loss prevention (DLP) technologies help mitigate today's threat landscape. The SonicWall and SolarWinds attacks, which took advantage of zero-day exploits, are perfect examples of where MDR, IPS/IDS, and LTD would have prevented the cyber attacks and saved networks and significant clients from suffering major losses. CloudJacketX is a flexible security-as-a-service platform that allows for a layered approach where clients can choose from only the service modules they need including:

Detection and Prevention Technology works in-line and passively to actively detect and block based on severity, source, reputation, geography, custom tuning, advanced heuristics, and deep packet inspection.

Internal Threat Detection is designed to mimic legitimate services, such as servers and file shares, in order to attract and detect unauthorized access, which provides effective protection against Advanced Persistent Threats, Ransomware, and Insider Threats.

Lateral Threat Detection help stops the spread of internal infection throughout your network by allowing our SOC to detect threats as they attempt to spread between hosts and working locations.

Security Information and Event Management (SIEM) centralizes data by collecting logs and events generated by host systems, security devices and applications on a single platform. These logs and events are then translated into actionable reports and alerts.

Vulnerability Management Vulnerability scans detect and classify the system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

Security Operation Center Endpoint protection, integrated security vulnerability scanning and reporting, and integrated cloud configuration assessments. Real-time security monitoring, immediate analysis, and response from our 24/7/365, U.S.-based SOC, staffed by U.S. citizens who are all SECNAP employees.

SECNAP
NETWORK SECURITY

Differentiate & Grow Your MSP Business

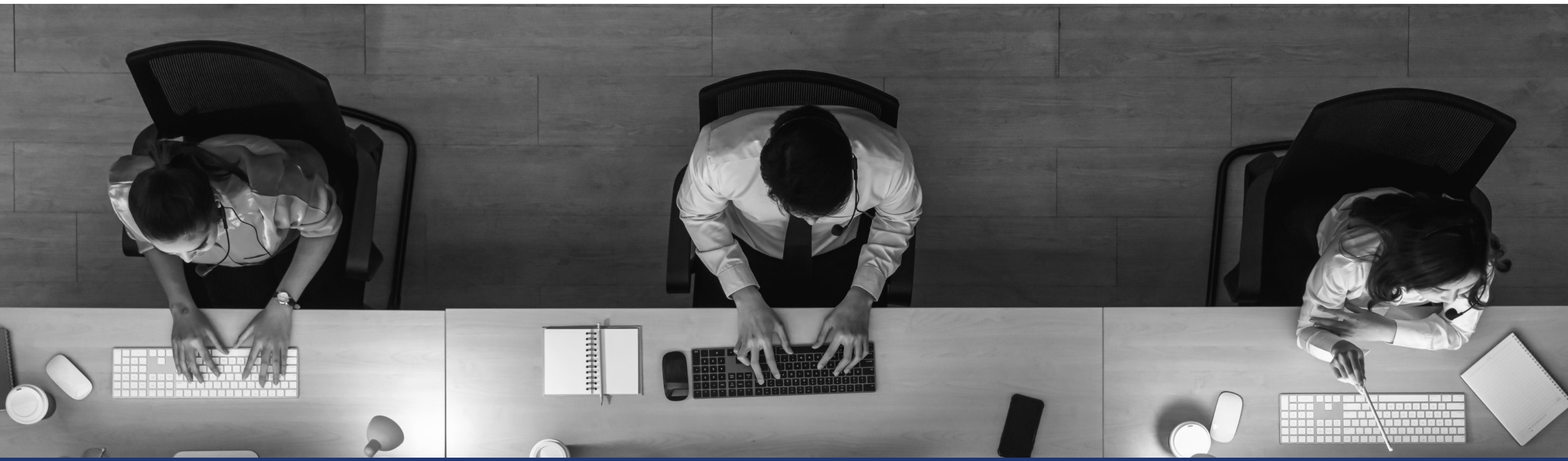
As standard MSP services, such as remote administration and backup, rapidly become commoditized, MSPs must cultivate new service offerings to remain competitive.

SMBs and mid-market companies are accelerating their spending on cybersecurity as the ongoing pandemic forces them to expand their remote-work infrastructures. Over one-quarter of SMBs and nearly one-third of mid-market businesses expect their cybersecurity spending to be higher than originally planned, even after COVID-19 restrictions are relaxed. An increasing amount of this spend is going towards remotely managed security services, where spending growth is projected to reach 13% per year between 2020 and 2024.

The SECNAP Partner program positions MSPs to take advantage of this rapidly growing demand for managed security services. By becoming a SECNAP Partner, your MSP will be enhanced with a team of security experts, enabling you to differentiate your business in a crowded marketplace and grow your client base with minimal responsibility or overhead costs. You'll also open up a new revenue stream from existing clients which will also bring added opportunity to sell your core service offerings.

The benefits of being a SECNAP Partner include:

- **Simple Sales Programs** – Quarterly sales incentives with no quotas or tiering.
- **Steady Recurring Revenue** – Business growth through predictable evergreen and recurring revenue.
- **Cybersecurity Training** – MSP-specific sales and technical training.
- **Easy Implementation** – Fully managed implementation as needed.
- **Sales and Marketing Enablement** – Collateral for prospecting including sales presentations as needed.
- **Partnership Feedback** – Continuous partner feedback and partner communications with full transparency to maintain and enhance the business relationship.



844.638.7328 | SALES@SECNAP.COM | SECNAP.COM/PARTNERS

SECNAP
NETWORK SECURITY

Find out more about the

SECNAP Partner Program

and apply to be a partner today.

About SECNAP Network Security

Since 2001, SECNAP Network Security has been combining human intelligence with innovative technology to protect organizations of all sizes against cyber threats, including data breaches, ransomware, phishing, and advanced persistent threats (APTs). Our proprietary, patented and patent pending CloudJacketX managed security-as-a-service platform addresses common pain points faced by IT teams, such as alert fatigue, challenges with meeting regulatory compliance requirements, lack of resources, and hidden vulnerabilities.

SECNAP's proactive cybersecurity approach combines ongoing network security assessments with managed detection and response (MDR) services, an advanced SIEM solution, and a patented intrusion detection and prevention system (IDS/IPS) to provide multiple layers of detection and protection, which are monitored 24/7 by our U.S.-based security operations centers (SOCs). SECNAP utilizes proprietary security technologies that were developed in-house.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

GSA Advantage!

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM/PARTNERS