LogMeIn
Resolve

Cybersecurity First Approach to MSP Services

Executive Summary

In today's digital-first world, the threat landscape facing businesses is more dynamic and dangerous than ever. For managed service providers (MSPs), adopting a cybersecurity-first approach is no longer optional—it's a strategic imperative and a clear competitive differentiator. With cyberattacks and ransomware incidents on the rise, MSPs are gatekeepers to vast amounts of sensitive client data, making them prime targets for cybercriminals.

This white paper explores the crucial elements of building a robust cybersecurity business plan, from understanding common vulnerabilities to leveraging cutting-edge tools like LogMeIn Resolve for endpoint security and compliance. By prioritizing cybersecurity, MSPs can strengthen their service offerings, bolster client trust, reduce downtime, and increase productivity—all while positioning themselves as industry leaders. Take the first step toward a secure future with a free trial of LogMeIn Resolve for MSPs.

1 Introduction

With the acceleration of remote and hybrid work, the security challenges facing managed service providers (MSPs) have never been greater. According to a 2023 Verizon Data Breach Investigations Report, over 50% of small and midsized businesses have suffered a cybersecurity incident in the last two years—many of them targeting MSPs as an indirect attack vector.

Real Life Use Case:

In 2021, a North American MSP experienced a multi-client ransomware event. Due to limited segmentation and a lack of multi-factor authentication (MFA), a single compromised credential enabled attackers to propagate ransomware across dozens of client endpoints. The incident led to damages exceeding $1.3 million and permanent loss of several clients.

The cost of inaction is high:
financial, legal, and reputational damage, crippling client trust. In contrast, MSPs who champion cybersecurity-first approaches increasingly report sustained revenue growth and higher renewal rates.

Expert Insight:

Security experts at LogMeIn Resolve recommend a simple, but powerful approach: Never automatically trust access to your clients' computers and data and always double-check who's connecting and what they're doing. This zero trust philosophy of never trusting and always verifying allows you to stay alert to suspicious activity and forms a bedrock of a modern MSP cybersecurity defense posture.

2 Understanding The Current Cybersecurity Landscape

Why Cybersecurity Matters for MSPs

Today's MSPs are trusted to protect sensitive client data and essential business operations. Criminals recognize MSPs as a high-value, high-impact target: gaining access to one platform can offer a path into hundreds of downstream client networks.

New Research:
According to a 2024 Datto Global State of the MSP Report, 70% of MSPs identified cybersecurity as the #1 driver of client renewal and win rates.

Competitive Differentiator: Technology Marketing Toolkit tracks client satisfaction across 700+ MSPs. Firms that proactively address security not only have 40% higher client retention but also close sales 30% faster, as security-first approaches signal trustworthiness to prospects.

Common Vulnerabilities and Ransomware Trends

Internal vulnerabilities—particularly human error and weak credentials—are consistently implicated in breaches. Verizon's 2023 report found 82% of breaches involve a human element; password reuse and phishing are still rampant.

Externally, unpatched software, insecure remote access, and misconfigured cloud services provide attackers with entry points. In the last year, ransomware groups have increasingly mimicked legitimate MSP vendor communications to launch phishing attacks.

Trend Watch—Ransomware-as-a-Service (RaaS):
A 2023 incident saw an Australian MSP locked out of 250+ client servers after a single phishing email. Attackers deployed ransomware, demanding $2 million. The firm's effective incident response plan (IRP)—including segmented backups—enabled restoration without payment. Those without IRPs see average downtime of 21 days and brand damage that can last years.

3 Building a Cybersecurity-First Business Plan

Reviewing Your Current Security Tools & Practices

Whether you're running a one-person MSP or have a small team, the foundation of any cybersecurity-first business plan is understanding where you stand. Start by taking inventory of all the tools and processes you use to support your clients remotely. Look for areas where things might slip through the cracks—like computers that regularly skip software updates, commonly shared passwords, or unclear rules about how remote access is granted.

Tools like LogMeIn Resolve make this easy by providing dashboards and automated reports that show, at a glance, which devices need updates or have weak security settings. Even a simple checklist or regular review can help you spot risks before they turn into bigger issues.

Setting Up Simple, Actionable Security Steps

Developing and Implementing Strategies

You don’t need a big staff or formal roles to be ready for security problems. Instead, write down a step-by-step plan you’ll follow if something suspicious comes up—such as a client calling about an odd computer message or a phishing email. Your plan should include:

1. How you’ll use your remote support tool to quickly look at affected computers

2. What specific actions you’ll take right away (like resetting a password, running a quick malware scan, or applying security updates)

3. Who you’ll contact for advice or escalation if the problem is bigger than expected (for example, a vendor helpdesk or industry peer group)

4. How and when to update your client throughout the process

If you have even a small team, make sure everyone knows these steps, and practice running through them with scenarios, so you’re prepared for the real thing.

Creating Goals and Tracking Your Security Improvement Plan

With your baseline, set realistic and meaningful security goals for your business and your clients. These can be as simple as:

1. "Turn on two-factor authentication for all remote access tools by end of quarter"

2. "Update all client devices to the latest patches each month"

3. "Send a quarterly security tip email to all end users"

Write down the steps needed for each goal—such as scheduling time to turn on new features, sharing clear instructions with clients, or setting reminders for monthly checkups. Review your progress every month or quarter and adjust your approach if certain steps take longer or don't go as planned.

Using Tools and Automation to Level Up Security

When running a business by yourself or in a small team, the right tools can be your best ally. Use features like automatic alerts for suspicious activity, regular patch management, and secure credential storage to lessen your manual workload and reduce the risk of things being missed.

Practical Tip:
Customize your remote support platform to send alerts for any device falling behind on updates or showing repeat login issues. This way, you catch possible threats early—without extra effort.

4 Overcoming Challenges in Cybersecurity for MSPs

Budget Constraints

Security improvements add costs, which can be hard for smaller MSPs that know every dollar counts. However, inaction can carry greater risks for your business: IBM's 2023 Cost of a Data Breach report places average costs at $4.45M USD. MSPs can avoud this by leveraging cost-effective tools to protect your investment. Solutions like LogMeIn Resolve, for instance, combines remote management, zero trust controls, and audit tools in a single license, helping you handle more without paying multiple different vendors for services.

Practical Tips:

- Choose tools that automate patching, alert you to risks, and let you manage many clients from a single dashboard.
- Take advantage of vendor deals, partner resources, and community forums for free or discounted security training and software.

Keeping Up With Evolving Threats

Cyber threats constantly change, and it's tough for a small team—or a one-person MSP—to stay ahead. Make continuing education and regular review a habit:

- Schedule a monthly "security check-in" to read up on the latest scams affecting MSPs and small businesses.
- Join cybersecurity groups or sign up for newsletters from trusted vendors or organizations, so new threats are brought directly to your inbox.
- Use your remote support platform's built-in alerts and suggested actions to react to new risks right away.

Practical Tips:

- Make a simple playbook for the most common issues—like how you'll handle a phishing email, or a device showing signs of malware.
- Lean on your support software to send automatic warnings if a problem is detected, so you don't have to watch everything manually.

Managing Regulatory Compliance

Clients, especially those in fields like health care, finance, or law, often face strict requirements around privacy and security—even if you're a small business supporting them. Don't let compliance needs become overwhelming. Look for tools that:

- Provide built-in reports and logs you can easily share with clients or auditors
- Offer straightforward ways to use strong encryption and access controls
- Help you stay organized with regular reminders and audit checklists

Practical Tip:

- Save or print out compliance checklists for each client, marking off items as you complete them.
- Use remote support tools to generate proof of updates, user access, and other security-related activity.

LogMeIn Resolve offers encrypted data-at-rest and in-transit, MFA, role-based permissions, and out-of-the-box audit trails, making compliance documentation straightforward.

5 Benefits of a Cybersecurity-First Approach

Preventing Problems Before They Happen

By putting security front and center in your MSP business, you can stop many issues before they affect you or your clients. Regularly updating client devices, using strong passwords, and enabling two-factor authentication mean viruses, hacks, and ransomware attacks are much less likely to disrupt your work or your clients' businesses.

Increased Productivity and Reduced Downtime

MSPs adopting a proactive approach to security report up to 25% more efficiency across operations. With automated device management and patching, help desks shift focus from reactive firefighting to strategic projects. This can help free up your time to focus on other tasks or grow your business.

Practical Tip:

- Set up automatic alerts for out-of-date software or risky login attempts, so you're not checking each device manually.
- Use easy-to-read dashboards to track where action is needed, helping you prioritize your time.

Enhanced Client Trust and Competitive Advantage

Clients want to know their business and their data are in good hands. When you take security seriously, you earn their trust, stand out from competitors, and are more likely to keep their business. Clients who feel protected are also more likely to refer you to others, helping you grow your business.

Leveraging Technology for Simplification

LogMeIn Resolve's all-in-one platform enables unattended access, scheduled scripts, granular permissions, mobile device management, and unified ticketing. MSPs can deliver personalized service with powerful automation—reducing manual errors and boosting client satisfaction.

Testimonial

> "The efficiencies unlocked by LogMeIn Resolve has halved the time required for anti-virus and disk management. It is allowing us to tke on more customers, since the process for setting up and managing customers is so simple."
>
> **Jonathan Donnelly**
> Managing Director of Alpha CC

6 How LogMeIn Resolve Supports Cybersecurity

Built-in Zero Trust Security

LogMeIn Resolve is designed to make security simple and easy to use so you don't have to learn how to use different tools and worry about missing an update. With built-in security features like MFA and strong encryptions, every action in LogMeIn Resolve is authenticated and authorized before granting access.

Intuitive Features for Faster Threat Response Times

LogMeIn Resolve's automation tools enable quick deployment of security patches at scale, with minimal disruption. MSPs can launch background updates, quickly isolate compromised devices, or revoke access in real-time. The single-pane-of-glass dashboard brings MDM, patching, user management, and compliance tracking into an accessible interface. This allows you to act fast on a single platform even if you're juggling multiple clients.

Practical Tip:

- Set up automated security checks so Resolve notifies you about outdated software or risky activity.
- Use unattended access to handle updates at off-hours, so you don't disturb client business.

Helping Meet Client and Regulatory Needs

Many of your clients may need to show they're compliant with industry rules like HIPAA or GDPR. LogMeIn Resolve can help by automatically tracking software updates, who accessed what and when, and generating clear reports you can share during audits. This not only protects your clients—it proves the value you bring.

7 Gain a Competitive Edge in Cybersecurity

Standing out as an MSP is more than just fixing computers fast; it's about earning your clients' trust by keeping their businesses safe while providing value to help them grow. By making cybersecurity a core part of how you can keep your clients safe, it helps send a powerful message: your clients' protection comes first.

When you use practical, easy-to-manage tools like LogMeIn Resolve, you show that security isn't just something you talk about. It's built into your day-to-day support, from keeping devices updated, to catching threats early, to supplying clear reports when clients need proof they're in good hands. This helps your business in several ways:

Winning more clients. Businesses are looking for MSPs who make security a priority. Marketing your security-first approach helps you stand out and win trust—especially with clients in healthcare, legal, finance, or retail.

Building loyalty. When clients know you're proactive about security, they stick with you longer and refer others.

Working smarter, not harder. Automation and clear processes save you time, so you can grow your business or focus on new services.

The right cybersecurity plan doesn't need a big staff—it just needs practical steps, reliable tools, and your commitment to keeping clients safe. In today's landscape, that's the edge that sets successful MSPs apart.

LogMeIn Resolve

Ready to transform your MSP with best-in-class security?

Start your free LogMeIn Resolve trial today and see firsthand how you can protect your clients, improve operations, and gain a competitive edge.