eBook

10 Things MSSPs Need in an Email Security Solution

IRONSCALES™
SAFER TOGETHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Being a Service Provider Carries a lot of Responsibility

The Importance of a Service Provider

Whether it's managing compliance, security controls, or client devices, you're often the most important security investment for your customers. As business security needs and the cyber threat landscape have evolved and expanded, Service Providers have become a must-have for organizations that don't have the internal resources to manage their networks.

This need is reflected in the expansion of the managed security services market, which is forecast to grow from $27.7 billion to $64.73 billion by 2026. And your services are transformative to the businesses that use them – it's not just an improvement in their security posture, it's access to your expertise, more time for their security team to focus on operations, and a subsequent drop in costs.

The Growing Threat of Email

Email is an attack vector that's shifting at a faster rate than businesses can keep up with. According to the 2021 Verizon Data Breach Investigations Report (DBIR), the incidents of phishing attacks in data breaches increased from 25% to 36% over the previous year, which accounted for an increase in Social Engineering Attacks, Business Email Compromise (BEC), and Malware and Ransomware attacks. Phishing is now the biggest concern of 90% of IT professionals – with hackers constantly switching and leveling up the style and complexity of their attacks, organizations are struggling to find the time, training, and tools to fight back.

Given the importance of email for communication in businesses of all sizes, industries, and locations, most are well aware of the inevitability of malicious emails. But that doesn't mean they have the resources or expertise to address the risks.

Today's Solution

How are organizations dealing with email security now?

What are the issues with this approach?

How can businesses avoid these issues?

FOR USERS

Most organizations leave it up to their employees alone to identify email threats like phishing and business leaders assume their IT staff have the experience and resources required to address any issues.

The reality is that users don't always recognize the tell-tale signs of phishing, and with attacks becoming harder to spot – even for the experts – the responsibility for identifying malicious emails cannot be put solely on the user.

Overcoming these issues requires a solution that's easy and simple to use, with regular training boost users' phishing knowledge and easy-to-use reporting tools to make them an integrated part of the solution.

FOR SECURITY TEAMS

If and when threats are identified, it's up to analysts, or general IT staff, to investigate and remediate each reported event individually.

Leaving it up to humans alone to manually remediate threats is unrealistic and unsustainable, not to mention the risk of overwhelming staff and causing "alert fatigue."

Deploy a solution that fits seamlessly with the security staff's workflow, remediating threats automatically and removing malicious emails from inboxes without the need for any manual input.

A Solution for Service Providers

Most organizations don't have the time, people, or budget to deploy and manage their existing information technology, let alone add new solutions to the stack.

That's where you come in.

By offering an email security solution, you can help address these resource gaps for your clients, increase stickiness and customer loyalty, boost recurring revenue, and enhance your offering with innovative technology.

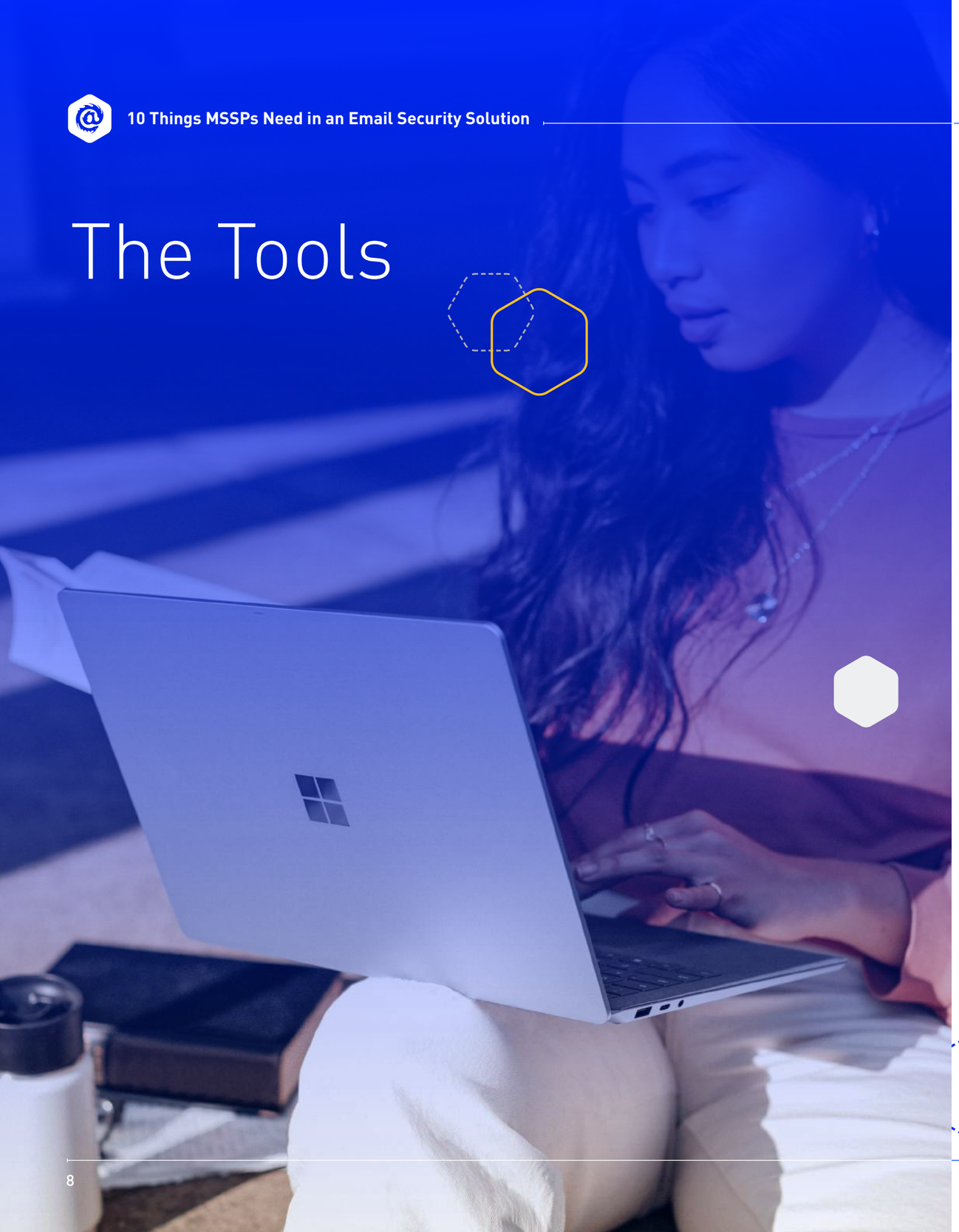
But it's unfeasible, even for a service provider, to keep up with every evolving cyber threat in today's landscape. Whether you're looking to add email security to your toolbelt or upgrade your existing offering, it's not enough to simply offer an anti-phishing tool with advanced threat protection.

You need a next-generation tool that will evolve as threats evolve.

This guide will take you through exactly what you should be looking for in an email security solution.

Let's dig in!

The Tools



1. Flexibility in email environments

To support all your existing and potential customers' different requirements, your chosen solution should be scalable and extensible. Choose a security solution that natively integrates with key mail providers via API, supporting your customers' different environments and ways of working. This also removes the need for IT Admins to make configuration changes that could introduce risks or interruptions.

Look for a solution that works across:

- Cloud environments
- Premises-based environments
- Hybrid environments

Supporting the major email providers:

- Microsoft Office 365 (O365)
- Google Workspace (GWS)
- Microsoft Exchange

2. Easy implementation

Choosing a solution with simple implementation reduces the workload for both your team and your customers' teams, showing just how valuable you are as a Service Provider before you've even begun protecting their inboxes.

By simple implementation we mean:

- Minimizes end-user disruption during implementation and onboarding
- Automates wherever possible
- Clusters services under one solution
- Provides multi-lingual support
- Offers multiple SIEM/SOAR integrations

The Tools

3. Automation

By automating the process of predicting and identifying emerging phishing threats, you can make detection and remediation faster, cheaper, and more accurate. And for automation to be effective, it needs to make full use of Artificial Intelligence (AI) and Machine Learning (ML). With AI and ML shouldering the burden of analyzing and responding to threats, IT SecOps teams are able to see through the noise and focus on other security activities.

Automate the process by:

- Completely removing emails from user inboxes at scale
- Using AI and ML to get real-time recommendations on every open incident
- Auto-classifying and clustering threats to lower response times

4. Awareness and training

Technical solutions can only do so much, even when using the most advanced AI and ML. Employees can play a vital role in catching emerging threats and social engineering attacks, but this requires more than an occasional "security awareness briefing." To build long-term protection for your customers' environments, you should offer a solution that continually provides employees with personalized phishing simulations built on real-world data. By combining this personalized education with AI-powered technology, you can empower email users to identify signs of phishing attacks and report them before any damage is done.

Build long term protection by:

- Offering thorough and engaging ways to boost phishing awareness
- Personalizing phishing education with simulations catered to their role and permissions
- Empowering users to easily report phishing attempts

5. Multi-tenant deployment with a centralized dashboard

When you're working across multiple clients at the same time, your email security solution should use a multi-tenant approach and a centralized console or dashboard, so you never have to collate client information from different places. This saves time on reporting and managing phishing incidents, allowing you to better meet customer expectations.

Look for a solution that:

- Provides multi-tenant deployment
- Manages security across all email inboxes from a central dashboard
- Provides status and reporting on incoming threats for you and your customers

6. A self-provisioned licensing model

As a service provider, real-time visibility into your inventory of available and provisioned licenses is a must-have. This includes access to granular license details for all of the customers in your portfolio and the ability to make quick changes to license assignments to meet their changing needs.

Look for a solution that:

- Has visibility across all of your licenses
- Is flexible enough to make quick changes to license assignments

7. Detailed analytics

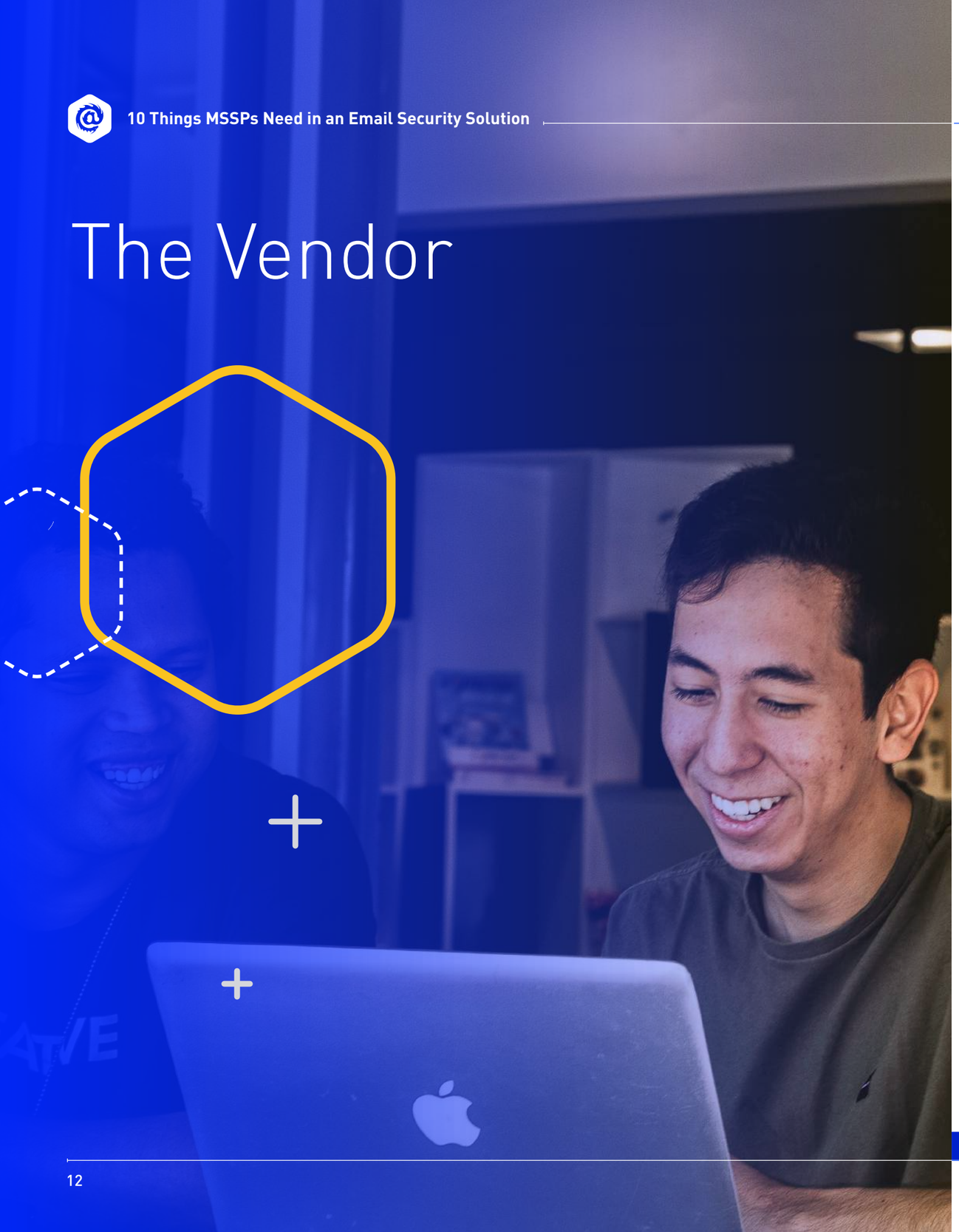
To communicate your value as a Service Provider you have to show, not just tell. Getting key performance metrics, pulled from detailed analytics reports, helps current and future customers see how transformative your services are, increasing all-important customer stickiness.

Communicate key performance metrics by:

- Providing detailed analytics immediately
- Offering up-to-date information on total:
  Inspected emails / Resolved incidents / Remediated phishing attempts / Analyst time saved

To learn more and see examples of each of these tools head over to
https://IRONSCALES.com/10Things-Resources

The Vendor



8. Dedicated managers

When working with multiple clients, you need to know that your selected email security solution provider is there to support you. Having a dedicated Partner Manager and Customer Success Manager helps to get you up and running efficiently and resolve any issues as soon as they arise.

Make sure a provider assigns you:

- A dedicated Partner Manager
- A dedicated Customer Success Manager
- A dedicated Marketing Manager

9. Sales support

The ability to win new customers and cross-sell to existing ones is vital as a Service Provider. Your chosen solution should help you move customers through the sales funnel, supporting your product demos, Proof of Concepts (POCs), and providing all the content your sales team needs to communicate your value to new and existing clients.

The ability to win new customers depends on:

- The solution's ability to support you in running product demos and POCs
- The sales support should provide you with the sales content you need, including:
  - Sales decks
  - Training, both sales and technical
  - Battlecards and Solution briefs and white papers

To learn more and see examples of each of these tools head over to
https://IRONSCALES.com/10Things-Resources

The Vendor

10. Marketing support

When you take an email security offering out to customers, building trust in your new solution is key. Whether it's through events, webinars, blogs, ads, datasheets, or videos, receiving and using marketing support about a solution helps you get in front of more customers and convince them of your value.

Your marketing support should:

- Provide marketing content that complements sales motions
- Offer go-to-market strategy and coordination assistance
- Assist in running events, webinars, lead generation, and surveys

About IRONSCALES™

As the world's fastest-growing email security company, we know everything there is to know about email security, and our leading technology reaches more than 700,000 mailboxes globally

The IRONSCALES platform fights phishing where it hurts the most — directly in your customers' mailbox. Our self-learning, AI-driven email security platform continuously detects and remediates advanced threats in your customers' mailboxes. And our advanced threat assessment and phishing training simulates real phishing scenarios, educating employees and boosting overall organizational security awareness.

At IRONSCALES our simple email security platform is the perfect addition to your MSSP solution portfolio. With our **Service Provider Program**, you can offer your customers fast onboarding, coverage for multiple email platforms, and protection against advanced phishing attacks. And our corresponding marketing content, short sale cycles, and product demo support boost your success as a Service Provider.

We'd love to chat with you about your email security offering.

For more information on the IRONSCALES platform and how it benefits MSPs & MSSPs, visit **ironscales.com.**

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

IRONSCALES™

5 Concourse Pkwy, Suite 850
Atlanta, GA 30328
Partners@ironscales.com

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS