How to Sell and Deliver Internal Threat Detection with Cyber Hawk™

By Win Pham, Vice President Development

RapidFireTools®
A Kaseya COMPANY

Overview

No business or organization with a computer network is immune from the threat of data breaches, unauthorized access, and malicious activities performed from **inside** the firewall. Almost 70% of companies feel vulnerable to insider attacks, and they are more worried about negligent and inadvertent insider data breaches than they are about malicious intent.[1] These threats do not just happen to large, well-known corporations; 43% of all cybersecurity incidents are directed at small companies. [2]

Managed Service Providers (MSPs) can provide a range of enhanced internal cybersecurity services for all their clients, without increasing staff or making big investments. Offering an internal cybersecurity service has three core benefits:

1. **Service Differentiation**: MSPs are constantly pursuing a competitive edge by offering innovative high-value services to clients and prospects. Security is a top-of-mind issue that will help open doors to new clients and expand services to existing clients.
2. **Significant New Revenue**: There are few services that universally appeal to all clients, and cybersecurity is one of them. Affordable tools have made it possible for MSPs to incorporate an internal cybersecurity service into their standard managed service offerings. This service allows them to generate significant incremental revenue through upselling to higher levels of security, or in additional billing for the identification and remediation of cyber threats as they are detected.
3. **Increased Client Retention**: The more services a client has with an MSP, the “stickier” the relationship. Regular meetings to review reports deepens communication and builds further rapport.

This white paper explains how to use a subscription-based cybersecurity offering to set up a repeatable, scalable, automated security service that MSPs can deliver to their clients cost effectively, while also providing high-value peace-of-mind.

The Technology

At the heart of the solution is Cyber Hawk, which identifies a wide range of internal cybersecurity threats and generates a daily email alert or internal ticket of anything suspicious it discovers.

As a stand-alone software appliance, Cyber Hawk is attached to an individual client’s network and configured to run a daily internal cybersecurity scan.

Cyber Hawk’s proprietary scanning technology is non-intrusive, but it does a deep dive through the network in search of anomalous user behaviors, along with unexpected changes to network settings, configurations, assets, and other types of internal threats.

Examples of typical internal threats that Cyber Hawk can discover include:

- Unauthorized logins or attempts to restricted computers
- New user profiles suddenly added to the network
- Applications just installed on a locked down system
- Unauthorized wireless connections to the network
- New users just granted administrative rights
- Unusual midnight log-in for the first time by a day-time worker
- Sensitive personal data such as credit card numbers, social security numbers, and birth dates stored on machines where it doesn't belong

Some of the threats that Cyber Hawk uncovers are based on pre-configured settings. Others are based on "Smart-Tags" that an MSP sets up based on that client's specific policies and permissions. Cyber Hawk also establishes baseline system configurations and recognizes user trends over time, a critical component for identifying anomalous behaviors and activities.

An MSP can create rules telling Cyber Hawk where to send the various kinds of threat alerts that can be detected by the software. Some MSPs opt to have user- or permission-based threats go directly to a key contact at the client to self-triage these alerts. For example, there may be an action that would appear to be an anomalous user behavior threat, such as an unauthorized employee accessing a sensitive machine, that the client knows about and verifies special permission was granted. The threat can be ignored if a one-time event, or an MSP can set up a Smart-Tag for this permission to avoid future false positives. MSPs can have alerts that are more technical in nature bypass the client and go directly to the appropriate technician.

In addition to the daily alerts, Cyber Hawk will automatically issue a weekly notice. Weekly notices contain additional information from the daily alerts, such as new broadcasted wireless networks, DNS changes, and switch-port connection changes. These notices can be saved and used as part of client reporting or archived for future threat analysis.

Creating and Enforcing Internal IT Security Policies

Looking for internal cybersecurity threats is more challenging than managing threats from the outside.

Consider a security procedure put into place to protect a VIP at a special event. The first layer of security is typically a controlled perimeter, where vehicles are prohibited from entering, and every person attending must go through a metal detector and submit to a pat down before entering the venue. Those processes are the equivalent of standard cybersecurity protections – firewalls, antivirus, and anti-malware software – and that's the easy part.

Setting up an exterior security checkpoint can be standardized, as it is a simple one-way passage. However, once on inside, every venue and event are unique, and the internal security team needs to be familiar with the venue to create the proper security measures. They need to be vigilant and watchful of the crowd, scanning people's facial expressions, body language, and movements. They are always on the lookout for anyone concealing a weapon who might have gotten through the perimeter security.

The same is true with networks. It's relatively easy to set up a firewall or install antivirus and anti-malware software. Until now, there hasn't been a practical way to know if any of the client's IT security policies were being breached from inside the network.

Cyber Hawk makes this possible through an intuitive, checkbox-driven menu that allows each site to be quickly configured and precisely aligned with each client's unique IT security policies. Here are some examples of the kinds of policies that Cyber Hawk can track:

Access Control

- Restrict access to accounting computers to authorized users
- Restrict access to business owner computers to authorized users
- Restrict access to IT admin only, restricted computers to IT administrators
- Restrict access to computers containing electronic protected health information to authorized users
- Restrict access to systems in the cardholder data environment to authorized users
- Restrict users that are not authorized to log into multiple computer systems
- Authorize new devices to be added to restricted networks
- Restrict IT administrative access to minimum necessary
- Strictly control the addition of new users to the domain
- Users should only access authorized systems
- Strictly control the addition of new local computer administrators
- Strictly control the addition of new printers to the network
- Investigate suspicious logons to computers
- Investigate suspicious logons by users

Computers

- Changes to locked down computers should be strictly controlled
- Restrict Internet access for computers that are not authorized to access the Internet directly
- Install critical patches for DMZ computers within 30 days
- Install critical patches on network computers within 30 days

Network Security

- Remediate high severity internal vulnerabilities immediately (CVSS > 7.0)
- Remediate medium severity internal vulnerabilities (CVSS > 4.0)
- Detect network changes to internal wireless networks
- Detect network changes to internal networks
- Only connect to authorized wireless networks

Whatever security policies that you set up are checked by Cyber Hawk, and any violations – or attempted violations – are recorded and reported.

As an example, assume there are computers in a network where access to these systems is restricted to only users who have administrator level rights. These can be important systems like Domain Controllers, Web Servers, Database Servers, Exchange Servers, or servers where there are strict access and change management controls.

The Cyber Hawk user-interface allows MSPs to apply a Smart-Tag to all the IT ADMIN users, and a separate RESTRICT IT ADMIN ONLY Smart-Tag to the specific relevant computers. Once these tags are set up, if any user who has not been identified as IT ADMIN accesses one of the IT-ONLY computers will be viewed as a threat, and that incident will show up in the form of daily alert.

Another scenario is when the client’s network needs to be tightly controlled in compliance with strict network change management policies and procedures, essentially locked down regarding any new devices. Applying a single Restricted Network Smart-tag to the IP range is all that is needed to trigger an alert on the incident if a new device is added to the network.

This unique approach to internal IT security allows for granular control and ongoing refinement.

Process and Automation – Service Delivery System

Having a tool like Cyber Hawk allows an MSP to improve the level of IT security that they offer by adding a layer of internal security alerting to the external protection already being provided.

Without a system like Cyber Hawk, discovering potential internal cybersecurity threats can be tedious. It would require at least one dedicated, full-time security technician to manually pore through hundreds of pages of SIEM logs every day, looking for anomalous end-user behaviors, changes to the network or individual computers, and other types of suspicious data.

Cyber Hawk streamlines service delivery, reduces labor time, and allows for a scaling of internal cybersecurity services across an entire client base. The subscription-based, pre-packaged offering includes everything that MSPs need to automate the service described above and to allow for the creation of completely customized, branded offerings.

The Cyber Hawk subscription package includes the following elements:

- A license for unlimited Cyber Hawk software appliances
- Interactive email response system
- Web and mobile friendly alert management portal
- Four pre-configured “best practice” service plans
- Customize service plan creator
- Direct PSA service ticket integration (Kaseya BMS, Autotask, ConnectWise, Tigerpaw)
- Sales & marketing collateral to help sell-in your service

Interactive Email Response System

One of the key advantages of Cyber Hawk is the option for the MSP to have select interactive email alerts sent directly to the client for vetting before escalation. The email alert will state the issue and prompt the recipient to choose whether they want the event investigated further or ignored. Alerts sent directly to clients include dynamic action links embedded in the email. This alert can be used as a revenue-generating tool by allowing the client to authorize work outside the scope of what’s included with the managed services contract.

Client Alert Management Portal

In addition to providing access to manage the incidents, MSPs can optionally give clients direct access into the portal for limited control over certain features. Because of this client access, we offer the option for the MSP to brand the portal, increasing the perceived value of the service and the MSP.

For example, in the previously mentioned situation where an MSP might allow the clients to self-triage access-related alerts, clients can also take care of false alarms themselves. Marking the issue as a false positive in the portal allows clients to request their own Smart-Tag updates before MSPs even get involved. It is like having a home security system that allows the homeowner to disable an alarm that goes off by mistake before the monitoring company responds with a costly service call.

The partial “self-serve” option isn’t for everyone. Some clients don’t have the time or ability to deal with the alerts. Some MSPs want to provide their clients with a completely seamless and “behind-the-scenes” service. In those situations, all alerts go straight to the MSP. However, there are many situations where the client does have internal people who can quickly review and vet many of the non-technical alerts, saving the MSP significant time and allowing the service to be offered at a lower cost without impacting profitability. Sending the alerts directly to the clients also helps to raise their awareness of the potential insider security threats, helping to justify the need for the service.

In addition to having non-technical alerts sent to the client, the portal is also ideal for MSPs who rely on third-party Network Operations Centers (NOC) for Level-One technical response. All or some of the daily alerts can go directly to the NOC, and the NOC techs would have access directly into the Client Alert Management Portal. This allows seamless collaboration between the NOC and MSP in serving the client’s internal security issues.

Direct PSA Service Ticket Integration

Cyber Hawk subscribers using Kaseya BMS, ConnectWise, Autotask, or Tigerpaw as their ticketing system have the option to automatically or manually create tickets based from alerts. Incidents in the daily alert emails that require investigation can either be addressed through creating service tickets within the portal or sending them directly to their PSA to automate the process. This saves time by eliminating the need for technicians to manually create tickets from scratch and speeds up the remediation process.

Four Pre-Configured Service Levels

Prior to Cyber Hawk, it was difficult for MSPs to deliver internal cybersecurity services. Many MSPs lack the time, resources, or framework for designing, packaging, pricing, and marketing such a service. We have created four basic internal cybersecurity “blueprints” that are built into the tool, in the form of pre-configured service plans with accompanying marketing materials.

The four plans are generically labeled as Bronze, Silver, Gold, and Platinum in the tool; but the names can be changed by the MSP, and the actual plan elements modified to create unique and branded offerings.

Bronze Level Service

The Bronze Level is an introductory tier that should be provided to all clients free of charge (even if the client is break/fix only). To minimize costs, the Bronze Level only includes alerts that should be directed to the client using the email end-user workflow. When potential threats are detected, clients are emailed first and able to provide authorization for an MSP to investigate and remediate issues.

To profit on this level of service, MSPs should be sure the contract specifies that responses to any client requests for investigation and/or remediation will be charged at the appropriate billable rates.

The alerts that are part of the Bronze Level are access control related, bringing a higher degree of network awareness to clients and providing MSPs with an opportunity to upsell additional security services.

Below is the pre-configured basic policy set for the Bronze Level:

Access Control

- Restrict access to accounting computers to authorized users
- Restrict access to business owner computers to authorized users
- Restrict IT administrative access to minimum necessary
- Strictly control the addition of new users to the domain
- Strictly control the addition of new local computer administrators
- Authorize new devices to be added to restricted networks

The Value of the Service

This plan level addresses the most basic security:

1. Improper administrative access
2. Improper access to computers with sensitive information
3. Lack of change control leading to rogue users and systems on the network

With the basic Bronze Level service, MSPs should identify a key contact at the client who would be responsible for “self-triaging” the incidents identified on the daily alerts. This self-triage presents several critical benefits for both the MSP and the client:

1. Keeping security top-of-mind at the client site. With someone continually reminded by the daily alert, and acting on them, the entire company should become more aware of potential threats.
2. Triaging by the client minimizes the incremental time the MSP needs to invest as the client manages the scans and alerts.
3. If the self-serve option is offered at no cost, the MSP’s service contracts should be structured to include a separate hourly fee for any time spent investigating and/or remediating internal cybersecurity incidents. This will most likely save the

client significant dollars in loss prevention, fines, and public embarrassment, while generating incremental revenue for the MSP.

Implementing the Service

The table below shows the tasks involved and the purpose of each:

Task	Cost	Purpose	Level
Configure Basic Policy Set	Included	Detects violation to the most common high-value policies	Bronze
Initial Configuration of Smart-Tags	Included	Configure the policies for the specific customer's environment	Bronze
Ongoing Smart-Tag Refinement	Included	As the customer's environment changes, keeps the Cyber Hawk configuration up to date	Bronze
False Positive Adjustments	Included	Refine the Cyber Hawk configuration by adjusting Smart-Tags to eliminate false positives and improve detection	Bronze
Investigate Alerts	Additional Service Hours	Investigate and determine the root cause of a particular issue and present findings to the stakeholder	Bronze
Perform Remediation	Additional Service Hours	Investigate and remediate the underlying issue by carrying out the recommended actions	Bronze

Pricing: No monthly fee for basic "self-serve" automated system
Hourly charges for investigation and remediation

Required One-Time Set-up Tasks:

- Deploy a Cyber Hawk software appliance to the client's site
- Configure the appliance using the built-in Bronze Plan
- Set access control alerts to be sent to the client for self-triage

Requests made by the client to ignore an alert will be handled by the NOC to adjust Cyber Hawk to tune the alerts and remove false positives. Investigation requests made by the client create a work order, which leads to additional service revenue. Typically, clients will only contact the MSP under this plan if and when they want further investigation.

Silver Level Service

The Silver Level is the minimum level of coverage that should be provided to **all** managed services clients. Although MSPs can charge for this plan, we recommend bundling it into a standard managed services offering and adjusting the total fee accordingly.

This is a high-value security service, which will go a long way toward differentiating MSPs when it is included in pitches to prospects and clients. It is a great value-added service that will cement client relationships, reduce churn, and lead to additional project and service revenue through client-approved, built-in work authorizations.

The Silver Level adds some alerts which are configured to be sent to technicians directly. These alerts are designed to help prevent configuration drift and allow the MSP to get ahead of potential issues that could lead to increased costs to deliver managed services.

This level of service would be the most appropriate for many clients. It will cover the most common internal threats. Your Managed Service Agreement (MSA) should include a provision to charge separately for any internal security investigation and remediation of discovered incidents.

Below is the pre-configured basic policy set for the Silver Level. Note that the policies in *italics* denote the incremental detection protocols that are covered by the Silver Level service, above and beyond that in the Bronze Level:

Access Control

- Restrict access to accounting computers to authorized users
- Restrict access to business owner computers to authorized users
- Restrict IT administrative access to minimum necessary
- Strictly control the addition of new users to the domain
- Strictly control the addition of new local computer administrators
- Authorize new devices to be added to restricted networks
- *Restrict access to IT admin only restricted computers to IT administrators*
- *Restrict users that are not authorized to log into multiple computer systems*
- *Users should only access authorized systems*
- *Only connect to authorized printers*

Computers

- *Install critical patches on network computers within 30 days*

Network Security

- *Only connect to authorized wireless networks*

The Value of the Service

This plan level addresses the most common security vulnerabilities:

1. Inadequate or no perimeter defense
2. Inadequate patching to prevent vulnerabilities
3. Improper administrative access
4. Improper access to computers with sensitive information
5. Lack of change control leading to rogue users and systems on the network

With the basic Silver Level service, MSPs should identify a key contact at the client who would be responsible for “self-triaging” the incidents identified on the daily alerts. This self-triage presents several critical benefits for both the MSP and the client:

1. Keeping the client conscious of network security. With someone continually reminded by the daily alert, and acting on them, the entire company should become more vigilant regarding potential threats.
2. Triaging by the client minimizes the incremental time the MSP needs to invest as the client manages the scans and alerts.
3. A service agreement should be structured to include a separate hourly fee (beyond a managed service retainer) for any time spent investigating and/or remediating internal cybersecurity incidents. This will most likely save the client significant dollars in loss prevention, fines, and public embarrassment, while generating incremental revenue for the MSP.
4. Cyber Hawk alerts reduce the MSP’s cost for supporting the network through drift awareness, quickly addressing changes to the environment that may not have been visible previously

Implementing the Service

The table below shows the tasks involved and the purpose of each:

Task	Cost	Purpose	Level
Configure Basic Policy Set	Included	Detects violation to the most common high-value policies	Bronze Silver
Initial Configuration of Smart-Tags	Included	Configure the policies for the specific customer's environment	Bronze Silver
Ongoing Smart-Tag Refinement	Included	As the customer's environment changes, keeps the Cyber Hawk configuration up to date	Bronze Silver
False Positive Adjustments	Included	Refine the Cyber Hawk configuration by adjusting Smart-Tags to eliminate false positives and improve detection	Bronze Silver
Investigate Alerts	Additional Service Hours	Investigate and determine the root cause of a particular issue and present findings to the stakeholder	Bronze Silver
Perform Remediation	Additional Service Hours	Investigate and remediate the underlying issue by carrying out the recommended actions	Bronze Silver

Pricing: Suggested one-time set-up fee + $100 - $250 per client monthly

Required One-time Set Up Tasks:

- Deploy a Cyber Hawk appliance to the client's site
- Configure the appliance using the built-in Silver Plan
- Set access control alerts to be sent to the client for self-triage
- Set remaining technical alerts to be sent to the standard NOC for technical triage

Requests made by clients to ignore an alert will be handled by the NOC to adjust Cyber Hawk to tune the alerts and remove false positives. Investigation and remediation requests made by the clients create work orders, which lead to additional service revenue.

Technical alerts are validated by the NOC and escalated as necessary to remediate issues, such as a drift in patching compliance.

Gold Level Service

The Gold Level offering is considerably more comprehensive than the Silver and should be considered for your main, high-value clients. This package represents an important upsell opportunity. The most important, prized clients fall in the 80/20 rule – that is, the 20% of clients that are generating 80% of an MSP's revenue.

The built-in configurations for this service plan cover a more comprehensive set of security issues and deliver enhanced security by incorporating internal vulnerabilities scans.

Below is the pre-configured comprehensive policy set for the Gold Level. Note that the policies in *italics* denote the incremental detection protocols that are covered by the Gold Level service, above and beyond that in the Silver Level:

Access Control

- Restrict access to accounting computers to authorized users
- Restrict access to business owner computers to authorized users
- Restrict access to IT admin only restricted computers to IT administrators
- Restrict IT administrative access to minimum necessary
- Restrict users that are not authorized to log into multiple computer systems
- Strictly control the addition of new users to the domain
- Strictly control the addition of new local computer administrators
- Users should only access authorized systems
- Authorize new devices to be added to restricted networks
- Only connect to authorized printers
- *Investigate suspicious logons to computers*
- *Investigate suspicious logons by users*

Computers

- Install critical patches on network computers within 30 days
- *Changes on locked down computers should be strictly controlled*
- *Restrict Internet access for computers that are not authorized to access the Internet directly*
- *Install critical patches for DMZ computers within 30 days*

Network Security

- Only connect to authorized wireless networks
- *Remediate high severity internal vulnerabilities immediately (CVSS > 7.0)*

The Value of the Service

Because of the truly deep nature of the network scans included with this level of service, and the more severe nature of some of the threats that it can discover, the recommended price point for the Gold Level service is between $200 to $300 per month per client. At that price, just two Gold Level internal cybersecurity service will cover the cost for an unlimited use Cyber Hawk subscription. That's what makes this such a compelling opportunity.

This plan level addresses a large array of additional security weaknesses and follows best practices dictated by security frameworks like the NIST 800-171 for detection.

1. Inadequate or no perimeter defense
2. Inadequate patching to prevent vulnerabilities
3. Improper administrative access
4. Improper access to computers with sensitive information
5. Lack of change control leading to rogue users and systems on the network
6. *Lack of change control on specific high value systems*
7. *Limiting or restricting Internet access on high value systems*
8. *Detect and remediate internal network vulnerabilities*
9. *Identify and investigate suspicious user behavior*

Implementing the Service

The table below shows the tasks involved and the purpose of each:

Task	Cost	Purpose	Level
Configure Basic Policy Set	Included	Detects violation to the most common high-value policies	Bronze Silver Gold
Initial Configuration of Smart-Tags	Included	Configure the policies for the specific customer's environment	Bronze Silver Gold
Ongoing Smart-Tag Refinement	Included	As the customer's environment changes, keeps the Cyber Hawk configuration up to date	Bronze Silver Gold
False Positive Adjustments	Included	Refine the Cyber Hawk configuration by adjusting Smart-Tags to eliminate false positives and improve detection	Bronze Silver Gold
Investigate Alerts	Additional Service Hours	Investigate and determine the root cause of a particular issue and present findings to the stakeholder	Bronze Silver Gold
Perform Remediation	Additional Service Hours	Investigate and remediate the underlying issue by carrying out the recommended actions	Bronze Silver Gold
Configure Suspicious Login Policies	Included	Automatically analyze audit logs across several machines looking for suspicious user behavior	Gold
Identify and Configure Locked Down Computer Policies	Included	Closely monitor changes on important servers and workstations, including changes to installed applications or the addition of removeable drives	Gold
Configure Specialized DMZ Patching Policy	Included	Internet-facing systems are the most likely initial targets of outside hacking attempts – These systems should always be kept up to date on patching	Gold
Perform Weekly Internal Vulnerability Scans and Identify High Risk Items	Included	Non-addressed internal vulnerabilities allow hackers and malware to exploit weaknesses in software and configuration – Identifying and remediating the most severe issues helps mitigate this risk	Gold

Pricing: Suggested one-time set-up fee + $150 - $300 per client monthly

Required One-Time Set-up Tasks:

- Deploy a Cyber Hawk appliance to the client’s site
- Configure the appliance using the built-in Gold Plan
- Set access control alerts to be sent to the client for self-triage
- Set remaining technical alerts to be sent to the standard NOC for technical triage

Requests made by clients to ignore an alert will be handled by the NOC to adjust the Cyber Hawk to tune the alerts and remove false positives. Investigation and remediation requests made by the clients create work orders, which lead to additional service revenue.

Technical alerts are validated by the NOC and escalated as necessary to remediate issues, such as a drift in patching compliance.

Platinum Level Service

The Platinum Level internal cybersecurity offering offers high-end internal cybersecurity services that MSPs can upsell to those clients whose lines of business deal with highly sensitive data and strict IT compliance requirements. Typically, this would be any covered entity in the healthcare field, any client involved with financial services, any client doing business with sensitive government agencies, and any with an e-commerce site, retail operation, or where financial transactions pass through the organization's networks.

Below is the pre-configured comprehensive policy set for the Platinum Level. The policies in *italics* denote the incremental detection protocols covered by the Platinum Level service, above and beyond those included in the Silver and Gold Levels:

Access Control

- Restrict access to accounting computers to authorized users
- Restrict access to business owner computers to authorized users
- Restrict access to IT admin only restricted computers to IT administrators
- Restrict IT administrative access to minimum necessary
- Restrict users that are not authorized to log into multiple computer systems
- Strictly control the addition of new users to the domain
- Strictly control the addition of new local computer administrators
- Users should only access authorized systems
- Authorize new devices to be added to restricted networks
- Investigate suspicious logons to computers
- Investigate suspicious logons by users
- Only connect to authorized printers
- *Restrict access to computers containing electronic protected health information to authorized users*
- *Restrict access to systems in the cardholder data environment to authorize users*

Computers

- Install critical patches on network computers within 30 days
- Changes on locked down computers should be strictly controlled
- Restrict Internet access for computers that are not authorized to access the Internet directly
- Install critical patches for DMZ computers within 30 days

Network Security

- Only connect to authorized wireless networks
- Remediate high severity internal vulnerabilities immediately (CVSS > 7.0)
- *Remediate medium severity internal vulnerabilities immediately (CVSS > 4.0)*
- *Detect network changes to internal wireless networks*
- *Detect changes to internal networks*

The Value of the Service

Based on the value of this service to a client and the required investment of time on the MSP's part, the minimum fee that should be charged for this service is $500/month or more, if the client is larger. Clients in this category have a tremendous stake in protecting data, and they may be exposed to more potential threats from the inside than the outside. This can be easily demonstrated, and for a very modest cost to the client for this critical service, MSPs can deliver a great deal of protection and peace-of-mind.

The Platinum plan builds upon the Silver and Gold plans and increases the level of detection to the standards required for regulations such as PCI and HIPAA. The plan is designed to address the proactive detection requirements of these security frameworks and addresses the issues below:

1. Inadequate or no perimeter defense
2. Inadequate patching to prevent vulnerabilities
3. Improper administrative access
4. Improper access to computers with sensitive information
5. Lack of change control leading to rogue users and systems on the network
6. Lack of change control on specific high value systems
7. Limiting or restricting Internet access on high value systems
8. Detect and remediate internal network vulnerabilities
9. Identify and investigate suspicious user behavior
10. **Compliance-level auditing**

Implementing the Service

The table below shows the tasks involved and the purpose of each:

Task	Cost	Purpose	Level
Configure Basic Policy Set	Included	Detects violation to the most common high-value policies	Bronze Silver Gold
Initial Configuration of Smart-Tags	Included	Configure the policies for the specific customer's environment	Bronze Silver Gold
Ongoing Smart-Tag Refinement	Included	As the customer's environment changes, keeps the Cyber Hawk configuration up to date	Bronze Silver Gold
False Positive Adjustments	Included	Refine the Cyber Hawk configuration by adjusting Smart-Tags to eliminate false positives and improve detection	Bronze Silver Gold
Investigate Alerts	Additional Service Hours	Investigate and determine the root cause of a particular issue and present findings to the stakeholder	Bronze Silver Gold
Perform Remediation	Additional Service Hours	Investigate and remediate the underlying issue by carrying out the recommended actions	Bronze Silver Gold
Configure Suspicious Login Policies	Included	Automatically analyze audit logs across several machines looking for suspicious user behavior	Gold Platinum
Identify and Configure Locked Down Computer Policies	Included	Closely monitor changes on important servers and workstations, including changes to installed applications or the addition of removeable drives	Gold Platinum
Configure Specialized DMZ Patching Policy	Included	Internet-facing systems are the most likely initial targets of outside hacking attempts – These systems should always be kept up to date on patching	Gold Platinum
Perform Weekly Internal Vulnerability Scans and Identify High Risk Items	Included	Non-addressed internal vulnerabilities allow hackers and malware to exploit weaknesses in software and configuration – Identifying and remediating the most severe issues helps mitigate this risk	Gold Platinum

Pricing: Suggested one-time set-up fee + $500+ per client monthly

Required One-Time Set-up Tasks:

- Deploy a Cyber Hawk appliance to the client’s site
- Configure the appliance using the built-in Gold Plan
- Set access control alerts (including the suspicious login alerts) to be sent to the client for self-triage
- Set remaining technical alerts (including locked down system changes and internal vulnerabilities) to be sent internally to technical support staff, or to the MSP’s standard NOC for technical triage

Requests made by clients to ignore an alert will be handled by the NOC to adjust the Cyber Hawk to tune the alerts and remove false positives. Investigation and remediation requests made by the clients create work orders, which lead to additional service revenue.

Technical alerts are validated by the NOC and escalated as necessary to remediate issues, such as a drift in patching compliance.

Cyber Hawk Blueprint Recap

Feature	Bronze	Silver	Gold	Platinum
Configure Basic Policy Set	✓	✓	✓	✓
Initial Configuration of Smart-Tags	✓	✓	✓	✓
Ongoing Smart-Tag Refinement	✓	✓	✓	✓
False Positive Adjustments	✓	✓	✓	✓
Configure Suspicious Login Policies			✓	✓
Identify and Configure Locked Down Computer Policies			✓	✓
Configure Specialized DMZ Patching Policy			✓	✓
Perform Weekly Internal Vulnerability Scans and Identify High Risk Items			✓	✓
Configure Compliance Level Policies				✓
Monitor Changes on Wired and Wireless Networks				✓
Investigate Alerts (authorized by customer in process flow)	Additional	Additional	Additional	Additional
Perform Remediation (authorized by customer in process flow)	Additional	Additional	Additional	Additional
Suggested Pricing	Free	$100-$250 per month	$150-$300 per month	$500+ per month

Each of the four internal cybersecurity services levels summarized above – Bronze, Silver, Gold, and Platinum – create a set of unique offerings with clear value propositions for the full range of MSP clients. They are designed to fill a critical need for any client at a price point they can afford and will also generate revenue for the MSP. Each of these plans are pre-configured, ready for MSPs to offer out-of-the-box or to modify and rebrand for further customization of service offerings.

How to Sell Internal Cybersecurity Services

These pre-set service plan blueprints are built into the Cyber Hawk and provide MSPs with most of what is needed to deliver these services. Cyber Hawk also includes sales and marketing materials that can be dynamically produced, based on the plans an MSP wants to offer.

Branded Service Plan Catalogs

A branded catalog including all the details of any, or all, of the four pre-configured service plans are built into the tool and can be easily generated for presentation purposes. Any plans that the MSP customizes by modifying the policies to be managed can be optionally included in the catalog. Any number of variations of the catalog can be produced with any combination of the built- in and customized service plans. This gives the MSP a powerful tool for presenting different plan options to the client, including a dynamically built catalog with all the service delivery details for each plan.

Service Plan Comparison Matrix

If there are multiple plans in the catalog, the system will also automatically generate a plan comparison matrix. This professionally designed comparison chart is dynamically built based on the detailed components of each plan. The complete list of all plan components is generated in the first column, alongside check marks for each of the included components. This serves as a powerful sales tool to walk clients through each of the components, each of the plans, and help them decide on the right plan for them.

Internal Cybersecurity Marketing

Most clients aren’t even aware that internal cybersecurity services are available and, more importantly, why they need them. To help educate end-users about the need for internal cybersecurity protection, the Cyber Hawk tool includes a brandable brochure that MSPs can use to generate leads for new services.

Costs and Return on Investment

Cyber Hawk is an invaluable tool that gives MSPs the ability to offer a compelling, high-value security service across an entire client base. Virtually every business, organization, and government agency are vulnerable to potential internal cybersecurity incidents, making this the perfect upsell opportunity for every existing client.

Cyber Hawk is sold through affordable, fixed fee subscriptions that give MSPs a license to deploy an unlimited number of Cyber Hawk software appliances. The features and benefits that Cyber Hawk provides, at this price point, is a fraction of the cost of having a Security Engineer on staff to provide similar levels of internal cybersecurity services at 20 times the price.

With this “fixed cost” subscription, MSPs can now offer enhanced internal cybersecurity to all clients, building goodwill, reducing churn, and closing new business through high-value service differentiation. Even with complimentary Bronze level service, Cyber Hawk will produce additional incremental revenue through client-approved “investigation” and “remediation” authorizations built into the Cyber Hawk process flow and business methodology. Clients can be upgraded to the Silver, Gold, or Platinum level of service, which would generate an additional $100-$500/month per client. Since the cost of Cyber Hawk is fixed, that adds up to a 10x to 20x return on investment with just 10 clients taking the service and much more as additional clients are added.

Conclusion

Every single company, non-profit organization, and government agency with a computer network is at risk from internal cybersecurity threats. While most MSPs offer some type of commoditized external security offering such as firewalls and antivirus, very few have the resources, knowledge, or tools to protect their clients from many types of internal threats.

Cyber Hawk is the first affordable end-to-end internal threat detection tool that allows virtually any MSP to configure, market, sell, and deliver a range of profitable services that can be tailored to meet the needs of any client.

With even a modest roll-out to a handful of clients, an investment in Cyber Hawk will yield a 10x to20x return on investment for the MSP, with considerably greater returns when rolled out across an entire client base.

For a free consultation and personalized demo, contact us at sales@rapidfiretools.com.

References:

1. 2019 Insider Threat Report, Cybersecurity Insiders

2. 2019 Data Breach Investigations Report, Verizon

RapidFire Tools, a Kaseya company, creates innovative business-building technology tools for Managed Service Providers (MSPs). More than 8,000 technology service professionals worldwide use our products to close more business, offer more services, keep more customers, and make more money. Our offerings include **Network Detective®**, a complete suite of IT assessment, documentation, and reporting tools; **Cyber Hawk™**, an insider cyber threat detection and alerting tool; and **Compliance Manager™**, an automated security and privacy compliance platform.

Our flagship product, Network Detective, is the #1 non-intrusive IT assessment and reporting tool. With it, MSPs can quickly and easily capture a vast amount of network assets, users, configurations, and vulnerabilities without installing any software, probes, or agents. Our proprietary algorithm analyzes the data to generate dozens of professionally designed, completely brandable reports in minutes. Network Detective includes six modules for different kinds of IT assessments. We also offer the Reporter add-on, which dramatically reduces time and labor by automating the network scans and report generation process. The subscriptions include an unlimited number of scans, on an unrestricted number of networks.

RapidFire Tools also offers Cyber Hawk, the first IT security tool designed to detect insider cybersecurity threats and generate daily alerts of suspicious network changes an anomalous end-user behavior. Cyber Hawk empowers MSPs to create custom, brandable, and unique cybersecurity services at an affordable rate.

Rounding out our offerings is Compliance Manager, a unique compliance process automation tool, with built-in modules to support the delivery of Compliance-as-a-Service solutions. Specific standards supported including HIPAA, GDPR, the NIST Cybersecurity Framework, as well as a specialized module for compliance with the security provisions of most cyber liability insurance policies. MSPs use Compliance Manager to ensure that the IT policies and procedures required by industry or government regulations are being followed and, critically important, documented.

To learn more, visit www.rapidfiretools.com or call 678-323-1300.