CyberQP

E-BOOK

The Security Automation Blueprint for MSPs

TABLE OF CONTENTS

Paul Redding,
SVP, Channel Marketing
and Community

INTRODUCTION

Thank you for downloading CyberQP's Security Automation Blueprint for Managed Service Providers.

This book gives you a complete guide to how your MSP can plot out and implement end-to-end automation across your security estate to augment your MSP technicians' efficiency and bring your company inline with the best practices required to stand up to today's threats and get coverage from cyber insurance vendors.

Together, we'll break down the trends that the CyberQP team is seeing today, explain what solutions you'll need to navigate today's cybersecurity landscape, and why that matters to both you and your clients, and how you can enhance your clients' security without sacrificing efficiency or your customer experience.

Thanks again for joining us, and let's make your security journey successful together.

CHAPTER 1

ACCELERATING MSP SECURITY OPERATIONS FOR TODAY'S THREATS

As the number of emerging threats continues to grow at an uncontrollable pace, attackers have recognized that targeting thousands of small-and-medium-sized businesses (SMBs) can be as profitable as targeting larger enterprise firms, with less effort.

Without tools designed for their specific needs or access to experienced cybersecurity professionals, SMBs face an uphill battle in keeping up with cyber criminals. Even if an SMB could afford to build out, staff, and train a dedicated security team and framework, enterprise firms can always afford to poach experienced professionals to fill their own talent gaps. To make matters worse, today's threat landscape has also made cyber insurance coverage more difficult to get, and more expensive to maintain.

In the face of these challenges, Managed Service Providers (MSPs) are the only solution to today's cybersecurity problems. This community of IT and security professionals can offer SMBs a human element to their cybersecurity, a helpful guide and support system for major issues, actually helping people when they have a cybersecurity problem.

However, in order to succeed, MSPs need to address these three key issues:

Evolving Attack Surfaces

As threat actors discover new vulnerabilities that they can exploit, the number of entry vectors and attack surfaces (across endpoints, the cloud, and beyond) they can target grows too. Furthermore, as SMBs adapt to the digital landscape, they create and rely on critical accounts, tools, and data for their day-to-day operations that they may not be aware of. It's up to an MSP to discover, monitor, and secure these privileged accounts and attack surfaces.

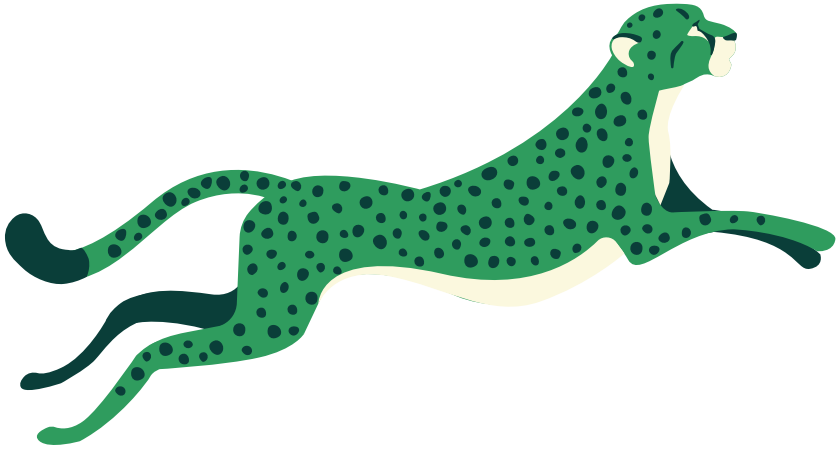
Existing Workflow Blockers

In the face of a major experience gap, MSPs need effective, automated solutions that both enable less experienced technicians and free up experienced professionals to focus on the projects and tasks that matter to your team by eliminating menial (and manual tasks), such as password reset tickets.

Addressing Identity-Based Issues

Today, cyber criminals continue to successfully steal sensitive user credentials, and navigate around today's elementary identity verification methods to gain access to sensitive accounts and data. And as MSPs and SMBs expand their operations, it's more challenging for technicians to tell if the person filing a ticket is who they claim to be.

In order to address these issues, MSPs need affordable, scalable solutions purpose-built for their mission. This guide will help you qualify potential additions to your security stack, so you can identify what you need in a cybersecurity partner for your end users, privileged accounts, and credentials.



CHAPTER 2

PUTTING THE POWER OF PASSWORD RESETS IN YOUR END USERS' HANDS

As hybrid work and Work From Anywhere policies become the norm, SMBs are no longer solely reliant on a local pool of talent. With the ability to hire professionals from the global talent pool, MSPs and SMBs may end up working with people that they've never met in person.

Moreover, as both an MSP and their clients grow, and as employees come and go, it can be difficult for your technicians to parse through which requests are legitimate - and which ones are from threat actors attempting to take advantage of this confusion and disguising themselves as a new or previously unintroduced employee.

To make matters worse, threat actors or impersonators can easily get around existing measures (like basic personal security questions), and these measures can mean longer times-to-resolution for password reset tickets, and a frustratingly slow customer experience.

In order to solve these issues, companies are adding another layer of security on top of their pre-existing passwords and multi-factor authentication (MFA) - biometric identity verification solutions. But unfortunately, too many of these solutions are designed for enterprise use (and restrictively expensive as a result).

MSP help desk technicians shouldn't have to be the final line of defense from an employee's account - and they need a way to free up the bandwidth that repetitive, manual tasks like password resets. What MSPs really need is a self-service password reset tool that will enable them to provide a better customer experience and optimize their workflows.

Password reset tickets amount to 20-30% of all help desk support requests	Password reset tickets cost up to a whopping $75 USD per incident.

The right password reset tool will put the power to get back online in an end user's hands and use modern security measures (such as biometric authentication) to eliminate frustrating phone calls and deter impersonation attacks. Moreover, a self-service experience will enable MSPs to resolve password reset tickets ten times faster.

CHAPTER 3

BUILDING THE FOUNDATIONS OF A ZERO TRUST HELP DESK WITH KEY AUTOMATIONS

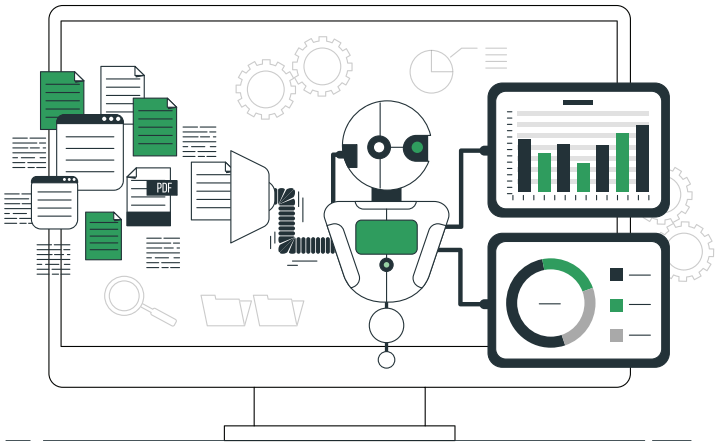
According to industry research, there are over 3.4 million vacant cybersecurity roles worldwide.[1] Unfortunately, this means that the cybersecurity landscape cannot keep up with the constant growing, unsatisfied demand for qualified workers, making it incredibly difficult for MSPs to find and hire talent from today's cybersecurity workforce, much less pay them a competitive salary.[2]

To make matters worse, even if an MSP finds the money and resources to build and staff a complete cybersecurity or SOC team, enterprise-level firms can either get to qualified talent first or poach promising candidates from the small-and-medium sized business (SMB) level.

That's why an MSP's tooling needs to be able to provide the same level of value across an MSP's team of techs, from the most skilled analysts to a non-technical Tier 0 technician with effective automations designed to accelerate ticket resolutions and make it easier to focus on the requests and tickets that truly matter.

In the case of password reset tickets, which make up to 20 or 30% of an MSP's support requests, and in the face of impersonation or social engineering attacks targeting credentials, MSPs also need a tool with built-in identity verification to make it quick and easy to screen callers, deter cyber criminals, all integrated with one management platform and across an MSP's technology stack.

While fraudulent account recovery and password reset requests have continued to plague internal IT and help desk technicians in recent years, it shouldn't be the most frequent single point of entry for a threat actor. By equipping a Tier 0 technician with automations and orchestrations designed for their needs, and security tools to filter out fraudulent requests, an MSP is prepared to create an effective front line against cyber criminals.



[1]ISC2 Cybersecurity Workforce Study 2022

[2]The State of Pentesting 2022: How Labor Shortages are Impacting Cybersecurity & Developer Professionals

CHAPTER 4

CUTTING OUT MENIAL TASKS WITH END-TO-END HELP DESK AUTOMATION

95% of your help desk tickets are costly, and require manual work that interrupts work that your technicians actually need to focus on. Moreover, today's help desk program models are not sustainable against constantly evolving threat actors launching social engineering attacks, using compromised credentials and looking for openings to deploy ransomware.

Ultimately, MSPs need to build a help desk program that implements automation to simplify their day-to-day workflows and optimize security. These automations need to help MSPs like you simplify end user identity verifications, and eliminate these manual tickets (including password reset requests). These automations should enable technicians of any skill level, enabling your team to achieve greater efficiency.

Moreover, they also need to streamline management, by giving your technicians one place to view a user account's status and sync passwords in real time.

But these automations also need to provide your MSP and your customers with an additional layer of security inline with today's best practices. Your MSP should be able to automate account provisioning, provide support across Active Directory and local accounts, as well as detect and track Active Directory password changes.

However, a key element of enabling end-to-end security automation is securing your privileged accounts - which we'll be covering in the next chapters.

CHAPTER 5

ACHIEVING BETTER DISCOVERY AND MANAGEMENT FOR YOUR TECHNICIANS

An average SMB employee may not know what a privileged account is, much less how to monitor one. However, as MSPs continue to grow by either adding new customers or merging with other MSPs through acquisitions, their security estates continue to steadily expand, as do the number of privileged accounts the MSP is responsible for.

However, identifying privileged admin accounts through discovery can be time consuming. And even if a MSP has complete visibility into every privileged admin account in their security estate (from Active Directory and Azure AD, to all of the local admin and service accounts), manually maintaining these accounts with regular password rotations is almost impossible.

So as MSPs continue to grow, how can they achieve and maintain that key visibility into and control over privileged accounts? How can they accelerate this discovery process and simplify management for these privileged accounts as they continue to scale their operations?

Questions like these are also driven by new cyber insurance requirements, who often ask MSPs how they manage privileged accounts, rotate key credentials, and configure accounts to align with best practices, such as the principle of least privilege.

The answer lies in Privileged Access Management (PAM) tools, which offer a set of tools and best practices to safeguard privileged accounts, whether they are local admin accounts across a client's endpoints or Azure AD/Office 365 tenant admins, the metaphorical keys to the kingdom.

Privileged Access Management enables MSPs to discover, monitor, and manage these privileged accounts using a variety of products including:

- A secure password vault
- Products that regularly rotate privileged credentials
- Temporary privilege escalation products
- Privileged account discovery tools
- Features that enable you to create documentation of client Windows credentials

By including these capabilities in your technology stack, your MSP can establish a strong foundation to defend against threat actors going after your company's (and your clients') key accounts.

CHAPTER 5

HOW TO IMPLEMENT A ROBUST PRIVILEGED ACCESS MANAGEMENT PROGRAM FOR MSP CYBERSECURITY TEAMS

Now that we've covered how Privileged Access Management enables MSPs with capabilities to help you discover and monitor privileged accounts, let's discuss what a good PAM solution will offer your MSP in order to accelerate your processes and improve security from end-to-end.

Your PAM partner should be able to offer **automated onboarding** that enables you to discover privileged accounts across your client base. Their tool should give you seamless integration with Active Directory, Azure AD, and Microsoft 365/O365 to enable quick and easy password syncs and automatic rotations without relying on AD syncs. This greater visibility should enable you to run account audits and ensure every user has an appropriate amount of access within an environment, and view access or password change histories with ease.

While some organizations may overlook local administrator accounts or service accounts, it's critical to secure these accounts and limit points of entry for cyber criminals. Any discovery or monitoring tools should be able to give you visibility into these, and also monitoring for stale credentials.

Your PAM partner should also offer integrations across your technology stack, integrating with your PSA to make password resets easier, or integrating with documentation tools like IT Glue and Hudu to securely document passwords, account information, and assets in a centralized, protected location, making compliance a breeze. A truly cybersecurity-focused partner may also offer their own **cyber grade vault** if an MSP is concerned about losing access to their documentation or about potential breaches.

Successfully cybersecurity programs focus on **people, processes, and technology**. The right partner for Privileged Access Management will enable MSPs to provide value to their people - from end users to experienced security professionals, and optimize their processes with technology purpose-built for their needs.

CHAPTER 7

CONCLUSION

By implementing solutions that address these issues and bring their clients in line with best practices, MSPs can secure their clients and build a scalable cybersecurity program that aligns with cyber insurance eligibility requirements, and best practices in line with compliance frameworks like NIST and CIS.

At CyberQP, we give you one security partner that helps you protect the information and accounts that matter to you. We help you keep your business secure and eliminate operational costs to maximize value for your customers.

Our privileged access management and security automation solutions enable you to protect customer admin accounts and secure customer identities. Our team is dedicated to offering the most comprehensive, intuitive, and useful solutions for MSPs to protect against cyber threats, automate help desk tasks, and adhere to compliance standards for greater productivity and a seamless IT management and monitoring experience.