CyberQP

E-BOOK

The Privileged Access Management Landscape for MSPs

Actionable Insights & Projections For the SMB Cybersecurity Landscape

TABLE OF CONTENTS

EXECUTIVE SUMMARY & KEY TAKEAWAYS

Thank you for downloading CyberQP's 2024 Privileged Access Management Landscape Report. We've compiled findings from research reports and industry experts across the cyber landscape to provide in-depth insights and analyses on the current state of the privileged access management landscape, and how MSPs can scale their cybersecurity programs with a growing business. Here are our key takeaways:

MSPs Face an Exponential Rise in Identity-Centric Attacks

Identity-based attacks and tactics involving malicious logins, compromised credentials, and unauthorized authentications are increasingly prevalent. In a report from the MDR provider Expel, identity-based threats accounted for **64%** of their SOC's investigations, a **144%** increase in attacks year-over-year.

MSPs Are Increasingly Concerned About Cyber Insurance

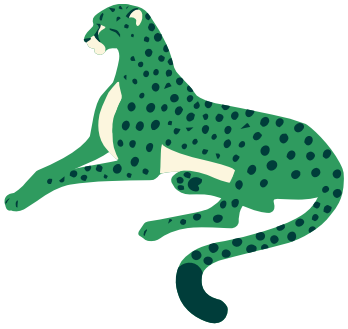
As lawmakers introduce new compliance frameworks, and cyber insurance providers begin enforcing stricter eligibility requirements, MSPs have pressing and costly incentives to offer cybersecurity services that align with required best practices- especially since SMBs accounted for 98% of claims in a 2023 NetDiligence study.

Threat Actors Increasingly Target MSPs and SMBs

Researchers confirm that threat actors are targeting all organizations regardless of size, especially as SMBs and MSPs deploy larger-scale services and infrastructure. According to the 2023 Verizon Data Breach Investigations Report, **58%** of reported breaches are targeted at SMBs. **54%** of these breaches involved compromised credentials, and social engineering attacks rank among the most common attack types.

Data Breaches Are Getting More Costly...

Especially for organizations with less than 500 employees. According to researchers from IBM, the average impact of a data breach increased **13.4%** for an SMB, from **$2.92** million to **$3.31 million USD**.

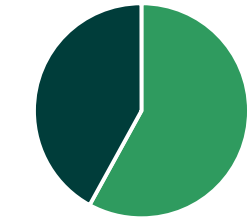


SMB CYBERSECURITY LANDSCAPE

With EDR, XDR, and MDR solutions becoming the norm, threat actors evolved beyond the traditional attack surfaces of compromising specific endpoints, servers, or cloud workloads.

While these attacks haven't stopped (ransomware and business email compromise remain the two leading attack vectors involved in cyber insurance claims, according to NetDiligence), cyber criminals have expanded their focus to a more vulnerable attack sector: compromised, stale, and reused credentials.

58% of reported breaches are targeted at SMBs.



SMB

Enterprise

54% of these breaches targeted and compromised an SMB's credentials.

SMB

Enterprise

SECURITY TIP

With these threats in mind, it's more important to account for human error than ever. Make sure your MSP is offering security awareness training to end users to ensure they can recognize threats like phishing attempts or impersonators, like in recent executive impersonation attacks.

Due to cyber criminals targeting privileged accounts in order to escalate their privileges or achieve lateral movement, SMBs are just as (if not more) vulnerable than their enterprise counterparts in the face of identity-based attack vectors.

On top of the usual cyber talent gap leaving SMB security estates vulnerable to exploitation, SMBs are likely unaware of the privileged accounts that keep their business' digital operations up and running. Moreover, MSPs face an uphill battle of creating named administrative accounts per technician in each of their customers' environments. Moreover, even when SMBs are aware of these risks and challenges, theydo not have the time or resources to manually rotate their privileged account passwords regularly.

Thus, the responsibility for discovering, monitoring, and managing these privileged accounts fall to the MSPs responsible for maintaining an SMB's security stack and their own security estates.

IDENTITY-CENTRIC
THREAT LANDSCAPE

Threat researchers across the cyber landscape, from MDR providers like Expel to analysts such as the Verizon DBIR team have observed an exponential increase in identity-centric threats from the year before, across different research in the threat landscape.

144% Increase Year Over Year in Identity Centric Threats (Source: Expel)

BEC attacks led to a combined loss of **$2.67 billion** for Americans in 2022.

40% of reported incidents were authentications to identity platforms like Microsoft Entra ID, Ping Identity, and Duo.

74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of Stolen credentials or Social Engineering.

The number of reported incidents involving unauthorized authentication through major platforms like Microsoft Entra ID, lead us to predict a renewed call for passwordless login solutions in the MSP landscape to offer a secure alternative to these enterprise-centric solutions.

THE MSP LANDSCAPE IS GROWING EXPONENTIALLY

Despite (or perhaps because) of the challenges their SMB customers face today, MSPs are still growing steadily in the face of economic headwinds.

Researchers believe that the MSPs that have survived and thrived in this landscape demonstrated flexibility and ability to drive efficiency with their offering, whether by offering co-managed IT for their clients or by adopting more flexible payment terms if they offer a hardware-based solution.

64.7% of MSPs in the United States and EMEA experienced a revenue increase.

38% of the surveyed MSPs above saw their revenue grow by more than 10%.

.

MSP GROWTH PROJECTIONS

Conservative Estimates

Gartner

Gartner predicts global IT spending will grow by 6.8% in 2024.

Encouraging Estimates

canalys

Canalys analysts project that managed services revenue will grow by 12% in 2024.

In a recent Canalys poll, 56% of channel partners expected over 10% year-on-year growth in their managed services businesses in 2024. A quarter of all partners in the same poll expected over 20% growth.

M&A activity in the MSP channel **will grow 50% in 2024,** according to Canalys.

Cybersecurity managed services revenue **will grow 15% in 2024.**

CYBER INSURANCE FINDINGS

Did You Know?

SMBs accounted for **98%** of cyber insurance claims, and **46%** of total incident costs analyzed in a 2023 study by NetDiligence.

The Cost of an SMB Data Breach

265 of reported SMB claims in NetDiligence's study cost more than $500,000 USD, and 254 of these claims were more than $1 million USD.

As data breaches grow more costly for SMBs, and as cyber insurance providers begin reinforcing stricter eligibility requirements and raising premiums to the point that they're restrictively expensive for even the most lucrative enterprise security decision makers, and impossible to acquire for MSPs and SMB stakeholders.

Only 26% of enterprise security decision makers have a standalone cyber insurance policy. Here's what coverage MSPs should expect from a standalone policy vs. cyber insurance packaged into other policies.

STANDALONE POLICY COVERAGE

- Comprehensive, security-specific coverage
- Up to $15M USD in coverage
- Streamlined claims, most likely to be accepted
- Access to security experts in an incident
- Premiums decided through risk assessment

PACKAGED POLICY COVERAGE

- Coverage limited to data breaches
- Vague coverage description
- Limited coverage and claims are more likely to be denied
- Little to no security expert support
- Lower premiums

COMPLIANCE FINDINGS

However, tightening cyber insurance eligibility requirements make it more challenging for MSPs to fulfill their responsibilities, and while industry reports largely focus on larger cloud security adoption, we believe that in our next annual report, we'll see an increase in identity security tooling adoption to align with compliance and cyber insurance controls.

Moreover, as the CMMC framework reaches the end of its public feedback period and lawmakers begin planning for its implementation and enforcement, more MSPs are looking at how they can comply with the outlined best practices.

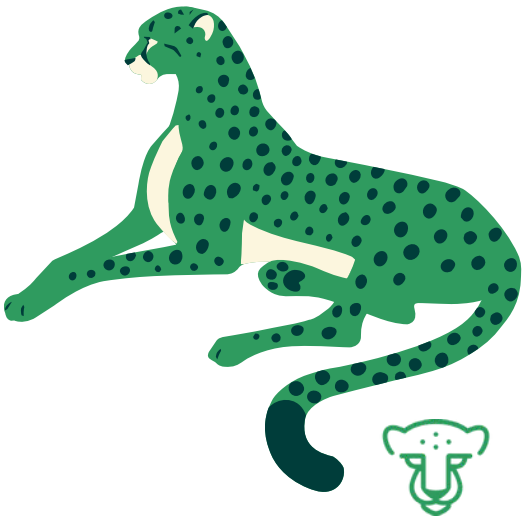
Researchers from Verizon recommend that MSPs look at aligning with security safeguards like CIS Control 5 which calls for privileged access management, CIS Control 11, which requires data recovery processes and automated backups, and CIS Control 14, which requires security awareness training on social engineering attacks, authentication, and best practices among other topics.

CIS CONTROL 5: ACCOUNT MANAGEMENT

- Establish and Maintain a Privileged, Service and End User Account Inventory (Safeguards 5.1 & 5.5)
- Require and Enforce Unique Passwords (with 8 characters for MFA-enabled accounts, and 14 characters for accounts without MFA) (Safeguard 5.2).
- Adopt Zero Standing Privilege and Least Privilege by Disabling Dormant Accounts & Restricting Admin Privileges, all from one dashboard. (Safeguards 5.3, 5.4, and 5.6)

SECURITY TIP

To support CIS Control 11's requirements, make sure that your MSP has a strong BCDR solution and strategy in place.



PRIVILEGED ACCESS, IDENTITY, & MSP

RECOMMENDATIONS IN 2024

Streamline capabilities and tech stacks in 2024.

We project that MSPs that focus on optimizing their ROI from their existing solutions with automations or integrations between existing tools will be more prepared to assess their cyber risks and prepare for changes to compliance frameworks or best practices.

MSPs should prepare to support external stakeholders to succeed in 2024.

Specifically, we project that MSPs with the technology to manage privileged access without expanding attack surfaces will be better-positioned and allow themselves to advertise a secure co-managed IT arrangement and fight the current cyber skills shortage.

Invest in IAM software to potentially save data breach costs.

According to research from IBM, organizations investing in IAM saved $180,358 during a breach. MSPs have a great opportunity to mitigate potential breach costs for their clients and themselves with a streamlined security stack designed to deter and respond to cyber threats. In fact, research also states organizations that engage an MSSP save $73,082 in data breach costs.

”Focus on managing privileged user accounts... with elevated access.”

The quote above is a recommendation from security experts at IBM. **32% of organizations surveyed by IBM plan to invest in IAM solutions after a breach,** and MSPs will need robust visibility and controls over these accounts by security group, role or organizational unit.

THANK YOU!

Works Cited

- Verizon Data Breach Investigations Report 2023." Verizon. Accessed February 1, 2024. https://www.verizon.com/business/resources/reports/dbir/.
- Walton, Aaron. "Expel Annual Threat Report 2024." Expel. Last modified January 23, 2024. https://expel.com/annual-threat-report/.
- Ody, Robin. "MSP Predictions 2024 - Executive Summary." Canalys. Last modified January 30, 2024. https://www.canalys.com/insights/msp-predictions-2024-executive-summary.
- Ody, Robin. "Partners Are More Bullish on Managed Services in 2023." Canalys. Last modified June 20, 2023. https://canalys.com/insights/partners-are-more-bullish-on-managed-services-in-2023.
- "Gartner Forecasts Worldwide IT Spending to Grow 6.8% in 2024." Gartner. Last modified January 17, 2024.https://www.gartner.com/en/newsroom/press-releases/01-17-2024-gartner-forecasts-worldwide-it-spendingto-grow-six-point-eight-percent-in-2024.
- Fichtner, Elizabeth, Amy Newman, Holly Pateman, Elise Rodriguez, and Eileen Weinberg. "Datto's Global State of the MSP Report: Trends and Forecasts for 2024." Datto, Inc. and Strategy Analytics. Last modified November 8, 2023. https://www.datto.com/resources/dattos-global-state-of-the-msp-report-2024.
- "Standalone vs Packaged Cyber." Cowbell Cyber. Last modified February 2021. https://cowbell.insure/wpcontent/uploads/2021/02/Cowbell-Standalone-vs-Packaged-Cyber.pdf.
- Chatfield, Dave, Heather Osborne, Sharon Lyon, Cait Osborne, Heather Goodnight-Hoffman and Patrick Florer."NetDiligence Cyber Claims Study: 2023 Report." NetDiligence & Risk Centric Security, LLC. Last modified October 2023. https://netdiligence.com/wp-content/uploads/2023/10/2023-NetDiligence-Cyber-Claims-Study_v1.1.p "Cost of a Data Breach Report 2023." IBM Security & Ponemon Institute. Last modified July , 2023. https://www.ibm.com/reports/data-breach.
- Shey, Heidi. "The State of Cyber Insurance 2023." Forrester. Last modified August 24, 2023. https://www.forrester.com/blogs/the-state-of-cyber-insurance-2023/.
- "CIS Controls Navigator." Center for Internet Security. Last modified May 18, 2021. https://www.cisecurity.org/controls/cis-controls-navigator.

Ready to take the next step? Book a demo with CyberQP here.

CyberQP redefines help desk security through privileged access management, help desk verification, and user privilege elevation. We empower MSPs and IT professionals to eliminate standing privilege risks, enforce compliance, and streamline operations. Committed to "Securing IT, One Privilege at a Time," CyberQP protects accounts, credentials, and identity verification with innovative, efficient solutions. Learn more: https://cyberqp.com/product-tours/