WHITE PAPER

The 2019 APAC Cybersecurity Survey

Four Key Findings for Service Providers Based on Original Research from SolarWinds

solarwinds msp

You've put multiple security controls in place.

You patch regularly, have endpoint detection and response solutions on your machines, and regularly back up critical data and systems in case of a ransomware attack. In short, you do the right things to prevent cybercriminals from harming your customers.

Unfortunately, you may still face a breach caused by one of their internal employees. Something as simple as an employee with a weak or reused password could cause an incident. Sometimes, we lose sight of internal threats in favor of external ones. This is one of the major findings we uncovered in our recent survey of technology professionals.

We surveyed 101 companies across Singapore and Hong Kong about their security practices and top challenges. Respondents included service providers and in-house technology professionals from both the public and private sector.

*We surveyed **101 companies** across Singapore and Hong Kong about their security practices and top challenges.*

We wanted to better understand:

- Trends surrounding security breaches and the threat landscape at large
- Technologies that tech pros use for security—and management challenges they face
- Professionals' confidence in their preparedness to manage the trends and technologies of the future
- Expected security budget changes in the near future

Below are four significant findings, as well as some advice, using the data we collected to further strengthen your security posture.

1. INSIDER MISTAKES TOP THE LIST OF SECURITY BREACH CAUSES

When asked about the root cause of security incidents over the previous twelve months, 65% of respondents cited "insider mistakes" as the culprit (only 12% said insider breaches were malicious). The good news here is most employees are honest and don't want to deliberately cause damage. The bad news, however, is businesses need more safeguards to prevent people from tripping over their own feet.

Looking further into the data, 66% said regular employees were to blame for one or more incidents, while 53% cited privileged admins. This makes sense—regular employees aren't as security conscious as admins. However, as an MSP, you have a heightened responsibility to help ensure your tech admins don't cause security breaches at your customers' sites. So pay particular attention to keeping your own MSP's security house in order.

Finally, we looked at what causes these incidents. The top reasons were bad passwords (46%), accidentally exposing, deleting, corrupting, or modifying critical data (45%); copying data to unsecured devices (38%); and not applying security patches (36%). This is a pretty broad mix of issues, but better password policies, consistent patching (and forced restarts as needed), and regular security trainings could help mitigate some of the risk.

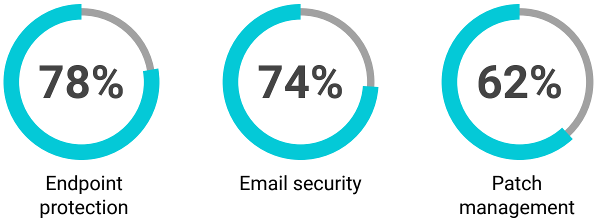
CAVEAT

We're not saying people should shift away from dealing with external threats. 43% of breaches came from external threat actors. That's still very high. Plus, a malicious external actor can do serious, long-term damage to an organization. You need to maintain a healthy mix of defense against both internal and external threats. You may need to assess the likeliest risks for your clients to best decide how to secure their systems.

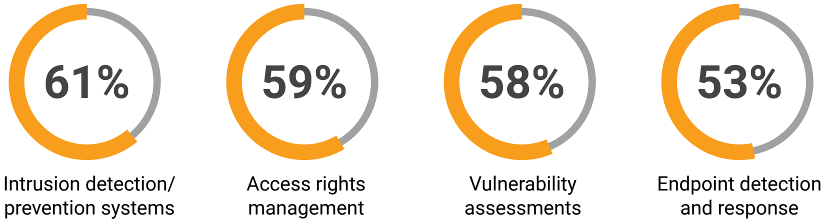
2. TECH PROS ARE USING A SOLID MIX OF SECURITY TECHNOLOGY

Next, we looked at the mix of technology solutions organizations use to detect and respond to threats. Here are the top responses in each group:

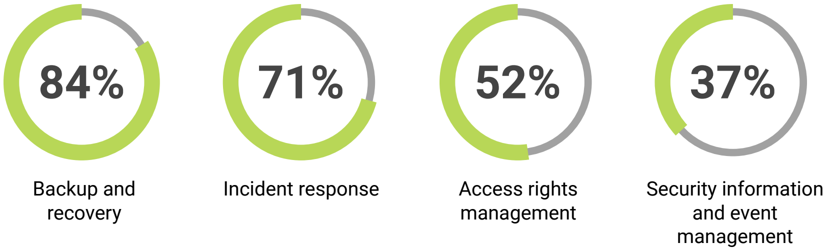
Protect



Detect



Respond



Let's start with **protection**. Respondents did a good job of adopting endpoint protection (78%) to keep advanced threats from breaking individual machines. Plus, many still use email security to prevent incoming email threats (74%), which is beneficial as it's one of the top threat vectors. However, even at 62%, patch management is still too low. This is the basic blocking and tackling of security—teams can't afford to slip up on this.

Next, let's talk **detection**. Some good numbers here were the usage of intrusion detection and prevention systems (61%), access rights management (59%), vulnerability assessments (58%), and endpoint detection and response (53%). It's promising that 61% use IDS/IPS systems, and even better that we're seeing high adoptions of endpoint detection and response at 53% (although, this number could improve as well).

Yet, only 35% used security-information-and-event-management (SIEM) tools for detection and only 28% use threat intelligence. By giving teams a central location to collect and analyze logs and security alerts, SIEM tools can provide a much-needed efficiency boost when tackling incoming security events. At only 28%, threat intelligence adoption is abysmally low. While you can prevent a good number of threats without any external threat intelligence, some of the most devastating threats are those you don't see coming. The right threat intelligence sources can offer much needed context to security events, allowing your team to tackle the most pressing emerging threats while ruling out false alarms quicker.

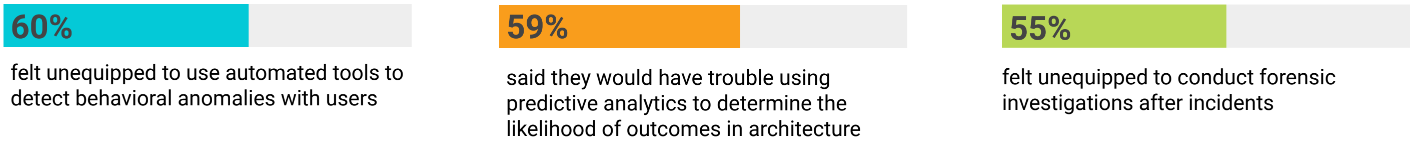
*Yet, **only 35%** used SIEM tools for detection and **only 28%** used threat intelligence.*

For **response**, the data seems straightforward. Backup and recovery were well represented, as were incident response (IR) tools. Again, though, without a SIEM to detect and provide context to the issues in the first place, teams relying solely on IR tools may miss important threats.

3. TECH PROS HAVE GAPS IN THEIR SKILLSET

Next, we asked participants if they were confident in their ability to handle the security tasks required to tackle today's threat landscape. Of the participants, 97% felt unequipped for at least one or more tasks we listed. Teams could benefit from additional training in these areas—and vendors may want to work to improve the user experience of their products.

Top 3 Gaps



60% felt unequipped to use automated tools to detect behavioral anomalies with users

59% said they would have trouble using predictive analytics to determine the likelihood of outcomes in architecture

55% felt unequipped to conduct forensic investigations after incidents

We'll discuss the top three areas of concern. First, 60% felt unequipped to use automated tools to detect behavioral anomalies with users. With the sheer number of threats facing businesses every day, choosing automated tools can help teams wrap their arms around the chaos of modern IT environments. Plus, with insiders identified as a top cause of incidents, behavioral analysis could help teams reduce risks.

Second, 59% said they would have trouble using predictive analytics to determine the likelihood of outcomes in architecture. As an MSP, you may benefit from using predictive analytics to better assess your customers' security weak points. Predictive analytics can help teams better assess risk, select appropriate controls, and set the right security policies.

Finally, 55% felt unequipped to conduct forensic investigations after incidents. If teams can't identify the origin and pattern of an attack, a repeat incident could occur, or cybercriminals could sit on the systems for months without being discovered, leaving the organization open to significant risks. While security engineers and forensic investigators do have different skillsets, you may want to invest in building out at least the basics of this function to keep your customers from getting attacked multiple times.

4. TECHNOLOGY PROFESSIONALS FACE MANAGEMENT-LEVEL BARRIERS

Finally, we asked respondents about the top barrier to improving or maintaining their security. Each respondent could choose only one answer. 36% answered that a lack of budget was the top barrier, while 18% cited competing priorities or initiatives.

TOP BARRIERS

***36%** answered that a lack of budget was the top barrier, while **18%** cited competing priorities or initiatives.*

Despite budget increases, many tech professionals still feel funding is inadequate to defend against today's threats. As cybercriminals continue innovating, defenders will need more budget. Don't expect this to change any time soon.

As an MSP, the budget issue may seem concerning on its face. However, don't forget that the respondents answered what the biggest barriers were to improving their security posture. This doesn't imply there won't be enough budget for security services for MSPs—it simply means teams want more budget.

In fact, the second point could be great news for MSPs. A good portion of respondents were in-house. When faced with competing priorities and initiatives, organizations may decide to keep their IT team on core business functions while outsourcing more security to MSPs.

WHAT YOU CAN DO

The data shows multiple opportunities for MSPs to improve their security offerings—and even capitalize.

For starters, **implement strong password policies and use a password manager**. With poor passwords cited as the leading cause of insider mistakes, implementing a corporate password manager can help you better enforce password security policies—both within your own MSP and at your customers' sites.

Second, **implement and deploy endpoint detection and response to your customers**. A little more than half of respondents use it to protect their customers. That's a good start, but we hope to see wider adoption. Since many modern threats are designed to evade traditional antivirus products, implementing an endpoint detection and response solution can help handle more advanced threats and keep your customers' endpoints safe.

Third, we can't overstate the importance of **security training** to prevent insider mistakes. Hold them for both your customers and your technicians. Make the training engaging, and also make sure people leave with handouts they can bring to their desks to retain information for the long haul. For your customers, it's worthwhile to periodically send emails to remind them of key security practices. This not only helps keep your customers safe, but also gives you plenty of opportunities to communicate your value.

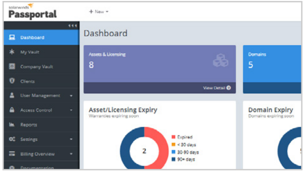
Fourth, **patch**. Get a good patch management solution to help keep machines up-to-date across the enterprise. Earlier in this eBook, we mentioned that 36% of insider mistakes came from unapplied patches. Despite this, only 62% of respondents use a patch management solution. This is way too low. Instead, consider getting a patch management solution that allows you to automate much of the process.

Fifth, organizations expect their MSPs to **recover business continuity fast after a downtime event**. This means MSPs need strong backup solutions that allow for rapid recoveries. While adoption was high among respondents, it's important to realize that backup comes in multiple flavors. For example, MSPs counting on local backups for fast restores could be in for a rude awakening if a cybercriminal deletes local backups during a ransomware attack. To combat this, pick a backup solution that's purpose-built for fast, secure cloud transfers.

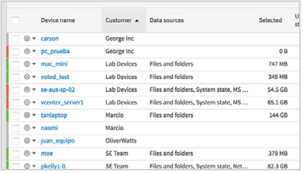
Finally, more organizations should **adopt SIEM tools** to help them better discover, contextualize, and manage security notifications. SIEM tools allow teams to centralize their security logs and, in many cases, add proper context via built-in threat intelligence. Plus, a strong SIEM tool with robust search capabilities can help teams more easily perform forensic analysis after an incident and, hopefully, close vulnerabilities to prevent reoccurrence.

HOW SOLARWINDS CAN HELP

SolarWinds MSP offers multiple tools to help you tackle the major issues facing teams today. Of particular relevance to this study, **SolarWinds® Passportal** is designed to help you enforce better password policies for your MSP to help keep your customers' data safe.
Learn more at passportalmsp.com.

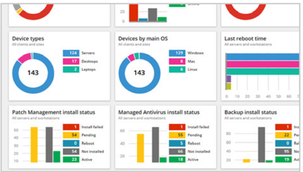


SolarWinds Backup is designed to simplify data protection and recovery. One web-based dashboard lets you view backup statuses across your customer base and offers multiple recovery options including bare metal restores and virtual disaster recovery. Plus, SolarWinds Backup was built cloud first, and uses multiple techniques to speed up data transfers for faster backups and rapid recoveries. And there's no need to purchase an expensive backup appliance.
Learn more at solarwindsmsp.com/products/backup.

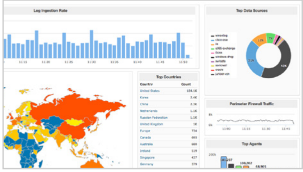


Device name	Customer ▲	Data sources	Selected
carson	George Inc		
pc_prueba	George Inc		0 B
mac_mini	Lab Devices	Files and folders	747 MB
volod_test	Lab Devices	Files and folders	345 MB
se-aus-sp-02	Lab Devices	Files and folders, System state, MS …	54.5 GB
vcenter_server1	Lab Devices	Files and folders, System state, MS …	65.1 GB
tanlaptop	Marcio	Files and folders	144 GB
naomi	Marcio		
juan_equipo	OliverWatts		
moe	SE Team	Files and folders	379 MB
pkelly1-lt	SE Team	Files and folders, System state, Net…	82.3 GB

Additionally, **SolarWinds RMM** offers multiple security tools, including automated patch management, web protection, email protection, and endpoint detection and response, within a single, web-based platform. This lets you practice and enforce strong cyberhygiene principles across your customer base without needing a multitude of disparate tools.
Learn more at solarwindsmsp.com/products/rmm.



Finally, we focused a lot on the importance of SIEM tools. **SolarWinds Threat Monitor** is built to help you detect threats across your customer base. With built-in alarms and the ability to customize alerts, you can set up Threat Monitor to fit your needs.
Learn more at solarwindsmsp.com/products/threat-monitor/.



Top Countries

Country	Count
United States	184.1K
Korea	2.4K
China	2.3K
Netherlands	1.1K
Russian Federation	1.1K
United Kingdom	1K
Europe	734
Canada	695
Australia	680
Ireland	519
Singapore	437
Germany	379

SolarWinds (NYSE:SWI) is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures. Targeted for MSPs, the SolarWinds MSP product portfolio delivers broad, scalable IT service management solutions that integrate layered security, collective intelligence, and smart automation. Our products are designed to enable MSPs to provide highly effective outsourced IT services for their SMB end customers and more efficiently manage their own businesses.

Learn more today at
solarwindsmsp.com

This document is provided for informational purposes only. SolarWinds makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information.