computing research

RESEARCH PAPER

Best practice makes perfect: malware response in the new normal

August 2020

Sponsored by

Malwarebytes

CONTENTS

Introduction

Cyber security teams already confessed to being overworked before COVID-19 – battling simply to keep their heads above a constant tide of security alerts, across numerous tools and reports. High profile security breaches, with malware at their root, were a seemingly weekly occurrence. The financial and reputational damage that followed were often as hard to recover from as the attack itself. It comes as no surprise that some businesses have resorted to simply paying off cybercriminals.

The effects of the COVID-19 pandemic are an added burden to the cyber risks security operations centre (SOC) teams are battling against. The massive rise in the number of employees working entirely from home, outside the traditional secure office environment, is testing pre-conceived notions of how to work safely and securely.

Computing surveyed around 150 cyber security decision-makers, representing organisations from a wide variety of industries, including education, finance, technology manufacturing and the public sector, to gain a detailed picture of the challenges facing security teams in the modern environment.

Our objectives were to explore how SOC professionals were reacting to the rise in remote working, especially the increased susceptibility of employees to malware attacks; identify how such attacks have changed in terms of scale and sophistication; and examine the importance of quickly isolating and remediating an attack. The research also looks at how to secure their organisations after the pandemic.

Key findings

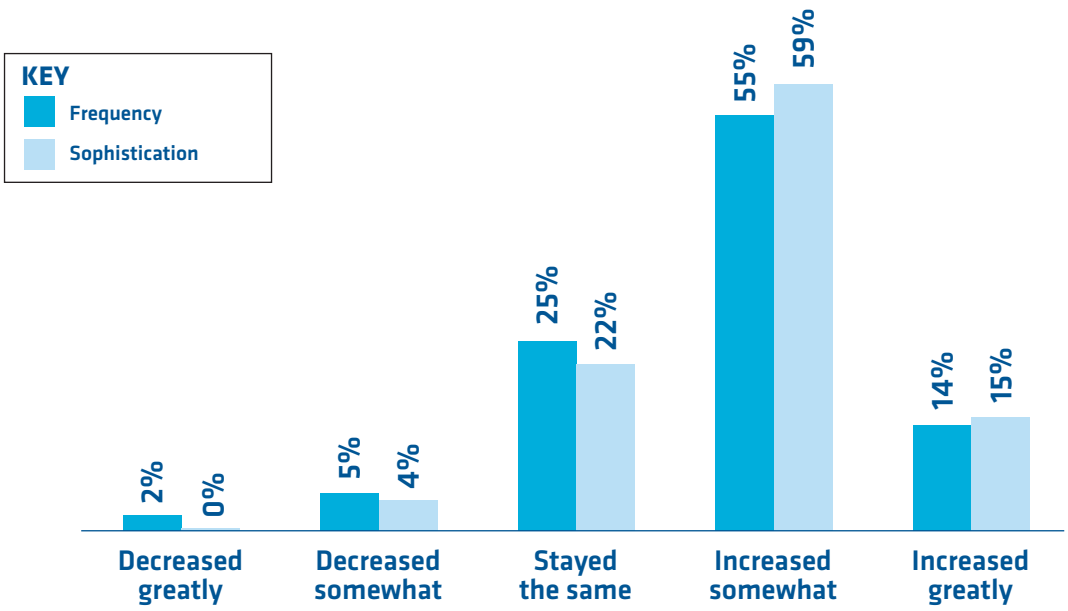
- The scale and sophistication of cyberattacks continue to climb, with 69 percent of respondents indicating that malware attacks against their organisation had increased in the past two years. Nearly three-quarters said that such attacks had also become more sophisticated.
- Cyber crime is becoming more professional. Help desks exist, and anyone can buy a basic exploit kit. At the same time, criminals are becoming more adapt at targeting critical parts of an organisation.
- Security professionals widely accept that their organisations will, at some point, suffer a breach, and more than 80 percent that malware remediation is just as important as prevention. However, only 17 percent were very confident in their ability to effectively respond to an attack.

- 82% say that remediation is just as important as prevention in an effective response strategy – but only 17 percent were very confident in their organisation's ability to recover quickly from a malware attack.
- Remote working has undergone a massive surge in the COVID-19 crisis, and 89 percent of companies we surveyed had increased their instances of remote working. Nearly three-quarters had more than half their employees working remotely at the time of our survey.
- The effects of COVID-19 on business have exposed new vulnerabilities to attackers. More than half of organisations had seen malware attacks playing on fears around COVID-19, and 44 percent said they were more susceptible to malware as a direct result of the increase in remote working. Many organisations – more than 60 percent – have changed or are changing their cybersecurity strategy to account for this.
- Anti-malware, VPNs and employee training – versatile, simple and cost-effective techniques – are the most popular security tools used to protect remote workers. More expensive and complex techniques, like SD-WANs and dedicated work-only networks, were much less common, but will probably rise in popularity if the remote working trend continues – which most firms expect to be the case.

Malware keeps climbing

It is no secret that cyberattacks are changing – from the targets to the techniques and the type of damage they wreak. In our research, more than two-thirds (69 percent) of respondents said that malware attacks against their organisation had increased greatly or somewhat in the past two years, and nearly three-quarters (74 percent) indicated that such attacks had become more sophisticated.

Fig. 1: How has the frequency and sophistication of malware attacks changed at your organisation in the last two years?



The rise in attacks comes alongside a clear trend towards the industrialisation of cybercrime. Attackers are more professional than ever, and many malware tools are now available as plug-and-play exploit kits for anyone to purchase and use. On top of that, businesses are now a major target for threat actors using vectors like trojans, botnets and ransomware – although adware also remains a staple of the criminals' portfolio.

While basic attack kits do exist, our research showed that respondents felt the sophistication of attacks was increasing. Many now use exploits, credential-stealing tools and multi-stage infections to achieve their ends, on top of the common – but, again, increasingly sophisticated – phishing and social engineering techniques.

It is not only attack vectors that are evolving, but the targets. More and more, criminals are not content to simply access a network, but specifically aim at 'crown jewel' data like customer lists, or mission-critical systems like industrial controls. These actions can easily cripple or even destroy a firm's business, especially if the attackers decide to not just copy information, but actively damage its integrity.

With the increasing scale and sophistication of attacks, even the most secure firms will suffer a breach from time to time. Twenty-seven percent of cyber security professionals said that there had been a successful malware attack at their company in the last two years, and 6 percent answered 'Don't know' – which in this context, we can take as a tacit acknowledgement. It should also be concerning that anyone with responsibility for cyber security strategy or implementation – as all of our respondents were – might not know if their organisation had been breached.

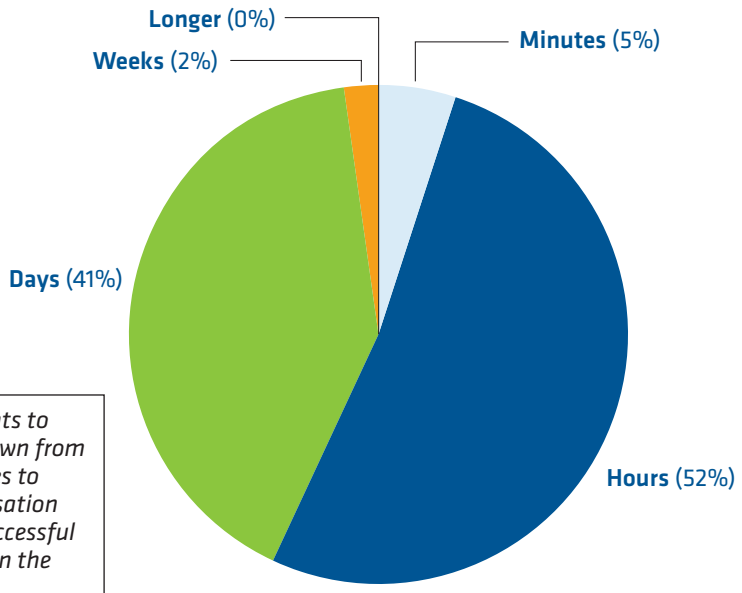
All cyberattacks are designed to be difficult to remediate, and modern malware takes this to a new level. Some strains lie low and work quietly, while others are more overt but lock users out of important remediation systems and tools. Regaining that access is critical, and 82 percent of respondents said that remediation is just as important as prevention in an effective response strategy – but only 17 percent were very confident in their organisation's ability to recover quickly from a malware attack.

While most respondents were able to address a malware breach in minutes or hours, a significant number (41 percent) took days to get up and running again. The remainder – just 2 percent – took weeks. *See Figure 2, next page*.

Being locked out of important systems and unable to work is difficult to bear, and the temptation to pay a ransom is always present; indeed, it is the business model that most malware attacks are built around. That said, there is only a chance of getting system and data access back after paying a ransom – attackers might also have corrupted it beyond repair, and that money then goes on to fund future attacks. Thankfully, the incidents of paying cybercrime ransoms are low: just 5 percent of our survey respondents had done so, with 2 percent preferring not to say.

82 percent of respondents said that remediation is just as important as prevention in an effective response strategy – but only 17 percent were very confident in their organisation's ability to recover quickly from a malware attack.

Fig. 2: Please indicate how long it took to remediate the attack?

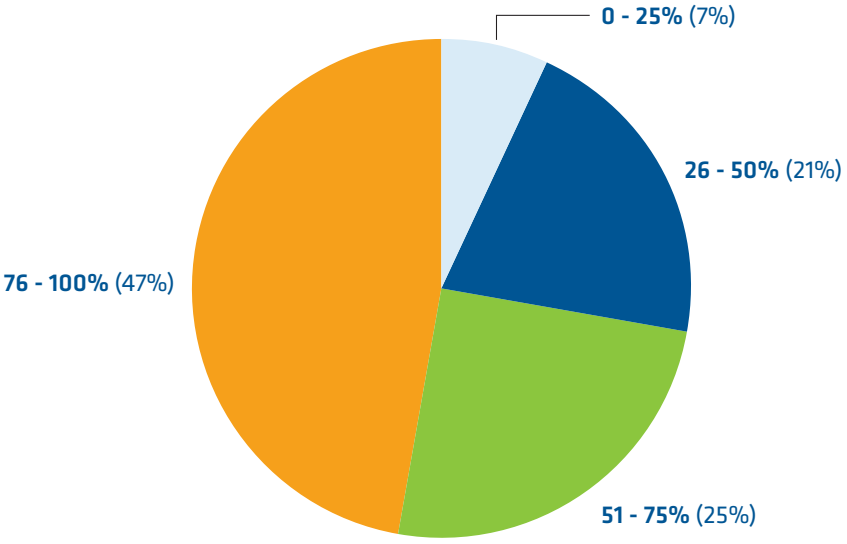


Note: Respondents to this question drawn from positive responses to 'Has your organisation experienced a successful malware attack in the last two years?''

The future of work?

While remote working's popularity has been steadily increasing for years, the COVID-19 pandemic has accelerated that transition – and related malware attacks. Many organisations that had previously ignored the possibilities of remote working were forced to quickly devise rules, policies and contingencies for doing so; but the sheer scale of the rise - 89 percent of companies in our research had increased remote working - has even challenged those firms where it was already supported.

Fig. 3: What proportion of your workforce are currently working remotely?

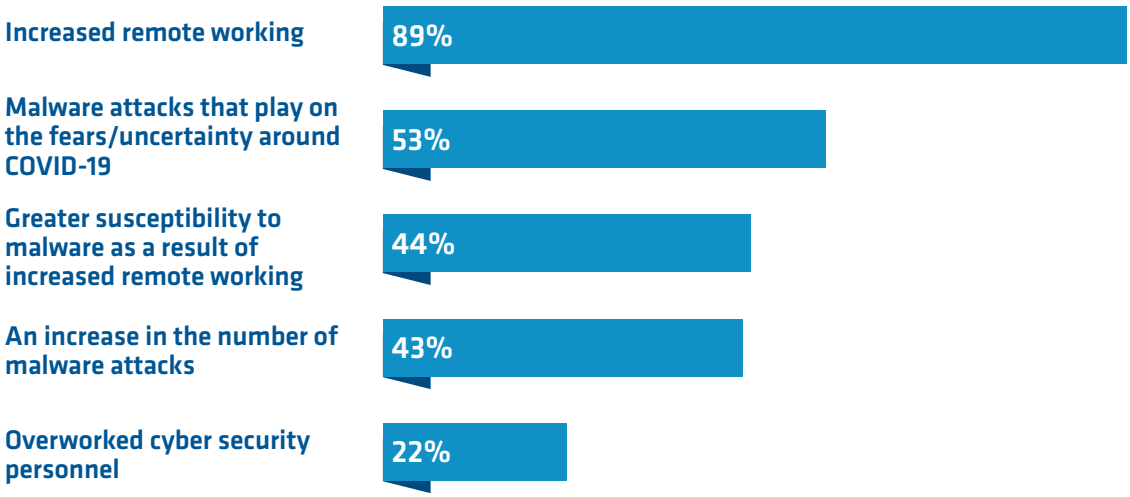


Almost half of the companies we surveyed had three-quarters or more of their employees working from home as a result of COVID-19. On the opposite end, about a third of companies had half of their employees or fewer working remotely, which may be due to the nature of their work.

Remote working has many benefits: increased flexibility, more spare time and money and a degree of autonomy. Many employees become more productive in this environment, once they have become used to not going to an office to get their work done.

However, the balancing act between work and play is perhaps the biggest drawback of remote working. It takes discipline, and an employee who has spent their entire career with a clear distinction between the office (work) and their house (play) may struggle. Aside from the normal distractions of home – other people, home electronics, pets – being in that familiar location can impart a false sense of security when it comes to...well, security!

Fig. 4: Which of the following effects have you experienced during the COVID-19 pandemic?



Whether it is using an unsecured WiFi hotspot, entering sensitive information on an unsecured device or visiting personal websites on a company laptop (or vice versa), employees often blur the boundary between their office and home lives when working remotely. Forty-four percent of respondents told us their companies had become more susceptible to malware attacks as a result of increased remote working, and more than half (53 percent) said they had seen attacks that played on fears and uncertainties around COVID-19 – establishing a clear need to focus on securing virtual environments.

Security during a global crisis

Cyber security is at the top of many organisations' priorities at the best of times, and the global pandemic has exaggerated the need for strong defences. Sixty-one percent of security professionals said that their companies were changing their cyber security strategy to enable increased remote working, with just 14 percent disagreeing.

Fig. 5: Which of the following technologies are you using to provide greater security to remote workers? Please select all that apply.

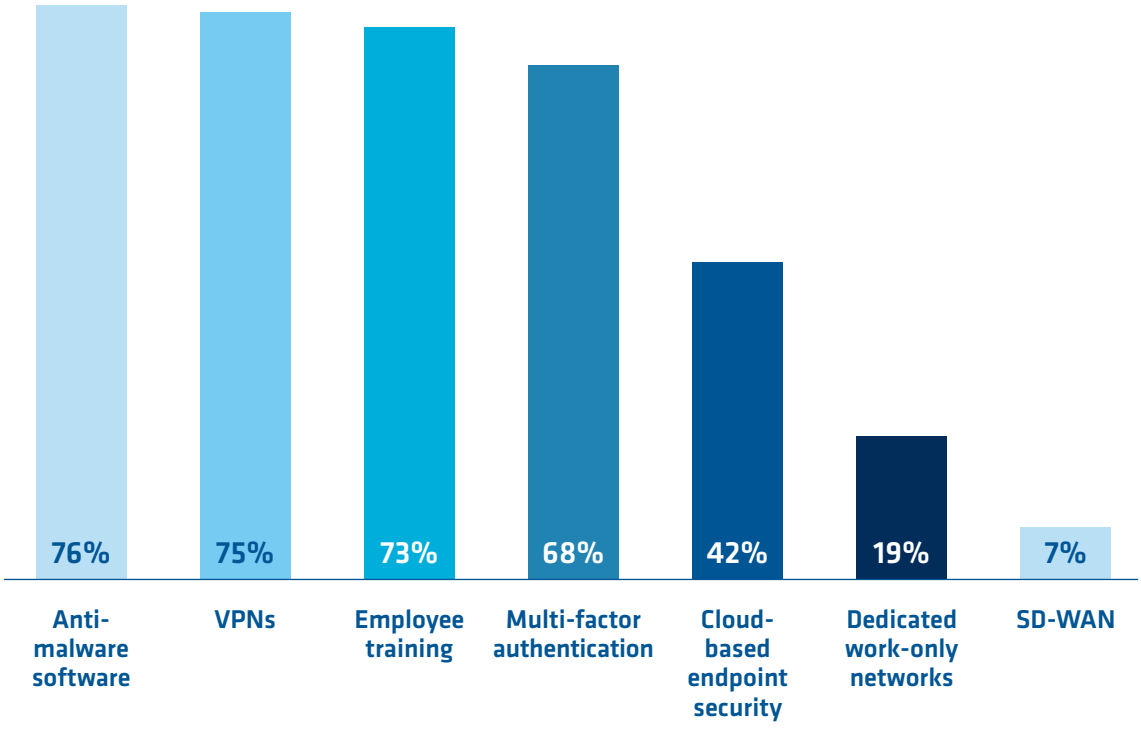
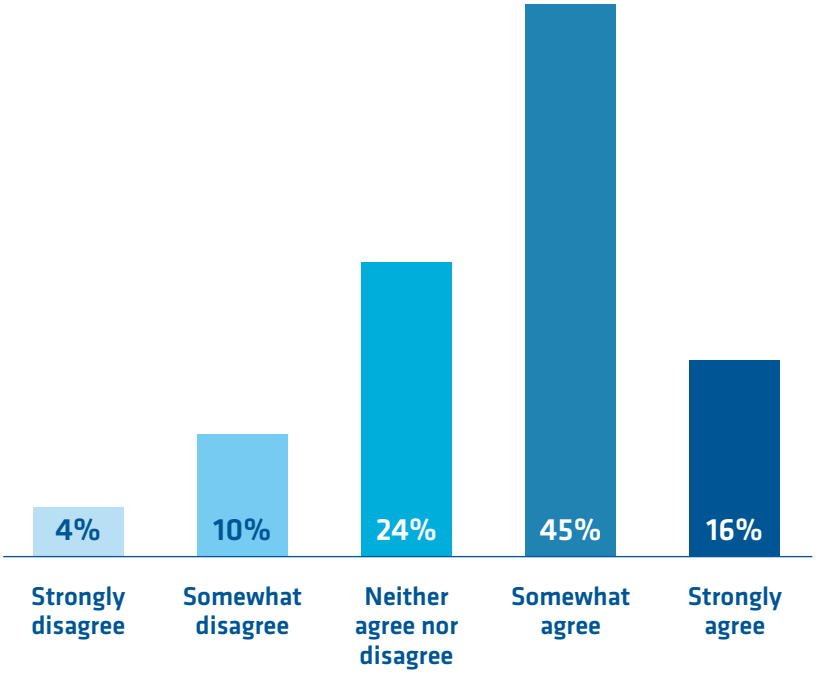


Fig. 6: To what extent to you agree with the statement, "We are having to change our cyber security strategy to enable increased remote working"?



Anti-malware is the first port of call for security professionals, and these types of software have a clear place in remote working environments, especially considering the increase in malware attacks and susceptibility to the same experienced in recent months (see above).

While there are many forms of cyber protection, anti-malware is one of the most versatile and cost-effective. Subscription packages are inexpensive for the security they offer – such as file and password protection, spam blocking and guarding against malicious software – so it should be no surprise to see this technology at the top of survey respondents' choices to protect their remote workers.

Investing in anti-malware mechanisms that provide automated endpoint incident response will significantly accelerate remediation efforts and will allow organisations to recover quickly – detecting and resolving breaches wherever they occur before they're allowed to spread. This is a particularly important point given that just 17 percent were very confident in their organisation's ability to recover quickly from malware attacks. Fortunately, respondents are aware of the importance of malware removal capabilities here – with 69 percent saying it will be critical in the immediate future.

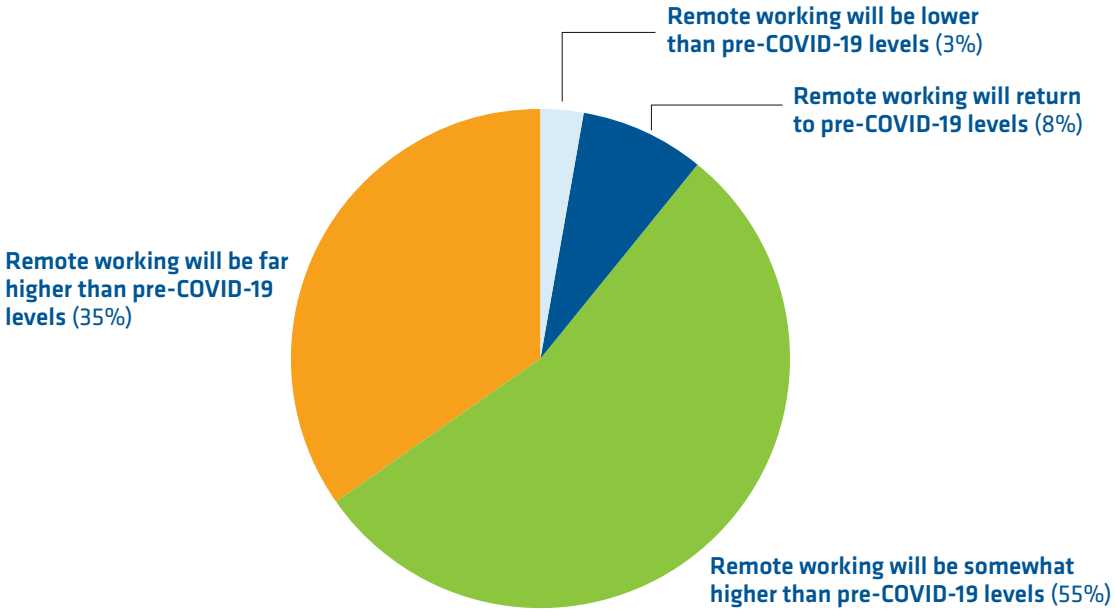
Anti-malware also has the advantage of simplicity, which could be just as important as the level of security offered, depending on the industry and employee. However, there is no need to rely on a single solution; the most secure option is to utilise layers of protection, which is why we asked respondents to select all options they are using.

As well as anti-malware, other cost-efficient technologies – VPNs, employee training and multi-factor authentication – were the most widely used security options. These are mostly software- or knowledge-based, and simple to set up. Other technologies, such as endpoint security, dedicated work-only LANs and SD-WANs, may offer the same or greater security by themselves but are both more expensive and more complex. LANs and SD-WANs are also vulnerable to illicit user behaviour, which other technologies can restrict.

Security in the new normal

Nine in ten firms have increased their remote working levels in the COVID-19 crisis, and just 10% of respondents expect those levels to go back to normal – or decrease – once the pandemic is over. The vast majority expected instances of remote working to increase somewhat (55 percent) or greatly (35 percent).

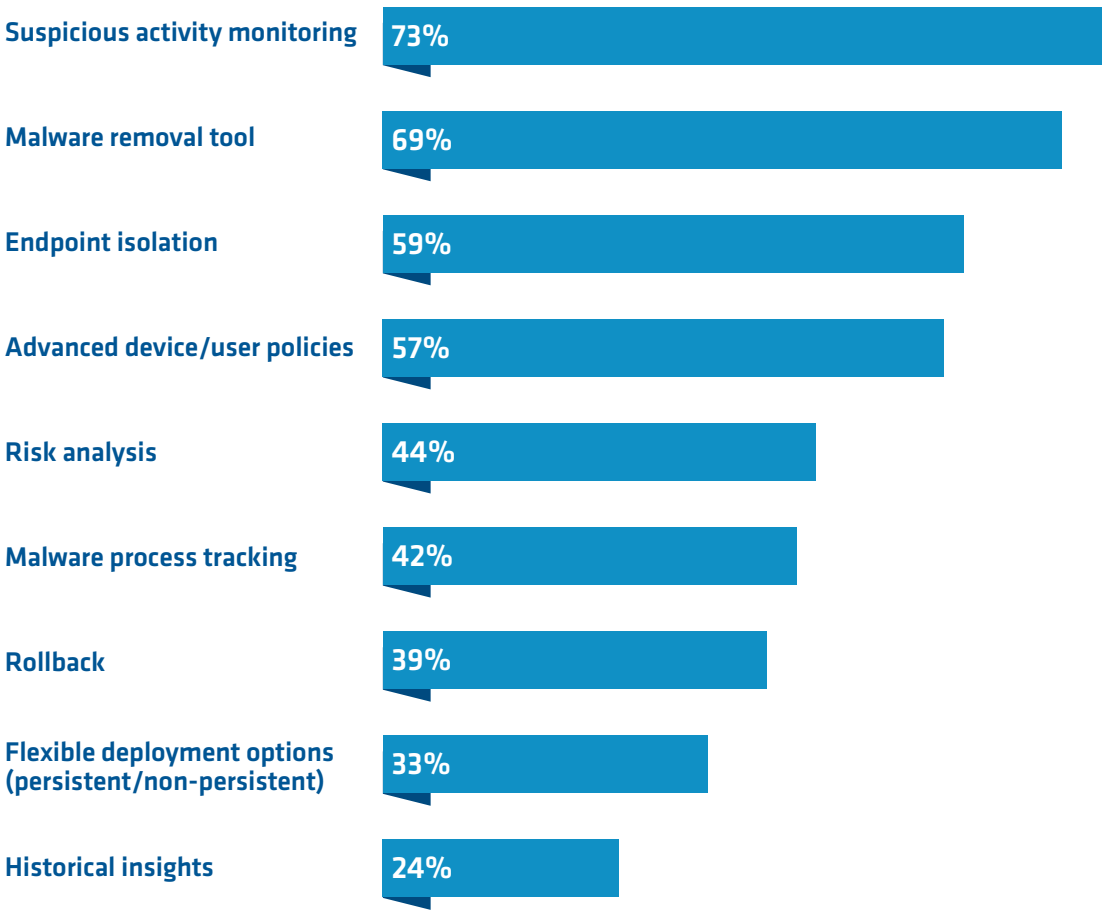
Fig. 7: To what extent do you think remote working at your organisation will return to pre-COVID-19 levels after the pandemic?



If remote working does increase (compared to pre-COVID levels) after the pandemic is over, expect to see changes to the technologies firms use. As companies settle in for the long haul they are likely to invest in more specific solutions, like dedicated networks, and policies that ban personal activities on devices used for work. There may also be pushback against the BYOD movement.

However, VPNs and anti-malware will remain a quick, easy and relatively cheap tool to set up on a remote worker's PC, and it is likely that they will remain the most popular security choice at all levels of work. These systems, like others, are evolving to address the challenges of a post-COVID world, and respondents said that monitoring users for suspicious activity, plus malware removal – in an environment where security teams will frequently be unable to physically access an employee's device – would be critical to anti-malware tools in the future. Endpoint isolation and advanced device/user policies were also popular.

Fig. 8: Which of the following features do you see as critical to anti-malware tools in the immediate future?



Conclusion

The pandemic has forced dramatic changes in both our work and personal lives, no matter where we live. When it comes to cybersecurity, it's clear that SOC leaders will need to adjust their security plans as well to meet the security needs of their organization's new working model.

Rapid change inevitably reveals weaknesses. New processes will be open to exploitation and vulnerabilities, company data may be more exposed and remote employees will lack the protection of employers' dedicated security systems.

Companies must think about how to counter both their weaknesses and threats in a sustainable, effective, and efficient manner. Adopting approaches that automate security functions–from protection to incident response–will provide an effective approach for a company to be better cyber-prepared. This will improve outcomes for a company's security posture and simplify security management across the dispersed workforce.

With the majority (82 percent) of respondents indicating that remediation is just as important as prevention in an effective response strategy, it is also important to look at how automation can provide advances in this area. Avoiding the potential negative outcomes from a breach requires fast response to halt an attack, yet 43 percent require days to weeks to remediate an incident.

To address this security weak point, it's encouraging that 69 percent of companies are planning to invest in malware removal tools in the near future. Indeed, investing in mechanisms that provide automated endpoint response will significantly accelerate an organization's response times and advance SOC security practices.

About the sponsor, Malwarebytes

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs.

For more information:

Visit: www.malwarebytes.com/business

Malwarebytes