MENLO SECURITY

The state of threat prevention: evasive threats take center stage

Digital transformation has rendered many traditional security solutions useless in the face of modern cyber threats.

REPORT

Organizations face a surge in Highly Evasive Adaptive Threats (HEAT)

The impact of the global pandemic resulted in a paradigm shift that drastically expanded attack surfaces as hybrid and remote working environments became the norm.

Employees now spend most of their time working in the cloud, tapping into SaaS applications and other tools that are pivotal to productivity. However, in doing so, their companies are now struggling to manage a variety of new blind spots in traditional approaches to security that aren't fit to protect modern work.

During the last ten years, cybercriminals have adapted to find new ways in which they can exploit and bypass legacy security systems. Consequently, there has been a surge in a new class of cyberthreats known as Highly Evasive Adaptive Threats (HEAT).

HEAT attacks target web browsers as the attack vector and employ techniques to evade detection from the traditional tools used in current security stacks such as firewalls, Secure Web Gateways, sandbox analysis, URL reputation, and phishing detection solutions.

Menlo Security conducted research to understand organizations' knowledge of these advanced threats, whether they are seeing more of them and how well equipped they are to deal with them. Here are the results:

Key findings

- An increasing amount of time spent working in the browser and accessing cloud-based applications has been accompanied by an uptick in browser-based attacks and compromised devices.
- Web malware and ransomware top the list of security threats that organizations are most concerned about.
- Despite the growing risks, most companies don't have advanced threat protection in place on every endpoint device used to access corporate applications and resources.
- Organizations are not being proactive enough in mitigating the risk of HEAT attacks, owing in part to conflicting views about the most effective way to manage security.
- There are several competing priorities for IT professionals when it comes to improving their security posture in 2022.

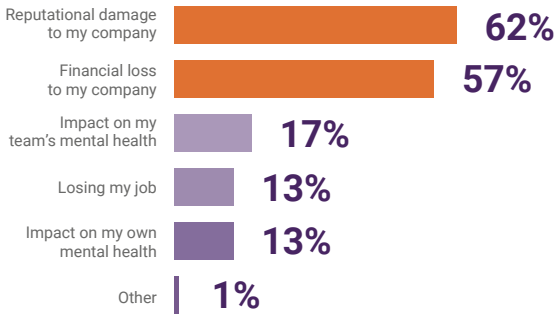
Insight #1:

Organizations are worried about ransomware

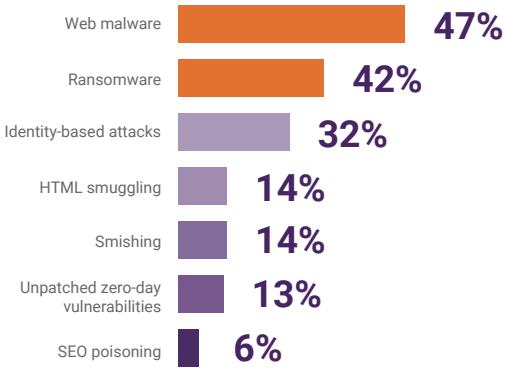
There can be no doubt that companies are concerned about modern cyberthreats. The European Union Agency for Cybersecurity (ENISA) recently stated that we are witnessing the "golden era of ransomware" – and for good reason. The consequences of such attacks can be catastrophic, from prolonged operational delays and data loss and exposure, to huge reputational damages. Meanwhile, cybercriminals are successfully extorting financial sums in the tens of millions of dollars from their victims.

The top two concerns of a security breach are reputational damage (62%) and financial loss (57%).

What are you most concerned about when it comes to a security breach?



Which of the following threats pose the biggest challenge to your organization?

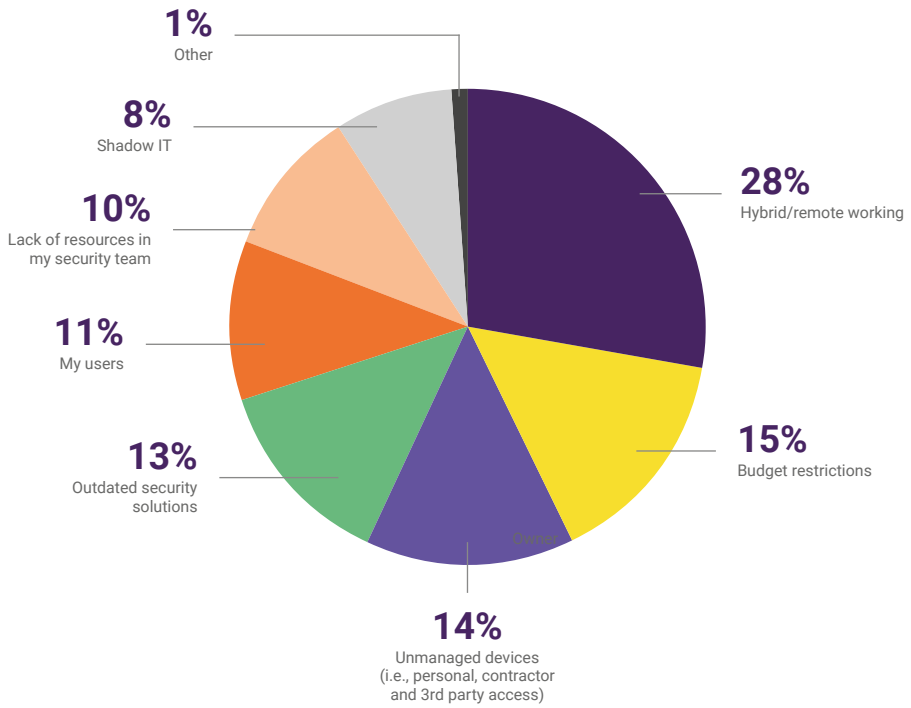


Web malware (47%) and ransomware (42%) are considered to be the threats that pose the biggest challenge to organizations.

Insight #2:

Modern work has added complexity

The shift to home working changed everything. Many security solutions became redundant almost overnight, with enterprises now struggling to manage potential vulnerabilities owing to a distinct lack of visibility into those unmanaged devices that end users are using to access corporate networks. A series of security blind spots have emerged that many organizations simply aren't aware of or able to manage. Couple this with the threat of more sophisticated attacks, and the security implications of hybrid and remote models are clear to see.

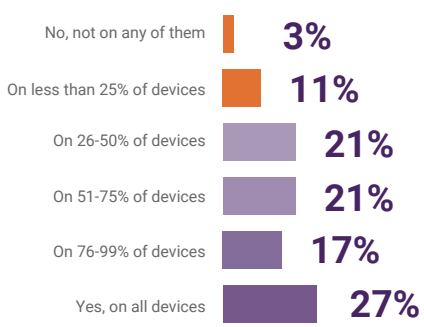


What is the biggest challenge you expect to face in 2022 when it comes to protecting your corporate network from advanced threats?

Hybrid and remote working (28%) is the biggest challenge organizations expect to face in 2022 when it comes to protecting the corporate network from advanced threats.

Less than 3 in 10 entities have advanced threat protection in place on every endpoint device used to access corporate applications and resources.

Do you have advanced threat protection in place on every endpoint device that can access your applications and resources?



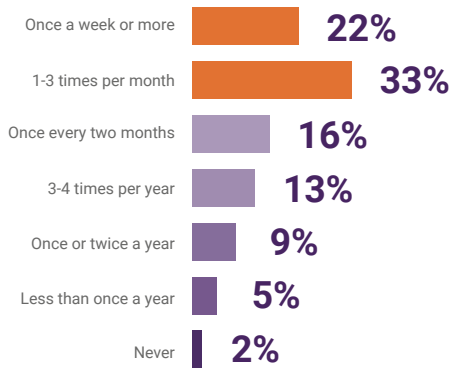
Insight #3:

Attacks are more frequent and successful

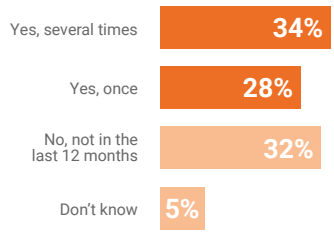
Threat actors today are not standing still. They are constantly working to tweak and change their methods in order to further evade security systems and exploit their targets successfully. The adaptiveness of HEAT attacks is a key challenge. If security teams find a fix, attackers will alter their tactics to work around it. If a new web browser-focused tactic is proven to work it is in turn exploited at scale, often by a thriving and growing ransomware-as-a-service landscape.

Over half (55%) of organizations encounter advanced web threats at least once a month, while 1 in 5 face them at least once a week.

How often do you come across advanced threats delivered via the web within your organization?



Have any of your organization's or employees' devices been compromised by a browser-based attack in the last 12 months?



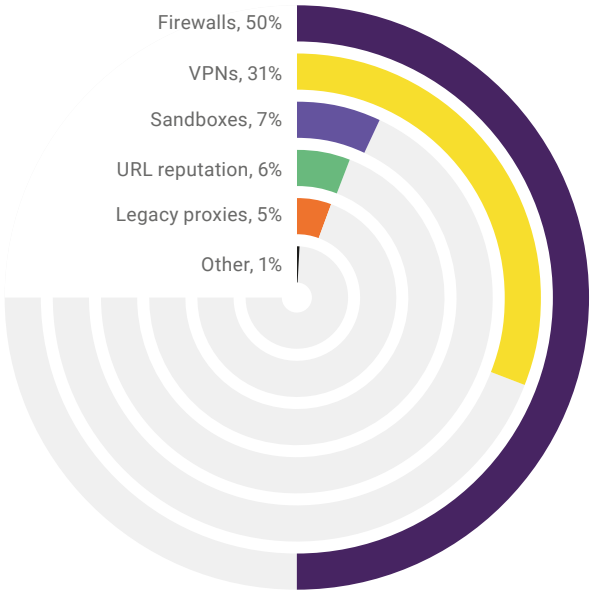
3 in 5 (62%) of organizations have had a device compromised by a browser-based attack in the past 12 months. A third (34%) report this has happened several times.

Insight #4:

Existing technology isn't working

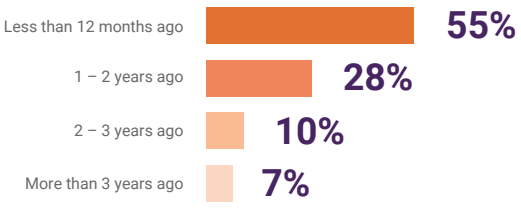
The transition to hybrid and remote working has expanded attack surfaces and exposed many new vulnerabilities, yet security has largely failed to adapt and properly serve these new operating environments. Organizations today are relying on outdated technologies from a different era to mitigate HEAT attacks. From antivirus software to firewalls, many of the solutions deployed for on-prem environments a decade ago simply are not fit for purpose in dealing with modern cloud-based threats and defending against browser-led attacks.

Which of the following network security solutions do you believe is the most successful at mitigating HEAT attacks?



One in two organizations think that firewalls are the most successful solution in mitigating HEAT attacks, followed by VPNs at 31%.

When did you last add capabilities to your network security technology stack?



45% of organizations have failed to add capabilities to their network security technology stack in the past 12 months.

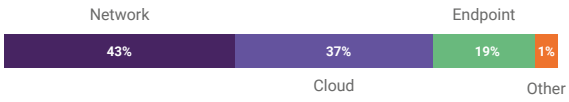
Insight #5:

Competing priorities present challenges

Working life today looks fundamentally different compared to pre-pandemic, from the applications needed to complete tasks to the devices used during the day-to-day. From a security perspective, this has created many different problems that each need unique solutions. In order to determine which should take precedence, organizations should consider what will provide the greatest return on investment regarding risk reduction, working to remediate the greatest risk areas first. Critically, a layered approach should be adopted to both prevent attacks and manage them beyond the perimeter.

There's a lack of consensus on where best to deploy security solutions, with 43% favoring the network and 37% choosing the cloud.

Which of the following do you believe is the most effective place to deploy security to prevent advanced threats, such as ransomware?



What measures will you be taking in 2022 to improve your security posture?

61%
Training staff in security best practice

60%
Increased investment in technology to protect my corporate network

50%
Adapting to new ways of working, i.e., hybrid or remote

46%
More investment in skilled security team members

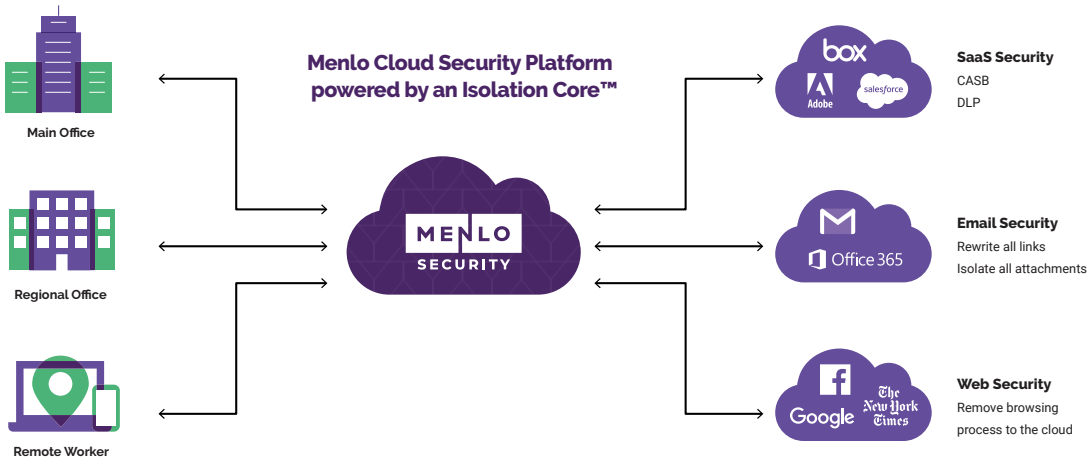
Priorities for improving security in 2022 include training staff (61%), technology investment (60%), adapting to new ways of working (50%) and investment in skilled security members (46%).

Preventative security pays dividends

Cyberattacks are a case of 'when' not 'if' for unprepared organizations. Security teams must stop relying on traditional tools and strategies that are no longer adequate in dealing with HEAT attacks.

Adopting a prevention-driven approach to security is the most effective way in which the opportunity for attackers to reach the network and endpoint can be dramatically reduced in the first instance.

Here, isolation technology should be the first port of call. By executing all active code from the internet in the Menlo Cloud Security Platform powered by an Isolation Core™, organizations are able to remove all the risk from web and email attack vectors.



It doesn't matter if there's a known or unknown vulnerability on the endpoint, because no content – whether it is malicious or not – is executed on users' browsers.

The logic is simple: if the malware isn't able to run on your network, it cannot affect you.

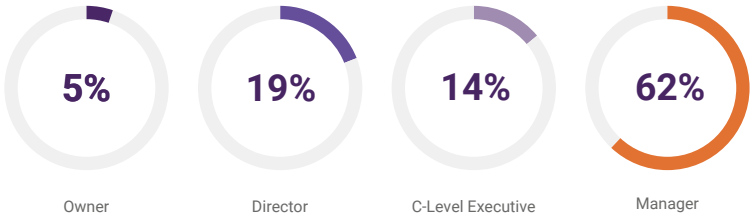
Learn more at www.menlosecurity.com

Methodology

Menlo Security surveyed 505 IT decision makers in the U.S. and UK who work for companies with more than 1,000 employees. The firm sent invitations via email in February 2022 and followed up with a link to the survey for targets who responded. Results are accurate to ±4.4 percent at 95 percent confidence limits.

Business size

Job role



MENLO SECURITY

To find out more, contact us:

menlosecurity.com

(650) 695-0695

ask@menlosecurity.com

About Menlo Security

Menlo Security enables organizations to eliminate threats and fully protect productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure Zero Trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward.