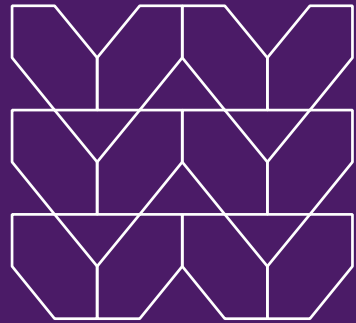


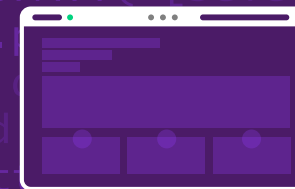
Hiding in plain sight: Examples and analysis of highly evasive threat campaigns

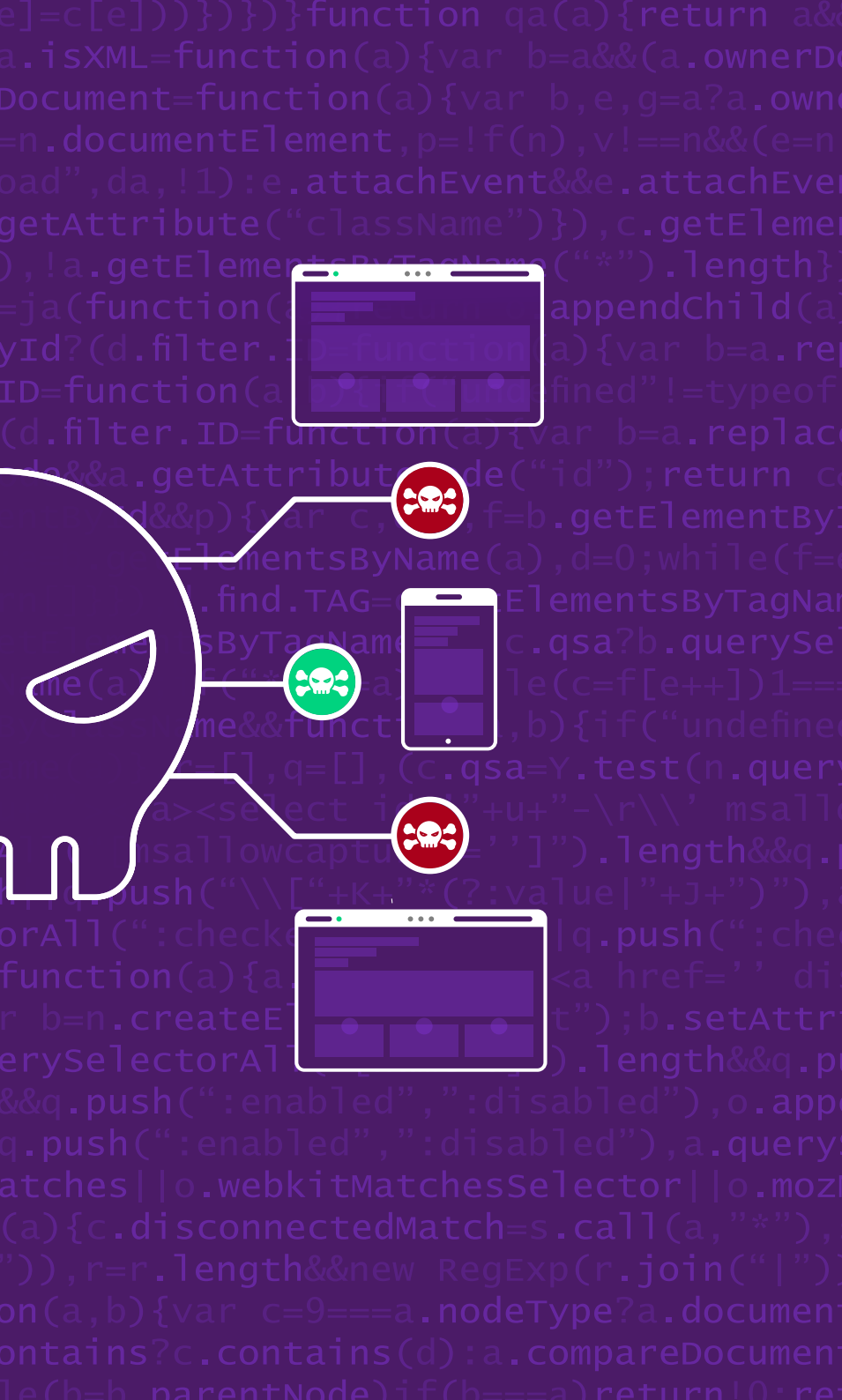


Page Contents



- 03 Remote work and the rise of HEAT attacks
- 04 The Menlo Labs research team analysis
- 05 The Lazarus Group
- 06 VIP3R
- 07 Qakbot
- 08 Template injection attacks
- 09 Preventing HEAT attacks





Remote work and the rise of HEAT attacks

The enterprise of today looks and operates a lot different than it did over a decade ago. With an array of technology that's flooded corporate networks to accelerate business processes and cater to the anywhere, everywhere workforce, the opportunities are endless...but so are the risks. Unbeknownst to many organizations, the primary challenge they face lies in [the security technology they've invested](#) in to protect the network...which is one of the few things that hasn't evolved along with the business.

The very technology we've placed our trust in is failing to protect organizations. That's because threat actors are no strangers to the fact that these solutions are primarily based on the notion of detecting and remediating threats and building rules around stopping the bad stuff. That's why they've adapted much quicker than security technology has—hence the endless “cat and mouse” references used in cybersecurity content.

One area that attackers have zeroed in on is exploiting the biggest productivity tool for knowledge workers today—the web browser. How? Through Highly Evasive Adaptive Threats (HEAT), which leverage web browsers as the attack vector and employ various techniques to evade multiple layers of detection in current security stacks, many times serving as beachheads for ransomware, advanced phishing, and zero-day malware.

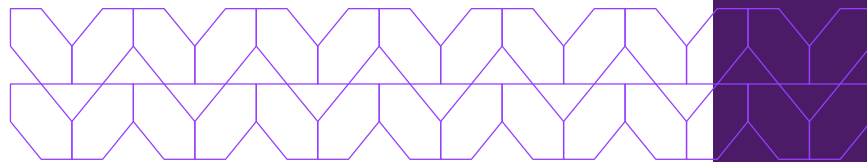
To be classified as a HEAT attack, the threat must feature one or more of the following evasive characteristics that bypass legacy network security defenses:

- Evading URL filtering
- Evading email security tools
- Evading file-based inspection
- Evading HTTP content/page inspection

This ebook explores the various examples of HEAT attacks that the Menlo Labs research team has analyzed, providing you with a glimpse of what they've observed and the opportunity to dive into the details of their research outside of this asset.

The **Menlo Labs** research team analysis

The Menlo Labs research team focuses on providing insights, expertise, context and tools to aid security teams. For some time now, the team has been analyzing HEAT attacks in a variety of threat campaigns. Once fully understood, the Menlo Labs team publishes their research which includes a variety of insights such as threat attribution, tactics, techniques and procedures (TTPs), in addition to indicators of compromise (IOC). Most importantly, they provide steps that organizations can take to protect themselves from future HEAT attacks.



50%

of HEAT attacks seen come from categorized websites.

Out of the more than 5 million malicious URLs analyzed.

73%

of Legacy URL Reputation Evasion (LURE) attacks—a HEAT technique—come from categorized websites.

Based on over 1 million urlscan.io records analyzed by the team.

70%

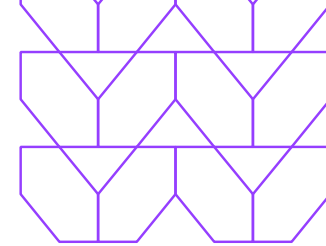
Increase in LURE attacks in 2022.

Of customer records analyzed from July 2021 to July 2022, a HEAT evasive technique that bypasses existing defenses, evading web filters that attempt to categorize domains based on trust.



HEAT Attacks

Based on recent research, the team has uncovered some telling insights regarding HEAT attacks. The following threat campaign examples provide a snapshot of their findings. For a complete rundown, be sure to visit the associated research blog post.



The Lazarus Group

The Threat Actor

The **Lazarus Group** is a cybercrime unit run by the North Korean state government. Many cyberattacks have been attributed to the group from 2010 to 2021, and some of the most notable attacks include the [2014 Sony Pictures hack](#) which resulted in a trove of stolen data from Sony's network, as well as the infamous [Wannacry 2.0 global ransomware](#) attack, which impacted upwards of 200,000 systems worldwide.

Most recently, the Lazarus Group was observed by the Menlo Labs research team across its customer base leveraging HEAT techniques to bypass current and in-use security technology to compromise victim organizations. Their method of choice? Browser exploits. Why? Because the web browser is the lifeblood of productivity for today's knowledge worker.

The group has been known to leverage browser exploits to ultimately install both malware and ransomware for monetary and intellectual property theft. The activity in question leveraged a critical Chrome browser vulnerability that was being exploited by the group, which [Google engineers eventually patched](#).

The Targets

[Google pointed out](#) that similar exploits were being leveraged by the group as far back as 2021, targeting organizations in news media, IT, cryptocurrency and fintech. Further research conducted by Menlo Labs across the Menlo Security customer base identified additional targets including U.S. government agencies and Japan-based crypto exchanges.

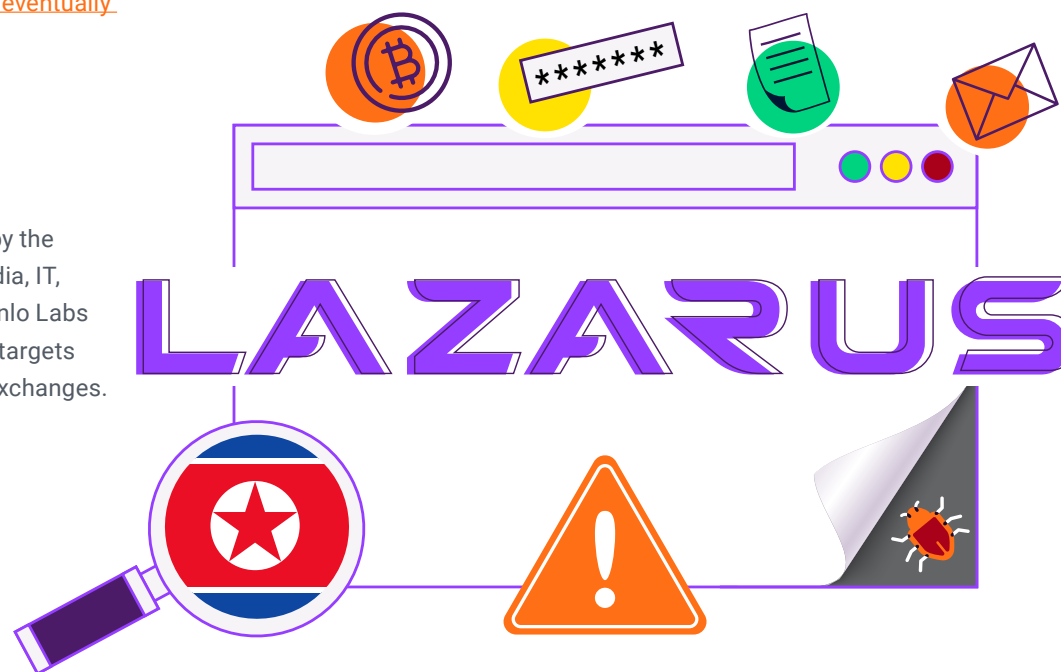
The HEAT technique

The first occurrence of indicators of compromise was as far back as October 2021. At the time, the threat actors created the domain, giantblock.org, as a [Legacy URL Reputation Evasion \(LURE\)](#) tool for their operation—a well-known HEAT technique. These LURE attacks bypass existing defenses, evading web filters that attempt to categorize domains based on trust.

Attackers do so by compromising poorly secured websites that are already trusted by these security systems— in some cases creating them from scratch—and using them to serve up malware or steal user credentials. This means that organizations that rely on earlier-generation Secure Web Gateways (SWGs) and traditional URL filters will find themselves increasingly at risk.



[Dive deeper in the Lazarus Group analysis.](#)



The Campaign

When it comes to a threat actor’s attack arsenal, they’re used to sticking with what works. That’s why email-based attacks are part of their tried and true methods of compromising users. According to [one recent study](#), organizations experienced 48% more email attacks during the first half of 2022 when compared to the second half of 2021. Of those same attacks, a majority (68%) were aimed at compromising credentials.

Depending on their motives, user credentials could be as valuable as cash for threat actors—allowing them to seamlessly access networks, siphon sensitive information, or live off the land to ultimately get at the crown jewel they’re after. Naturally, when the Menlo Labs research team discovered an open directory in 2022 filled with usernames and passwords, they immediately dug into the information.

After further analyzing the content in the directory, they determined that it was the result of a single campaign that leveraged evasive HEAT techniques to compromise the credentials of 164 users at a number of organizations. Upon analyzing the exploit kit associated with the campaign, the team discovered a unique string—DH4 VIP3R L337—resulting in dubbing the campaign VIP3R.

The Targets

A majority of the targets (19%) belonged to users at healthcare organizations while users at companies that offer professional services (16%) and the education sector (11%) followed closely behind. However, the campaign cast quite a wide net given there were more than 20 verticals impacted.

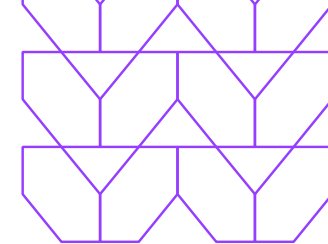


The HEAT technique

In the VIP3R campaign, attackers were able to evade file-based inspection by sending customized HTML attachment payloads to victims via phishing emails. Once a victim opens the attachment, a phishing page appears that impersonates a service typically used by the recipient. If the victim enters their password and selects the “Submit” button, they run through a validation and verification of the password that happens on the server side, ultimately resulting in compromised credentials. The HTML file used in the campaign evades file-based analysis on the endpoint, and the URL for the phishing page also evades URL filtering due to Legacy URL Reputation Evasion (LURE), another HEAT technique.



[Learn more about the details associated with the VIP3R campaign.](#)



The Qakbot Banking Trojan

The Campaign

When it comes to the malware family tree, banking Trojans really began to make an impact once banking customers became comfortable with the idea of online transactions. Once online banking became the norm, digital miscreants quickly moved into action and crafted malware specifically aimed to compromise banking credentials; enter banking Trojans. Some of the most notorious banking Trojans—including Trickbot, Dridex, and Emotet—easily evade detection, steal sensitive information, and even manipulate user data.

In today's threat landscape, banking Trojans are a popular tool among cyber swindlers who follow the money—so much so that studies suggest that [100,000 strains can be detected in a single year](#). Needless to say, banking Trojans are effective, and they aren't going anywhere any time soon, which is why this particular campaign came across the Menlo Labs research team's radar. Qakbot, also known as QBot or Pinkslipbot, is a prominent banking Trojan that's been making the rounds for the better part of a decade. Primarily delivered via phishing emails, threat actors have been maintaining and altering the malware since 2007, making it one of the leading banking Trojans globally.

Today, Qakbot is able to not only compromise banking credentials, but also spy on financial organizations, spread itself, and install ransomware. The Menlo Labs research team has observed several strains of Qakbot campaigns which use various HEAT techniques to successfully compromise victim organizations.



The Targets

As previously stated, Qakbot campaigns typically have no boundaries, with victim organizations and users located around the world. Most recently, an aggressive campaign was reported on [targeting U.S. organizations](#), and being run by ransomware collective Black Basta.

The HEAT technique

As reported by the Menlo Labs research team, the Qakbot campaigns observed have leveraged HEAT techniques such as Legacy URL Reputation Evasion (LURE)—which was also used by the Lazarus Group—as well as [HTML smuggling](#), which allows cybercriminals to evade static and dynamic content inspection. In these attacks, threat actors create a JavaScript BLOB (binary large object) element and dynamically fill it with content. In the [attacks witnessed by Menlo Labs](#), the content used to create the malware was encoded within the HTML page the user requested. Because the content is created dynamically from elements within the web page, a file request isn't sent over the Internet.



[Dive into the details tied to the Qakbot campaign here.](#)

Template Injection Attacks

The Attack

For the average knowledge worker, electronic documents are a critical aspect of their work. PDFs, Excel, Word or other Microsoft Office documents make up a majority of the files users interact with on a daily basis. That's why threat actors weaponize these documents to contain code and links that can release malware, Trojans, and even ransomware. The Menlo Labs research team keeps a close eye on any activity that features malicious documents, but they recently observed several weaponized decoy documents that leveraged [template injection techniques](#).

Threat actors are keen on template injection techniques because no suspicious indicators like macros need to be present in the document until the malicious template is fetched. Based on what they've observed, the Menlo Labs research team believes that template injection attacks will increase in popularity and may even be used to load exploits on the fly.

The team also observed several weaponized documents with unique camouflage techniques that [hide the URL to the naked eye](#). The documents contained a decimal IP address or used an obscure URL format for fetching a remotely hosted template.


[The latest analysis](#) from the Menlo Labs research team indicates that the threat actors behind some of these campaigns operate out of North Korea.

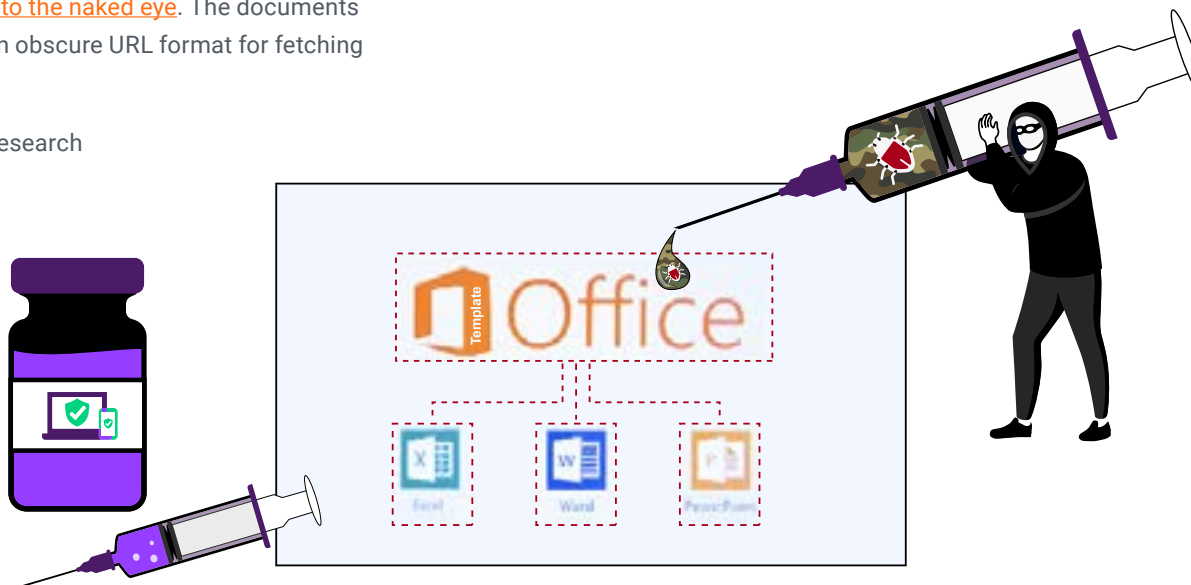
The Targets

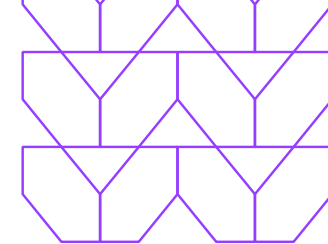
Given that similar TTPs were observed being used by a North Korean APT, [BlueNoroff](#), some targets include, but are not limited to, cryptocurrency companies. While the Menlo Labs research team is still conducting research, other targets may include diplomatic and government agencies [based on research](#) conducted into threat actors that leverage similar TTPs.

The HEAT Technique

While template injection attacks are considered a technique themselves, they also evade security tools and solutions by leveraging the Legacy URL Reputation Evasion (LURE) technique, which uses websites categorized as having good reputation by web filters to deliver malware.

 The Menlo Labs research team has covered these attacks extensively in [Part 1](#), [Part 2](#), and [Part 3](#) of this article series.





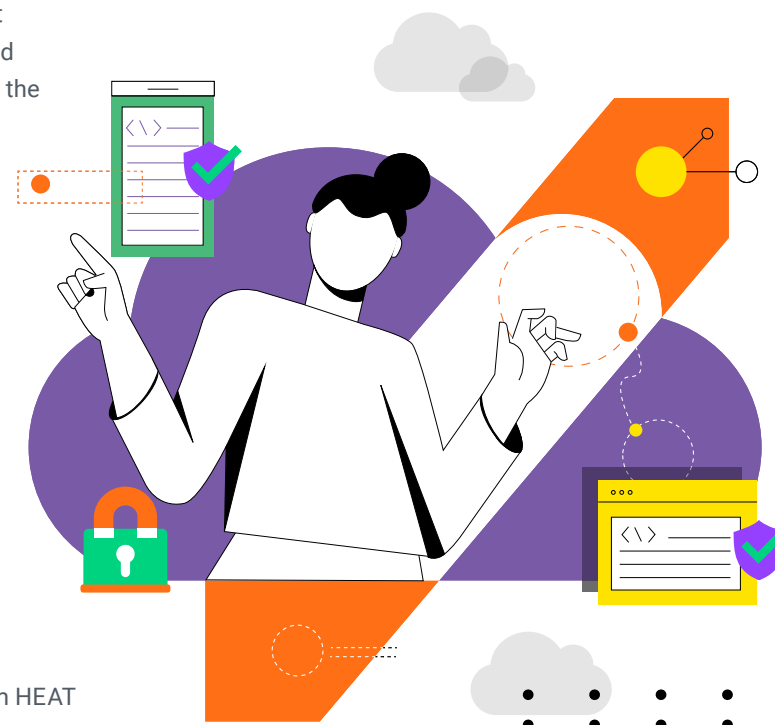
Preventing HEAT attacks

Protecting your organization

The infection vectors of HEAT attacks have been plaguing organizations for years, but given the recent evolution of the threat market resulting in part from accelerated cloud migration and the proliferation of remote work, these relatively unknown attacks pose the greatest threat for enterprises today. As mentioned before, all traditional security capabilities—including Secure Web Gateways, sandboxing, URL reputation, and filtering – are rendered ineffective against HEAT attacks. The challenge is that because HEAT characteristics have legitimate uses, simply blocking them won't work. Preventing the use of these techniques altogether is key.

One proven preventative approach is leveraging isolation technology, which delivers on the true promise of Zero Trust security. Separating an enterprise network from the public web—while still allowing users to access the Internet seamlessly—results in a Zero Trust Internet. One key characteristic that makes isolation technology appealing to organizations is that it ensures user productivity, while granting open access to the Internet—making security invisible to the end user. Additionally, it allows businesses to scale globally to support roaming users without impacting user performance.

Isolation moves the viewing of email attachments and web browsing from a user's device to the cloud. By isolating Internet content in the cloud, users are protected from HEAT attacks that bypass legacy security solutions and result in malware and ransomware. Not only would isolation technology have prevented each of the malware and phishing examples outlined in this ebook, but it's also proven to eliminate the most prolific sources of breaches.





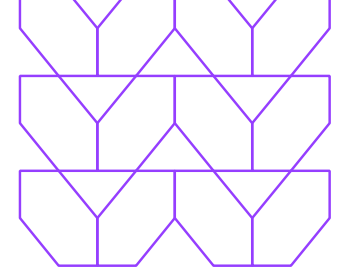
About **Menlo Security**

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. It focuses on protecting the single biggest productivity driver for knowledge workers – the web browser.

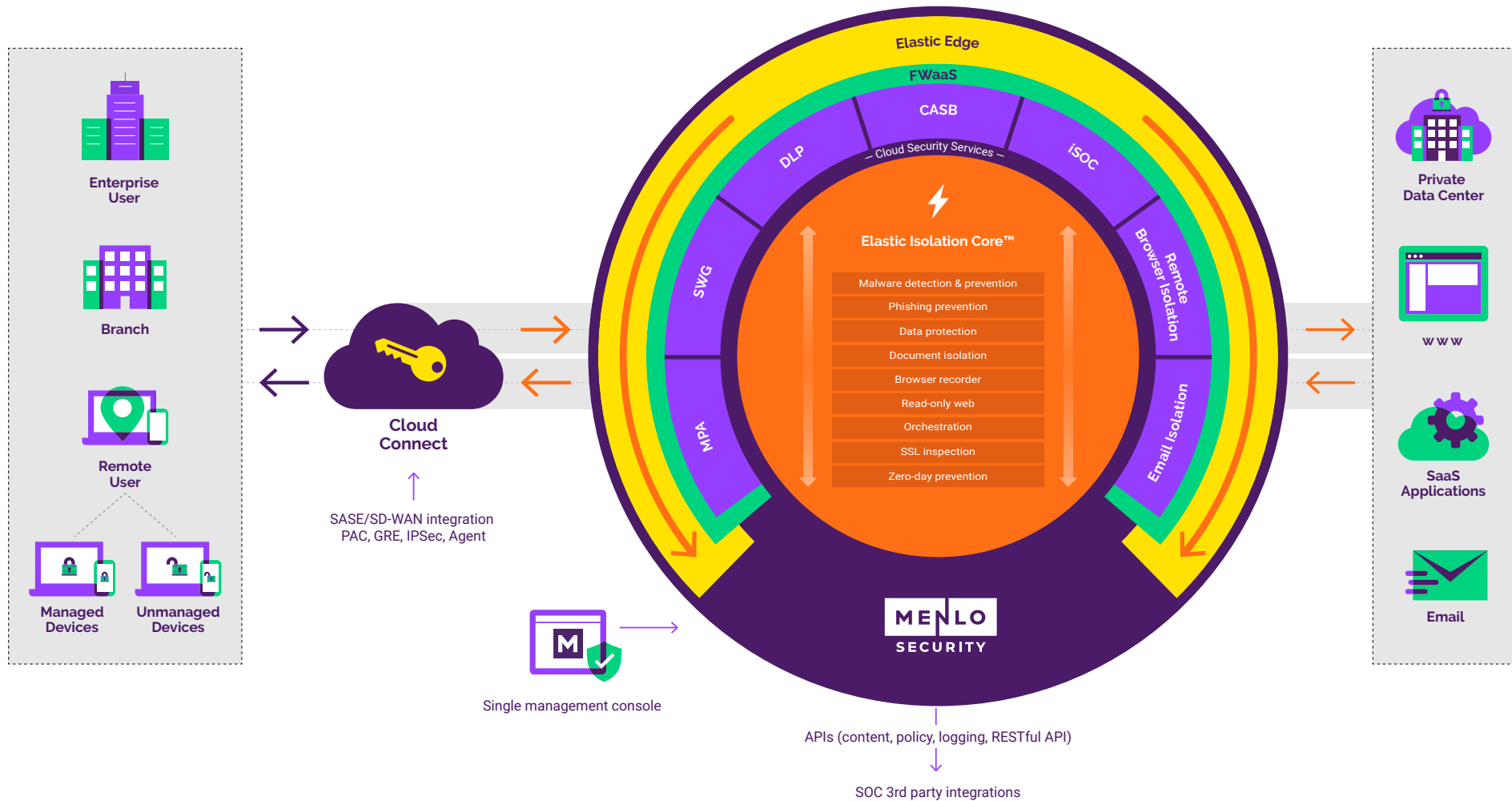
Menlo's Cloud Security Platform prevents threats from entering an organization and secures data and application access in a single, global cloud-based offering. Our Elastic Isolation Core™ creates separation between the user, content and applications where security, policy and visibility are applied. By preventing threats before they happen, as opposed to detecting and responding, organizations eliminate all threats, including Highly Evasive Adaptive Threats (HEAT) across web, email, SaaS applications and private applications.

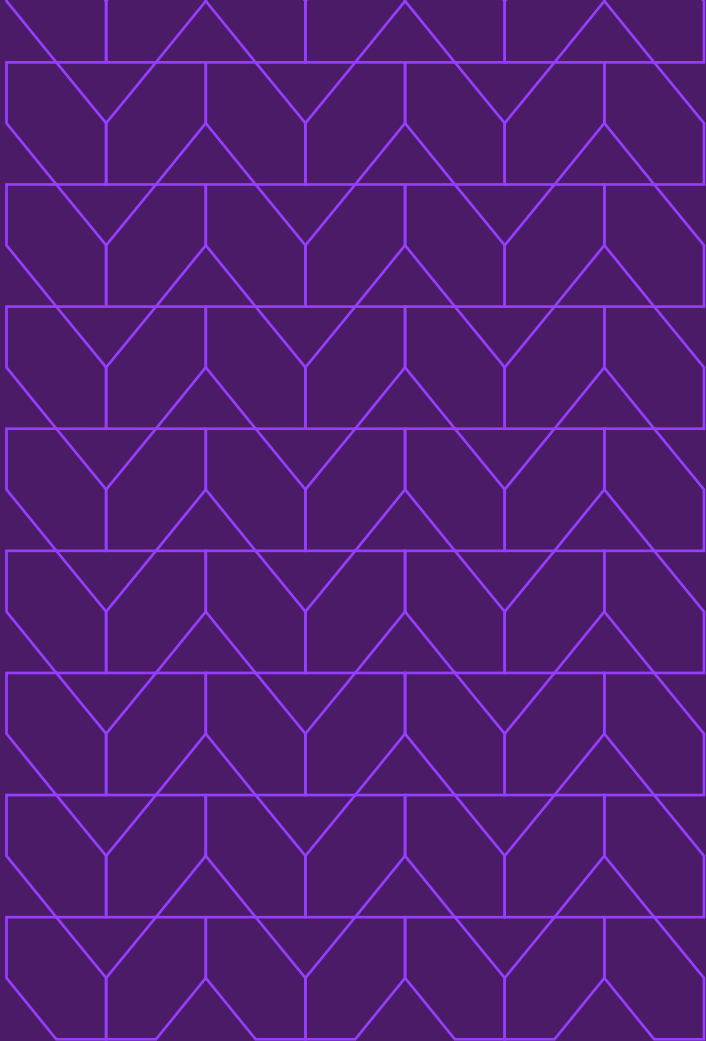
HEAT Check

Menlo Security provides a lightweight penetration assessment to help organizations better understand any susceptibility to various HEAT attacks. The assessment leverages various real-world HEAT attacks currently being used by threat actors, safely allowing organizations to deduce their exposure. Menlo's HEAT Check tool does not deliver actual malicious content.



Menlo's Cloud Security Platform





Get in touch with us.

Contact us today to learn if your organization is currently susceptible to HEAT attacks, but most importantly, how you can make them never happen in the first place.

menlosecurity.com/heatcheck

ask@menlosecurity.com



© 2023 Menlo Security, All Rights Reserved.

