Menlo Security

WHITE PAPER

Isolation: Separating Malware from the Network, Not Devices

Internet isolation provides 100% protection from web-based attacks without changing the native user experience.

The breach of 1.5 million patient records—including patient data for the prime minister—at SingHealth, Singapore's largest group of healthcare institutions, has been called the most serious breach of personal data in the nation's history. The breach was of great concern and created a chill of fear in many public and private organizations throughout the region and the world. If Singapore, one of the world's most connected countries, as well as one of the world's most cybersecure, could have a breach of this magnitude perpetrated against a national institution, why couldn't this happen to any organization, anywhere?

As Singapore has been a country leading the charge to disconnect the computers of its government agencies and ministries from the public Internet for some time, the nation's initial reaction was to disconnect staff computers from the Internet at public healthcare facilities country-wide. The Singaporean government had been mandating Internet surfing separation—disconnecting the endpoint devices of hundreds of thousands of civil servants and government employees from the Internet—since 2016. However, they had stopped short of including public healthcare institutions, such as SingHealth, in this form of air-gapping, commonly referred to as network separation.

While network separation is not a new tactic, and while it may seem simultaneously impervious to breach or hack, as well as being somewhat draconian in nature, it is not a panacea.

There is another, simpler, more cost-effective way that delivers 100 percent security while maintaining the user experience and productivity.

> Network separation means that if the user needs or would like to access the Internet or web, they will need to use a separate device provided by their organization for that access.

What Is Network Separation?

Network separation—also called air-gapping, or as it is referred to in Singapore, Internet surfing separation—is actually a simple concept: A user's device that is used for work cannot be connected to the Internet

or used to surf the web. If the user needs or would like to access the Internet or web, they will be provided a separate device by their organization for that access, or they may use a personal device for accessing the Internet or web.

It's a true physical separation of devices belonging to an organization's network and business from the Internet and web.

The thinking is that no web-based attacks—such as drive-by malware downloads, watering-hole attacks, malvertising, phishing websites, and the like—can infect a user's work device, because it's simply not connected to the web.

Many nations around the world have either adopted or attempted to adopt a form of network separation for a variety of different reasons and over an array of various entities.

The Cost of Network Separation

However, network separation comes at a cost—both economic and personal. It is sometimes economically infeasible to purchase a second device for each user just so they may access the Internet and web. The cost may be prohibitive for some organizations. That cost does not even begin to include the additional costs of provisioning, administering, and maintaining Internet-connected devices.

Network separation is also an issue for user productivity. A user who needs to access web-based work data or to access the Internet in order to do their job is now forced to access the web and Internet from a separate device, and to use another method to gather the information and data they need to be productive and share it with their disconnected work device. If an organization were to use a kiosk approach—where many users would access the web and Internet from a single device not connected to the organization's network—there is still an economic cost, and potentially a significant productivity hit.

Who Uses Network Separation?

Many nations around the world have either adopted or attempted to adopt a form of network separation for a variety of reasons and over an array of various entities.

Singapore was actually not the first country in the region to begin directing government agencies and ministries to cut the web and Internet cord from work devices.

South Korea has been moving toward network separation to secure its government networks since 2007, beginning with its National Intelligence Service and Ministry of the Interior. From there, network separation was instituted by other government ministries and state agencies. The Korea Communications Commission in 2012 adopted network separation for private sector companies, such as Internet Service Providers (ISPs) and

web portals with more than 1 million visitors per day, as well as defense companies and contractors. When a cyberattack in 2013 disabled computers throughout the country's television stations and networks and incapacitated the computing devices at top Korean financial institutions, the country's commissions and services that oversee the nation's financial services organizations extended network separation to the financial sector as well.

While network separation has helped decrease attacks on South Korea from their adversarial neighbor to the north, as well as from other nations and organizations, network separation conflicts directly with several initiatives that the Korean government has aggressively pushed, such as smart cities and smart-work initiatives. It also impedes the nation's desire to expand rapidly to the cloud in all aspects of government, business, and daily life, as many of the cloud services that users will need are isolated.

Other nations have also been recommending or have deployed network separation for specific government agencies, as well as recommending it for other markets. For example, "Network Segmentation and Segregation" was published in July 2012 and updated in 2018 by the Australian Cyber Security Centre to serve as an instruction manual for Australian organizations beginning to adopt network separation, segmentation, or segregation for security purposes. Countries including Italy, the United Kingdom, and the United States employ network separation for certain military and government computer networks and systems; mandate it through government or industry regulations for nuclear power plant control systems, avionics, and other aviation computing devices, and even certain computerized medical equipment; or recommend it for other businesses, such as financial computer systems like stock exchanges, and industrial control systems (ICS) like supervisory control and data acquisition (SCADA) devices used in gas and oil fields.

The one major benefit, though, that organizations deploying network separation expect this strategy to deliver is complete protection against malware and data breaches.

But even with the disadvantages of the network separation approach, the question of whether network separation truly delivers "complete" malware and data breach protection looms large.

Network Separation Is Not a Cure-All

Network separation is not a security panacea. Human error is always an issue. Network-separated devices can lull users into a false sense of security, and users can make mistakes that leave devices and networks open to attack.

Network separation is not a security panacea. Network-separated devices can lull users into a false sense of security, and users can make mistakes that leave devices and networks open to attack.

All it takes is a user and a malware-infected USB drive to transfer data downloaded from the web or Internet using a network-separated device. The user inserts the infected USB drive into a network-connected device, and a cyberattack is kicked off. The U.S. military, using air-gapped systems to protect against malware infiltration, was attacked in this way when a USB device infected with the Agent.btz malware was used to transfer data. "Project Sauron" is malware that relies on hidden partitions in an infected USB drive to remotely leak data from a network-separated device to an Internet-connected system. Simple worms that can spread through removable drives can also infect network-separated devices.

What if the fetch and execution commands were to happen far away from the user's device and web browser? What if the code were to be fetched and executed in a cloud-based platform?

Cyberattackers have also been busy and innovative in creating other ways of spreading malware and stealing data. University researchers in Israel have demonstrated how cell phone–based malware can be used to poach data via electromagnetic waves from network-separated systems. Another method uses acoustic signaling over an acoustical mesh network to circumvent network separation and steal data. "Airhopper" is yet another attack meant to infiltrate network-separated devices and exfiltrate data, this time by using FM frequency signals from a nearby mobile phone. "Bitwhisper" supports bidirectional communication, requires no additional hardware, and uses thermal manipulation to steal data from network-separated computers using a covert signal. "GSMem" uses cellular frequencies produced by a standard internal bus to convert the network-separated computer into a cellular transmitter antenna to steal information via GSM frequencies.

Other researchers have demonstrated how infrared capabilities of omnipresent surveillance cameras that have been compromised can provide a bridge between network-separated devices and Internet-connected devices. Another researcher shined a light into a room housing a network-separated computer, which was connected to a multifunction printer with a scan in progress, to show how they could receive and send attacks. "Powerhammer" leverages current fluctuations in power lines supplying electricity to network-separated computers, "Magneto" is a technique for passing data from network-separated computers to smartphones using electrical fields, and "Fansmitter" uses the fans in network-separated computers to send acoustic data.

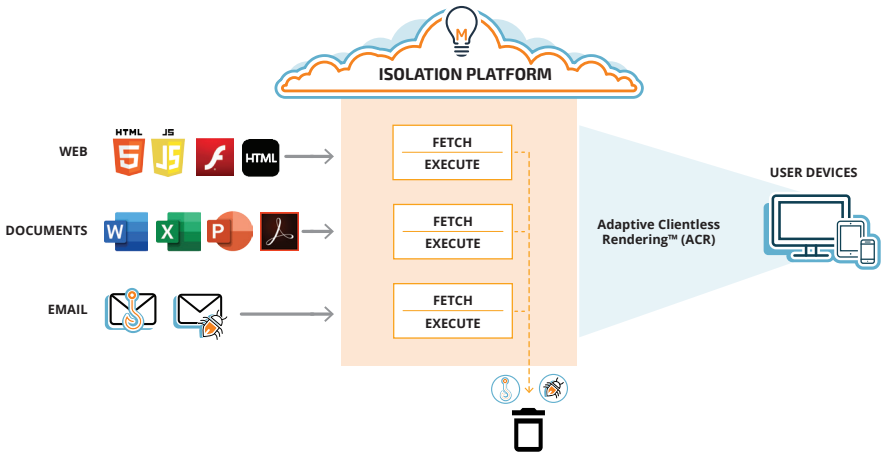
In general, the old adage, "Where there's a will, there's a way" holds true when it comes to infecting or exfiltrating data from even network-separated devices.

So even costly, productivity-sapping network separation does not "completely" protect networks and data.

But isolation does.

What Is Isolation?

Also called Internet isolation, browser isolation, or remote browsing, isolation is a technology that makes it impossible for any web-based attack to infect an organization's user devices. All web-based user activity—including webmail—is fetched and executed in a secure remote browser. Since no web pages are actually opened on a user's endpoint device, the user cannot inadvertently unleash malware on their device or any other devices it is connected to throughout the corporate network.



Menlo allows organizations to adapt a Zero Trust Internet policy, in which all web content is isolated in the cloud-based Menlo Security Internet Isolation Cloud.

Isolation is not a new concept. Previous—and current—efforts have been made to protect organizations against web-based attacks by executing all web content on remote computers. But Virtual Desktop Infrastructure (VDI) and other isolation technologies deliver a slow, glitchy browsing experience because the content is executed on a separate computing infrastructure and is rendered pixel by pixel on a user's screen. There is none of the active content that allows native web browsers to provide video as video instead of as a series of screenshots. Users have complained that VDI and similar isolation platforms slow web page loading and reduce responsiveness, forcing users to forego the capabilities of all modern browsers, such as the ability to print, copy, or paste content.

A web page is composed of code that is fetched from a web server and is executed in a user's on-device web browser. The web browser renders the web code in the human-readable form that everyone today knows as a web page. It is in the on-device execution in the browser where malware infections occur, leading to credential theft, ransomware, and data breaches.

But what if the fetch and execution commands were to happen far away from the user's device and web browser? What if the code were to be fetched and executed in a cloud-based platform?

That is the fundamental approach of Menlo Security's browser isolation. Menlo Security's isolation-based web security solution turns detection-based systems on their heads, employing Zero Trust Internet policies—in which all browser content is assumed to be risky—to prevent any browser-based malware from reaching end users. Instead of making the choice between running all web functions—fetch, execute, and render—in the web browser on a user's device, Menlo Security contains the fetch and execute functions remotely in a cloud environment. The Menlo Security Internet Isolation Cloud is essentially a virtual browser that operates on behalf of the user. This cloud-based virtual browser fetches and executes the thousands of lines of web code and all active content—such as Adobe Flash and JavaScript—served by a web server in its isolation platform. Active content that can serve as a conduit for a malware payload is stopped in the cloud-based Menlo Security isolation Platform, and is converted to safe HTML5 and H.264 video. All other web code that is used to create the fonts, images, Cascading Style Sheets (CSS), and other web page elements is stopped in the Menlo Security Isolation Platform.

The Menlo Security Internet Isolation Cloud is essentially a virtual browser that operates on behalf of the user. This cloud-based virtual browser fetches and executes the thousands of lines of web code and all active content.

Once all the active content and web code that might be infected or is able to carry a malware payload is stopped in the Menlo Security cloud environment, it is placed into a disposable virtual container, which is "shredded" and emptied at the end of every user web session. Menlo's patented Adaptive Clientless Rendering™ (ACR) technology then safely sends only clean website code to the web browser, which renders the malware-free website while completely preserving a seamless user experience. Printing, copy and paste, streaming video, cookies, and syncing all function normally, while users, their devices, and the network are protected from web malware and credential theft. The rendered web page looks and feels exactly the same as the actual web page—because it IS the web page, only with no malware risk.

Menlo allows organizations to adopt a Zero Trust Internet policy, in which all web content is isolated. It doesn't matter if the web code is or isn't infested with malware, or if the web page contains active content that is or isn't serving as a platform for malware. No analysis of, determination on, or decision about whether the fetched web code is good or bad is made. There is no detection. The Menlo Security Internet Isolation Cloud is agnostic: It treats all web code as if it were risky, and isolates it.

Menlo Security is an isolation pioneer that has created an approach that cleanly combines web, email, and document security with phishing and awareness training into a single, cohesive solution. Built from the ground up as a multi-tenant platform, the Menlo Security Internet Isolation Cloud delivers a scalable, 100 percent safe web environment without compromising user experience and productivity. Menlo Security is a Silicon Valley–based

cybersecurity company that has centered its brand around its security isolation platform. The platform is the core capability in Menlo's wide portfolio of services that also covers threat prevention and data protection in addition to email and web security.

Menlo Security's isolation solution addresses credential theft, zero-day attacks, ransomware, and malvertising, as well as secures corporate email and personal webmail, and helps organizations meet compliance regulations.

Conclusion

Network separation requires additional devices, adding significant cost for the organization and its security approach. It also negatively impacts user productivity and the user experience and forces users to adjust their daily workflow. User dissatisfaction can also be high. And then there is the "human error" factor—a user may become confused about which system or device to use for accessing the network and which to use to access the web and Internet. This can result in accidental malware infections, data breaches, credential theft, and more.

On the other hand, a Zero Trust Internet approach to cybersecurity—based on Internet isolation—does not have a negative impact on user experience and workflow, because the user's experience and workflow does not change. The native user experience and workflow are preserved, so there is no loss of productivity or user dissatisfaction. The organization also does not need to purchase additional devices for their users to access the web and Internet. The user can access the web and Internet from the same device, since all code from the web and Internet is isolated far from the user's device, and so is any malware. There is no room for human error or confusion, as the user doesn't have to decide between two devices to access their network or the web and Internet; all access is performed safely and securely from a single device.

Most importantly, isolation is 100 percent effective in eliminating web- and email-based malware, credential theft, and other risks and threats emanating from the web, email, and documents.

Not even network separation can claim that.

To find out how Menlo Security can provide your company with protection against cyberattacks, contact us at ask@menlosecurity. or vist www.menlosecurity.com

Menlo Security

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Zero Trust Internet. The company's cloud-based Internet Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com