IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation with Jonathan Lee

Carol Baker

As Menlo Security, a leader in cloud security announces an industry first by extending its cloud-based Secure Web Gateway (SWG) to include web isolation for mobile devices, we talk to Jonathan Lee, Senior Product Manager about the latest malware threats and phishing attacks facing users as they access the internet and email from their smartphones and tablets.

Jonathan Lee is a Senior Product Manager at Menlo Security (https://www.menlosecurity.com), a leader in cloud security. In this role he serves as a trusted advisor to enterprise customers, and works closely with analysts and industry experts to identify market needs and requirements, and establish Menlo Security as a thought leader in the Secure Web Gateway (SWG) and Secure Access Service Edge (SASE) space.

Experienced in leading technical development, launch and adoption of innovative security products, including email security, data loss prevention and end point security, Jonathan previously worked for Proofpoint and Websense. As an industry expert, media commentator and speaker, Jonathan is well versed in data protection, threat analysis, networking, Internet isolation technologies, and cloud-delivered security.

Can you tell our readers some background about Menlo Security?

Menlo Security is a venture capital backed cybersecurity vendor founded back in 2014, so we've been around in the security space for some time now. The founders came together formally after either starting companies or previously working for major cybersecurity vendors, such as Check Point Software. In 2014, they came together to look at whether they could develop a new approach to security, one that wasn't based on trying to work out what was good and what was bad, or what was benign, and what was malicious.

That is what the whole security industry is based on, trying to figure out if something is bad – great, if it is bad we can block it. But when you're dealing with very highly sophisticated adversaries, the type of attacks, tradecraft and the techniques that are being deployed now, right up to nation state attacks, increasingly, it's not possible at that point in time, every time to try and make that determination.

So, Menlo's founders were looking at ways that that we could reinvent that approach and look at a different way to protect users, networks, and organizations. What they came up with was 'isolation'.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Cloud based isolation, and the principle is fairly simple. Implementing it is a serious undertaking and we started that many years ago, so we've had a lot of time to develop isolation and test it in some of the largest organizations in the world.

But in terms of the principle, effectively if you take a user who visits a website, rather than all of what they see in their browser executing locally on the endpoint – and that could include malicious code, or malicious downloads and files that are coming down to their endpoint – when they visit that website, the actual web page itself is executed, and, and fetched on a virtual isolated browser that lives in the cloud.

That is basically a disposable virtual container that does all the hard work, and then it mirrors a safe, clean rendering of that web page down to the end user's machine. They are completely protected from any threats or malicious payloads that attempt to execute on the local endpoint. But in terms of the user experience, it's completely native.

As a user you would have no perception that you are now not physically going to that website. Instead, you are seeing a safe version or representation of it, because of user interaction, the clicks, copy and paste, everything is just as it would be if you are going direct to the website.

The platform itself is cloud based. It was built to be elastically scalable right from the beginning. So, as I said, we have some of the largest organizations globally that are running on it.

We subsequently took that isolation technology and developed it into a cloud based security platform, powered by that isolation core. One of the core tenants of that platform is our cloud based secure web gateway, or SWG, which is built on top of the isolation core.

This secure web gateway acts as a central aggregation point for an organization. All of their Internet bound traffic, regardless of where it originates from, whether the user is in an office at HQ, working from home or in a coffee shop, wherever that user is, all of the traffic that is going to the Internet, cloud apps and services or going to websites, all of that is going to pass through this secure web gateway at which point it can be safely isolated.

This ensures that the user is completely safe and secure when they go to any web based service or SaaS based app. It is also a place where you can integrate multiple security capabilities, such as cloud access security brokers (CASB), which provide controls for sanctioned cloud apps like Office 365, Google, Box or Dropbox, as well as unsanctioned apps which organizations may chose to block completely. Inline DLP rules can also be enforced here that prevent sensitive data from leaving the organization.

Also the other thing to note is that our cloud based security platform applies isolation to the email channel as well. We have an email security capability, which protects users from threats that enter the organization and target their mailbox in


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

the form of malicious links, or links to credential phishing websites and weaponized attachments, which are a huge problem.

For example, you can have Office documents containing some kind of Trojan or other active code or macros within them, which are trying to execute on the endpoint, or install something, like ransomware.

So it also applies isolation to the email channel as well to really focus on entirely where a user is spending the majority of their time. As we know, since we've been working from home, we are all spending a huge amount of time basically logged into the browser. It is estimated that between 60% to 80% of users working from home are spending the majority of their time in the browser accessing their email, using tools such as Salesforce, or doing research on the web – whatever it is, users will be in the browser. That is a huge attack surface that needs to be protected – and that is where Menlo Security comes in.

Which industry sectors are your customers in?

We have many millions of users that are protected by our cloud based security platform, including the US Department of Defense. We signed a contract with DISA which is the information security arm of the Department of Defense in the US who are responsible for implementing the systems and security for all of its mission partners, such as the Army and Navy, etc – and those users all over the world are being protected by our isolation platform.

We also have something like five of the top ten global banks running our services, and other very large enterprises in the global top 2,000.

We also have customers across a whole host of other industries and verticals, such as retail, manufacturing, travel, utilities, healthcare, etc – all with hundreds of 1000s of users all running our service.

What about security and mobile?

Although iOS is built on a very strong foundation with the sandboxing of apps to keep them completely separate, apps can talk to each other and are effectively still running the same browsers, which you have on the desktop. That is a huge attack surface in terms of the number of devices which are out there.

Whether it is a corporate owned or personal device, every single one of those devices, whether it's iOS or Android, is running a browser. Users are still clicking on links and are potentially more at risk when they click on those links on a phone or a tablet because of the reduced screen size where they are not necessarily able to perform the same checks, and validations that they would have working on a full browser on a desktop. But the very reduced address bar on mobile devices means the user can't see the full URL; can't check whether it looks right or not; and they won't necessarily be seeing the green padlock.

As a side note, just because you've got SSL encryption, or TLS encryption between the browser and the website doesn't make it secure – that is another misnomer.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Therefore, mobile users are more liable to fall prey to attacks. The amount of mobile usage and the amount of connections that we are seeing from mobile devices has gone through the roof.

We've actually just launched a new piece of research, our first Menlo Security Mobile Risk report, which shows that the majority of respondents – IT decision makers including CIOs and CISOs – admit that it's not possible to be prepared for all of the tactics and strategies used by attackers targeting mobile devices.

It's interesting that more than three-quarters (76%) of our respondents believe they are more vulnerable to mobile attacks than just a year ago, as businesses continue to shift to remote and hybrid work environments. Phishing, it seems, has been the main attack source for mobile devices over the last 12 months, followed by malware and advanced persistent threats or APTs.

What does isolation mean from a technical point of view?

From a technical point of view, I think the key thing again with isolation is it that it doesn't impact the user experience and we know in the case of Apple their entire brand, is effectively built on the principle that native is best.

Don't let security get in the way of what we've built and designed because everything works smoothly and seamlessly on iOS, and if you have an iPhone, you know that it does work very well. When you start putting things in the way of that experience users quickly push back and resist it.

The key thing for us in developing or adding support for mobile devices through the isolation platform was how we were going to implement our isolation technology or our remote browser capability so that it didn't impact the user experience.

To do this, we've built something called Smart DOM (Document Object Modelling) – and that is basically how a browser works and displays all the elements on a page.

In developing this new technology specifically for mobile we ensure that the user experience remains completely untouched: they can scroll, zoom, do all the touch gestures, copy and paste, etc that is really critical if you are developing security solutions for mobile devices so that it doesn't impact or get in the way of the user experience when they are on that device.

It seems the IT industry is always full of acronyms – it must be hard to keep up?

It is always hard to have conversations around IT security without more acronyms, but we are driven by themes, trends and concepts. One of those is something called SASE (it stands for Secure Access Service Edge). What it basically means is everything that was typically on the corporate network has now, as we know since COVID, really moved to the cloud at an incredibly accelerated rate through digital transformation.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Whereas before we came into the office, we connected to the network, and we accessed systems and services, which were physically located there. Now we're at home, and we're doing our work by accessing something like Salesforce direct to the cloud, security needs to be where the user is located – that is what this service edge means. The user needs to have protection, wherever they are working, whatever apps and services they are connecting to and using. Our platform is very much around building out that complete suite of capabilities.

To be in that market, you have the secure web gateway, cloud access security broker, data loss prevention, firewall-as-a-service – you also have something called private access. Rather than a VPN that connects you back to your corporate network, and then it then it takes you off to where you need to go, private access just gives you a secure direct connection to an app that you need for work that should only be available to employees. It provides that secure portal or access to one of those apps or services that you need to get to.

We are really expanding out the scope of our platform on an accelerated basis. Last year, we took an additional round of funding of $100 million, and a significant percentage of our funding and our annual spend is going into Research & Development (R&D), to really build out our capabilities, all while we continue to develop the isolation core.

This ensures that everything we do has that isolation core as its foundation to provide the comprehensive security that isn't so reliant on detecting if something's bad or not. Inevitably, things will get through and slip through the net.

We have all had to come to terms with and adapt to the new 'norm' and it has been incredibly powerful that we have been able to continue working during this difficult time. Whilst this has inevitably opened up a much bigger potential for attacks and threats to get through, there is a way to address that with a cloud based service that doesn't rely on backhauling traffic and, and trying to figure out how to make all the old architecture work. There is a way to protect those users and keep them productive – and that's where we believe Menlo Security can really help.