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

In Conversation with Mark Guntrip

Carol Baker

With remote and hybrid working set to remain, we talk to Mark Guntrip, Senior Director, Cybersecurity strategy, Menlo Security about why now is the time for organizations to re-evaluate their security strategies.

Mark Guntrip, Senior Director, Cybersecurity Strategy at Menlo Security (https://www.menlosecurity.com)

Mark Guntrip leads cybersecurity strategy at Menlo Security. He brings over 20 years' experience in the enterprise security market where, through a range of roles including engineering, product management and product marketing. He has a proven track record of building success in new markets as well as promoting growth within more established areas.

Prior to Menlo Security, Guntrip held various management roles within companies including Proofpoint, Symantec and Cisco.

Guntrip earned his Master's degree in Electronic Engineering from Southampton University, UK.

Why do you think companies have deep seated view when it comes to tackling cyberthreats?

Over the years, I've been very fortunate to work for some great companies. What I really like about being in cybersecurity is there is always the adversary you are trying to beat. At Menlo Security, our expertise is in stopping threats, and outwitting that adversary. In doing so we are helping our customers to stay protected as they grow.

By detecting threats as they come in, we help our customers stay ahead when it comes to preventing cyber-attacks.

However, many companies have a deep-seated view on what they need to do to stop the threats coming in. It's always been a case since the days of sandboxing if I can detect that it's bad, I'll block it. And if not, I'll let it in – and fingers crossed, I can fix it as quickly as possible. People have this pre idea of what they should do, what works, and what doesn't – but that is an old way of doing things, and ultimately it's not working.

Ransomware is constantly developing, so sticking to the old ways of cybersecurity is not going to work. Your cybersecurity strategy has to constantly change so that it not only evolves at the same time as cyberthreats but anticipates them and devises a plan of action before the cyberthreat has even arrived.

In our recent survey, over 75% of the respondents said that they were spending money knowing that it wasn’t going to solve the problem but felt that they had to do something (even if it is the wrong thing to do), just so that they can tick a box. Our perspective at Menlo is that it is pointless throwing money doing the same thing again, and again, and again, if it's consistently failing, and in our survey 75% of people agreed that their current cybersecurity strategy hadn’t worked in 2021, so there is no reason why it would work in 2022.

Is remote first the way to go?

During the pandemic the necessity to work from home meant that every organization had to rethink its remote access strategy. Unless companies were already 100% remote, they just didn’t have the tools, the scalability or the bandwidth for staff to work productively remotely. 90% of companies had to do something different. They had to add capacity, VPN concentrators and boxes etc were virtually impossible to obtain during the pandemic because the demand was too great. So those companies opt for an alternative . Many turned to Zero Trust Network Access or a similar technology, using cloud-based scalable solutions, where you don’t need boxes.

They reached the point where they had the connection, but couldn’t see what was going down that connection, and didn’t have the security to go along with it. In effect, they met their emergency need, and now they need to do much more, and revaluate remote access.

They may have augmented their existing VPN with something like a zero trust solution. So they now have two solutions to manage for two different groups of users, two sets of management, two sets of policy, two sets of everything – and these will need to be consolidated because having two systems doing the exact the same thing doesn't make much sense.

From our research, 53% of companies are saying that their staff want to continue to work remotely, especially those who would normally have long or time consuming journeys into the office. Businesses are realising that if they force the workforce back into the office, they will lose staff and with the trend for the ‘The Resignation’ already upon us people are switching jobs faster than ever before.

Can everything be done in the browser?

I foresee remote work technology continuing to develop with everything operating in the browser with zero touch deployment for the endpoint. This ends compatibility hardware/software issues as staff will be able to go to a URL, login, and their applications will be there.

Our research also looked at how organizations access applications. We need to shift to prevention as we look at remote access. The clientless approach Menlo takes in terms of enforcing policy within all the tunnels to those applications, allows us to see things from a data loss perspective as well as from a malware perspective. The ongoing management being in a single interface across everything from web to SAS and private access, as well as email – everything in a single interface. As a result, 90% of your workforce can be clientless.

As the internet becomes the new corporate network, controlling user access to private applications has become more important than ever. Organizations need to evolve their thinking from providing connectivity to the entire network to segmenting access by each individual application. The right zero trust approach will ensure seamless access between users and the applications they are authorized to use, while all other applications are invisible, preventing lateral discovery across the network.

What is Menlo's approach to clientless-first?

At Menlo Security we have a clientless-first approach to implementing Zero Trust Network Access. This enables organizations to secure access to applications from all devices including managed, unmanaged and mobile devices. It also minimizes the workload on IT and security for deployment, while maximizing the security posture of the company.

Unlike many ZTNA solutions that cannot monitor traffic being sent and received between an end user and a controlled application, Menlo Private Access ensures that security policy is always enforced by remaining inline between the end user and protected applications; and by utilizing our Elastic Insolation Core as a control point, we can prevent sensitive data loss and stop potential malware reaching the endpoint.