NAVIGATING THE DECADE OF THE ENDPOINT

THE DECADE OF THE ENDPOINT

In the next ten years, MSPs who can manage clients' endpoints most effectively and across a wide swathe of devices will be the ones who win out, according to Matthew Phillips, Senior Account Executive at NinjaOne

The surge in remote working, bring-your-own-device (BYOD) policies and the proliferation of IoT devices have all contributed to a steep rise in the number of endpoints in the wild, with this sprawl expected to continue at pace. Staggeringly, IDC estimated that the total number of connected devices may have risen to 55.7 billion by the start of 2025.

This is creating a complex challenge, with security and skills topping the list of concerns, but it also presents a lucrative opportunity for MSPs who can capitalise. The value of the endpoint security market in the UK is set to almost double to just over £2bn by 2029 according to data from Statista, with an annual CAGR of 14.31%.

At a recent roundtable in London, hosted by ITEuropa in collaboration with NinjaOne, MSP thought leaders discussed how MSPs can leverage these opportunities, by discussing hybrid working trends, security concerns, and assessed the challenges and opportunities that will define the decade of the endpoint.

IT Europa Leaders in Discussion sponsored by NinjaOne , London, December 2024

HYBRID WORKING AND DEVICE SPRAWL

The pandemic was a watershed moment for endpoint sprawl and in its wake, hybrid working looks set to stay. Attendees highlighted that this has become more of a social issue than a political one, with one participant noting: "Due to our innovative sector, there is no longer a question over whether we can facilitate working from home. It is now down to company leaders to decide if they want to."

Many executives have said yes to maintaining hybrid working post-pandemic and depending on where you are in Europe, between 35% to 45% of workers now spend at least two days a week working remotely.

Another attendee noted: "The concept of remote working is no longer a challenge, and that means every company is on a cloud journey. An MSP's role as an advisor depends on how far along their clients are and how much they are willing to buy in or being led."

Therefore, there are also fluctuating levels of understanding particularly surrounding security and management. One attendee said: "Understanding and managing access to endpoints is dependent on maturity of the

MSP. Our clients with mature business practices understand the complexity of the subject and will be using management tools to gain visibility and deliver business outcomes."

On the other end of the spectrum, small businesses are calling out for education. Another attendee said: "At the beginning of the pandemic, clients were surprised that we could give them remote access to their endpoint at home. Although understanding of these capabilities is growing, more can be done."

CYBERSECURITY CONCERNS PERSIST

Whilst more endpoints have facilitated the hybrid shift by boosting employee productivity and satisfaction, it also translates to more business risk, with the attack vector for cybercriminals growing exponentially. One attendee said: "Security is absolutely the outstanding problem post-pandemic as the landscape is both ever-expanding and ever-changing."

According to a 2023 report from the Enterprise Strategy Group and Syxsense, 75% of organisations have suffered at least one attack related to poor endpoint device management. Sprawl is having an effect as half of organisations with more than 15 endpoint security/ management tools say more than 20% of their devices are unmanaged. Furthermore, the average cost of a data breach has been increasingly steadily YoY.

Smaller organisations are struggling with endpoint security simply due to a lack of education and skills, and these organisations don't know what they don't know. One attendee noted: "Endpoint security is a big issue in the hyper-SME market. Picture a one-man-band working from home, putting all his data through one network shared with his kids and family. Most UK businesses don't have large IT departments that will have their endpoints covered."

However, that is not to say endpoint security isn't a major problem at the enterprise level, due largely to having many members of staff not following best practices. One attendee noted: "A big trend for us is applications being downloaded by remote employees that IT has not signed off on. This is what we call shadow IT." Everest Group estimates that shadow IT is over 50% of IT spending in large enterprises. This suggests that in big organisations, sprawl is too big to be secured without the help of a trusted MSP partner.

Attendees did highlight opportunities within the security challenge with one delegate highlighting security as a: "relevant and prevalent issue that provides a good conversation piece to have with your clients." He added: "Letting a client know their endpoints aren't safe is a natural lead in to providing solutions that protect them." Another highlighted: "Businesses are becoming more receptive to these conversations and more understanding because of high-profile cyberattacks. Seniors will understand the threat and want their endpoint security clamped down."

MSP BEST PRACTICE

This does not mean that every client will be receptive for the entirety of the sales process and one delegate stated that issues in endpoint security deals often boiled down to the 'yeah buts'. He said: "We get an agreement that endpoint security is needed but money can quickly cause a problem and lead to clients looking to cut corners. We tell them that there is no point in us building a wall but leaving the back door open."

Another attendee added: "In situations like these we have to say, 'let's either agree we are the subject matter experts in the room, or that we are not, but if you won't listen to us then we can't work together'. Constant

frank and honest conversations will always be appreciated."

Attendees agreed that the best MSPs have honest leadership that will tell their customers things they don't necessarily want to hear. One said: "In this market, you have to tell your clients hard truths, but we are moving into an era where customers don't want to hear lies and puff anymore."

One company in attendance shared that they win business in this space by having conversations about when things have gone wrong and educating customers that this isn't normal. He said: "People don't know what else is out there or what they should expect. Price doesn't drive movement in this space as much as a big problem or a new senior member of a team who knows what they are talking about."

Another pointed out the importance of demonstrating value for customers to ensure that price doesn't drive movement. He said: "Endpoint security customers can be managed wonderfully, but you get undercut because nothing has gone wrong, and the client hasn't understood your value. That is where a good management and monitoring tool will provide visualisation and reports that you can show off."

NINJAONE AND THE CHANNEL

NinjaOne positions itself as one of the fastest-growing vendor in the Remote Monitoring and Management (RMM) space and is currently empowering more than 20,000 IT teams with visibility, security, and control over all endpoints.

The company is looking to expand its UK channel through meaningful and mutually beneficial relationships with partners that are looking to thrive in endpoint management. As the channel program in the UK, and more broadly in EMEA,

Matthew Phillips, Senior Account Executive at NinjaOne

continues to grow, NinjaOne is also looking to distributors to support its efforts in the region.

Phillips said: "We are ramping up activity to highlight that RMM is more than just a nice solution to bundle into a service offering, it is a necessity." He noted that NinjaOne has built up a strong reputation in the RMM space and this is why some IT people show initial interest in NinjaOne. Matthew continues, "When first talking with us, they quickly realize all the useful tools we provide in our product stack and organizations see NinjaOne as a big opportunity for tools consolidation.

Concluding the roundtable, Matteo Rivetti, Account Executive, explained: "Our founders are IT people at heart with an hands-on approach, therefore our core identity builds on the foundation that our solutions are built from the ground up."

"This is a big motivator for people that chose to partner with us," added Rivetti. "Another reason is our consistently top ranked support service, helpful training, tools and free onboarding. We always aim to take a more consultative, friendly and supportive approach, where we want to be as easy and pleasurable to do business with as possible."

NinjaOne's dedicated Accounted Managers are tasked with retention as well as acquisition to ensure that relationships are properly fostered. To ensure they are mutually beneficial, NinjaOne invites feedback and hosts partners at its Dojo to understand what additional services or improvements MSPs would value. Phillips added: "Mobile device management is top of that list as it really improves life for their end-users."

Matteo Rivetti, Account Executive NinjaOne

To learn more about NinjaOne and discuss partnership opportunities, please visit: https://www.ninjaone.com/