SentryBay®

White Paper

Prioritise Security to Successfully Deliver BYOD in a Zero Trust Framework

Table of Contents

- Introduction
- The BYOD Market
- The Security Implications of BYOD
- BYOD Use Cases
- Analysts advocate critical security technology to mitigate BYOD/BYOPC risks
- Zero Trust and its Role in Enabling BYOD
- Managing Perceived Zero Trust Complexity
- How SentryBay can help
- Case Study: North American insurance company
- Case Study: Global investment bank & financial services firm
- Conclusion

Introduction

The shifting sands on which our working lives are currently based have propelled companies to make difficult decisions when it comes to the use of, and investment in, technology. At the beginning of the pandemic when face-to-face interactions of virtually any kind abruptly stopped, some organisations made budget cuts while they scrambled to support remote workers. Others reorganised their investment plans and accelerated digital transformation efforts.

It wasn't until hybrid working was accepted as the norm for the future, however, that most companies put in place long-term strategies and started investing accordingly.

Spending more, rather than less, seems to be the order of the day according to industry analysts. IDG, for example, forecasts traditional technology spend worldwide on hardware, software, services and telecoms to increase from $4,130,413 in 2021 to $4,453,674 in 2023[1]. Gartner forecasts worldwide IT spending to exceed $4.5 trillion in 2022, an increase of 5.5% from 2021[2].

Where previously organisations invested in guarding the network perimeter, spending now is focused more on trying to protect corporate data wherever it is entered, transmitted or residing. As a result, effort and investment is going into setting up or reinforcing Bring Your Own Device (BYOD) or Bring Your Own PC (BYOPC) models. This might seem counterintuitive – investing in technology that employees already own – but without securing those devices, the potential impact and cost of an intrusion could be devastating.

In the past, companies managing a flexible BYOD model put in place limits to network access, but as remote work has proliferated, so too has malware designed to take advantage of unmanaged endpoint devices. The result is that limiting network access is no longer sufficient to keep cyber-attacks at bay.

In a recent Twitter poll for SentryBay, 69.1% of security professionals said that a rethink is needed to deal with the cybersecurity threat now that devices and applications have moved outside the corporate network.

The main difficulty is the lack of control that organisations have when employees are using their own devices. How can they know the status of a home PC, laptop or smartphone? While many are protected by anti-virus software, this will be unlikely to stop a keylogging attack or an attempt to snatch sensitive personal or financial data through screen-scraping.

It's no surprise, therefore, that amongst the respondents to the SentryBay poll, almost a quarter (23.6%) were very concerned about security breaches against the backdrop of hybrid and remote working.

There is a solution to this.

> In a recent Twitter poll for SentryBay, 69.1% of security professionals said that a rethink is needed to deal with the cybersecurity threat now that devices and applications have moved outside the corporate network.

[1] IDC Forecast https://www.idc.com/promo/global-ict-spending/forecast

[2] Gartner PR October 2021 https://www.gartner.com/en/newsroom/press-releases/2021-10-20-gartner-forecasts-worldwide-it-spending-to-exceed-4-trillion-in-2022

The BYOD Market

At SentryBay, we understand the steps that need to be taken, and the importance of proactive data protection solutions that can be delivered through software that is specifically focused on protecting remote endpoint devices.

In this whitepaper, we will address the current status of BYOD, its use cases and security risks, and outline what companies need to do, the most important of which is to adopt zero trust.

The BYOD Market

The BYOD market is expanding. According to Global Market Insights[3], the sector is expected to hit $367 billion this year, up from just $30 billion in 2014. Much of this growth has taken place in the last two years because of the global pandemic. However, the ubiquity of digital devices has been a key factor in enabling employees to work remotely for over a decade and employers have taken full advantage of this.

It's easy to see why. Research[4] suggests that employees are more productive when using their own devices, saving over 80 minutes of time per week. In addition, less training is needed and typically, apps and programs are regularly updated by employees. BYOD is a key element in workforce flexibility and the sanctioned use of personal devices underlines this. However, the overwhelming corporate argument for BYOD is cost-savings. With spend on hardware, support, training and maintenance reduced, not just temporarily but through the whole lifespan of the device, or the employee's tenure with the company, it makes sound financial sense.

Making it work securely, however, does remain the responsibility of the organisation. The SentryBay poll found that for those companies that had adopted BYOD, 28% found user privacy concerns to be a challenge. This might be why over a third (33.5%) thought it was too complicated. Companies are clearly striving to find a balance between protecting access to corporate data and applications while simultaneously guarding employees' own privacy.

The SentryBay poll found that for those companies that had adopted BYOD, 28% found user privacy concerns to be a challenge.

[3] Global Market Insights 2016 https://www.globenewswire.com/news-release/2016/03/22/822021/0/en/Bring-Your-Own-Device-BYOD-Market-size-worth-USD-366-95-Billion-by-2022-Global-Market-Insights-Inc.html

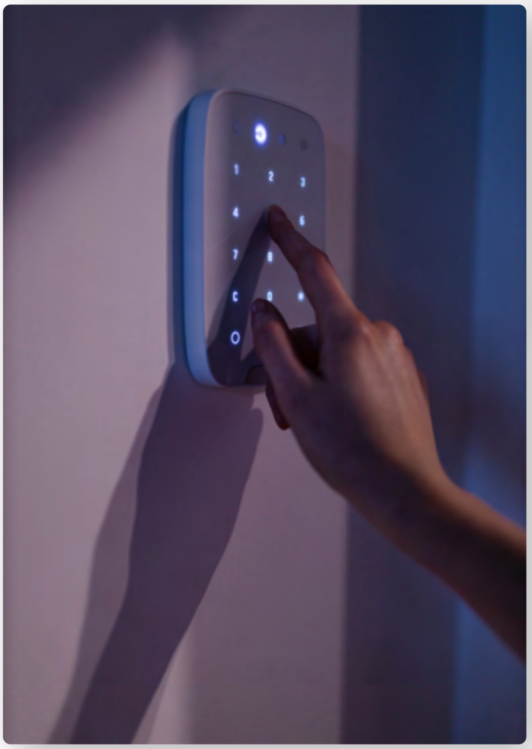
[4] Cisco Annual Report 2016 https://materials.proxyvote.com/Approved/17275R/20161014/AR_300358/INDEX.HTML#/40/

The Security Implications of BYOD

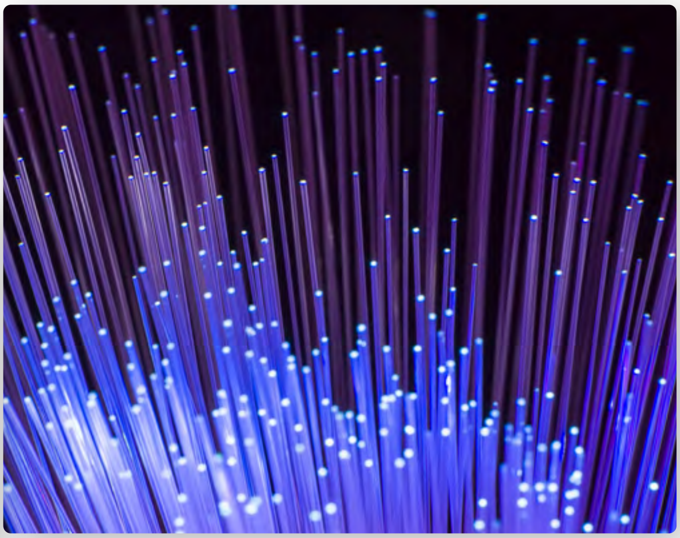
Along with the risk of devices being lost or stolen, and the hazards attached to unsecure Wi-Fi, particularly in public places, the main security threat of BYOD is malware. The pandemic presented many opportunities for hackers to exploit vulnerable systems, which increased global cyber-attacks by 29% in the first half of 2021[5]. There is every reason to think this will increase in the future.

Among the most common threats are keyloggers, screen scrapers, browser-based attacks, file interception, RDP double-hop or VNC attacks, and the impact of these cannot be underestimated.

Keylogging and screen grabbing are widely used to access sensitive data. If a keylogger is installed on a device being used remotely which is unmanaged, cyber-attackers can gain full access as the employee logs in and to everything they enter at the keyboard or display on their device.



All unmanaged endpoint devices present a threat. At SentryBay, our experience is that while companies might demand and implement stringent security for employees using a personal laptop, a home PC or a tablet when they are working remotely, they are caught unawares when it comes to enabling access to sensitive corporate data on a mobile phone. According to Microsoft, traditional computing devices such as servers, desktops and laptops represent only 40% of relevant endpoints. The remaining 60% are mobile devices and these are 'woefully under-protected'[6].



[5] Checkpoint Cyber Trends Report 2021 https://pages.checkpoint.com/cyber-attack-2021-trends.html

[6] Microsoft blog April 2020 https://www.microsoft.com/security/blog/2020/04/07/mobile-security-60-percent-problem/

BYOD Use Cases

Improving management of endpoints is the key to ensuring they can be used securely. Here we look at some of the most common BYOD use cases where management of remote devices is the priority:

- **VDI** – Desktop virtualisation simplifies BYOD and enables apps, data and storage to be managed centrally. Remote access is not restricted to traditional computing devices so it can incorporate mobile phones, and data is not stored on the individual device reducing the risk of hacking or theft. Common examples are VMware Horizon and Citrix Workspace. This category also includes thin client operating systems such as Stratodesk, which also enable VDI.

- **DaaS** – Desktop-as-a-Service outsources the device to a third-party which manages both personal and enterprise apps and data. This is stored in the cloud rather than on the device and encrypted before being distributed over the network. Common examples are AWS Workspaces, Azure Virtual Desktop (AVD), dinCloud and EvolveIP.

- **SaaS** – Software-as-a-Service is a popular means of securely enabling software use on a wide variety of remote BYOD devices. Apps and data reside in the cloud and can be made available via a browser. Most common examples include Salesforce, Workday, Microsoft 365 and ServiceNow.

- **UEM** – Unified Endpoint Management allows companies to control and secure desktops, laptops, tablets and mobile phones remotely via a software solution. An example of this is VMWare Workspace ONE, formerly AirWatch, with another being Microsoft Intune.

- **Collaboration apps** – Workspace chat and video conferencing tools have become increasingly popular during the pandemic, enabling employees to remain connected and providing access to file storage and applications. Examples include Microsoft Teams as part of the Microsoft 365 family of products, Zoom, GoToMeeting and Slack.

Analysts advocate critical security technology to mitigate BYOD/BYOPC risks

Where prior to the pandemic BYOD/BYOPC models were regarded as a means to enhance productivity for remote workers, they are now being seen as a critical tool to enable long-term hybrid and work-from-home practices. The rapid adoption of BYOD/BYOPC in response to the pandemic has, however, driven demand for a fresh approach to security, one which can envelop endpoint devices wherever they are being used to connect to the corporate network.

In 2020, Gartner highlighted BYOPC security as one of two technologies that would have a 'transformational impact on global businesses' and would 'reach mainstream adoption in the next two to five years.'

"Prior to the COVID-19 pandemic, there was little interest in BYOPC," said Rob Smith, senior research director at Gartner. "At the start of the pandemic, organisations simply had no other alternative. The urgent need to enable employees to work from home and a lack of available hardware bolstered its adoption globally. Gartner clients said their adoption of BYOPC is up from less than 5% in 2019."[7]

This prediction was borne out in August 2021 when ReportLinker announced that the global BYOD and enterprise mobility market would grow by $1.01 billion between 2021 and 2025. This was based on the organisation's holistic analysis, taking in trends, growth drivers, challenges and vendor analysis.[8]

But adoption of BYOPC and BYOD is not without its challenges, as Gartner has pointed out: 'As BYOPCs are often infected with malware or ransomware and fall victim to phishing attacks, IT must limit and control access by offsetting the PC hardware investment with critical security technologies such as MFA, cloud access security broker (CASB), zero trust network access, virtual desktop infrastructure and desktop as a service.'

The National Cyber Security Centre (NCSC) agrees: 'Although the conceptual aims of BYOD are an attractive prospect to most organisations, it comes with a conflicting set of security risks and challenges.' NCSC says that balancing an organisation's need to protect and maintain control of its data and systems against the usability, and privacy expectations of the device owner can be difficult[9].

NCSC has identified the benefits of Zero Trust and has produced guidance for organisations to help ease their journey towards a Zero Trust architecture. It says: 'Zero Trust allows strong authentication and authorisation, whilst reducing the network overhead of extending your corporate network out into your users' homes, as with a traditional VPN model.'[10]

In 2020, Gartner highlighted BYOPC security as one of two technologies that would have a 'transformational impact on global businesses'

[7] Gartner PR August 2020 https://www.gartner.com/en/newsroom/press-releases/2020-08-26-gartner-says-bring-your-own-pc-security-will-transfor

[8] ReportLinker PR August 2021 https://www.globenewswire.com/news-release/2021/08/02/2272666/0/en/The-Global-BYOD-and-Enterprise-Mobility-Market-is-expected-to-grow-by-1-01-bn-during-2021-2025-decelerating-at-a-CAGR-of-20-72-during-the-forecast-period.html

[9] National Cyber Security Centre 2021 https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device

[10] National Cyber Security Centre 2021 https://www.ncsc.gov.uk/blog-post/zero-trust-is-it-right-for-me

Zero Trust and its Role in Enabling BYOD

Companies should be implementing proactive protection delivered through fit-for-purpose software specifically focused on preventing sensitive data loss or leakage from the remote endpoint by wrapping applications so that they are securely confined. This should be an integral element in a zero trust approach.

The first, and most important step is to protect every endpoint that will connect with the company network. The motto "Never trust, always verify" is a useful reminder. Zero trust literally means that every employee (and their device) is treated as a threat by default, even those that are already inside the network. They cannot be granted access to the system at any level until they have been verified.

To clarify other terms that are regularly used, zero trust access (ZTA) is about controlling and understanding who and what is using the corporate network. This allows the appropriate level of access to be granted not just to the employee, but to the device too. Zero trust network access (ZTNA) relates more closely to brokered access for users to applications and is an element of ZTA.

It is a measure of how important zero trust has become in deploying a BYOD model, that in the Spiceworks Ziff Davis 2022 State of IT Report[11], which surveyed more than 1000 technology buyers in North America and Europe, 65 % of companies in Europe said that they were implementing or planning to use zero trust security solutions within the next two years.

The SentryBay poll backs this up with 58.3% of respondents saying that a zero trust approach to security was essential, and 19.9% saying it was important.

When it comes to implementing zero trust, however, this can be more of a challenge, and only a third (33.6%) said that they had, while 8.5% were in the process and 10.6% planned to do so in 2022.

Zero trust literally means that every employee (and their device) is treated as a threat by default, even those that are already inside the network.

[11] Spiceworks Ziff Davis State of IT Report 2022 https://swzd.com/resources/state-of-it/#chapter-4

Managing Perceived Zero Trust Complexity

Companies cite a variety of reasons for delays or difficulties in implementation. Among these are a lack of understanding when it comes to embedding identity and access management, concerns about the impact on productivity and a lack of budget or suitable resources to manage the process.

The key to a successful implementation is to look at zero trust holistically. It is not a single solution or a platform, it's an approach to security that demands verification of all users and all devices, and it needs to be built into a company's broad IT strategy.

Adopting BYOD and supporting remote working means companies must elevate their security posture. The traditional combination of internet security, anti-virus software and securing the wireless network with virtual private networking (VPNs) is no longer enough to defend against the onslaught of cybercrime. While each one of these has a role to play, none of them is a complete solution for managing today's threat landscape.

The key to a successful implementation is to look at zero trust holistically. It is not a single solution or a platform, it's an approach to security that demands verification of all users and all devices, and it needs to be built into a company's broad IT strategy.

How SentryBay can help

SentryBay advocates a layered approach that provides strength and depth and ensures that while a specific attack may bypass one security measure, it will be thwarted by another. The most precious corporate asset – data – and the applications that handle it, need to be placed at the centre, with security layers confining it protectively.

Our solutions are designed to do exactly this to enable BYOD and support a zero trust approach.

SentryBay recognises that companies are still assessing their options following the tumult of the last two years, and that many have a mixture of remote and hybrid infrastructure. The company is well placed to work with multiple different set-ups, providing a common security baseline. Its solutions are fit-for-purpose, wrapping data and applications securely, regardless of the status, the type of endpoint device being used or the infrastructure that it is connecting to, and this is effective in neutralising the threat of cyber-attack, particularly from insidious keyloggers, screen scrapers and similar malware.

The applications that are protected are those typically accessed remotely using SaaS, DaaS, UEM, VDI or collaboration apps. Organisations that are using one, or all, of these technologies and platforms can rely on our solution to work seamlessly.

SentryBay also supports the operational needs of its customers by offering multiple simple means of deployment, minimal support requirements, compatibility with the most widely used software packages, and with low process overheads. By protecting the data that is entered into these applications, organisations are, in effect, ensuring that even unmanaged devices are as secure as those that are fully managed by the organisation.

Perhaps most importantly, SentryBay's solutions are based on application confinement, which means that the applications and all the data that flows in and out of them, are constantly protected from malware without the need to identify it. When you combine this with kernel level anti-keylogging measures and always-on screen and video protection - it is the very definition of a zero trust environment.

By protecting the data that is entered into these applications, organisations are, in effect, ensuring that even unmanaged devices are as secure as those that are fully managed by the organisation.

Case Study

North American insurance company

The Challenge

With tens of thousands of independent agents working remotely, and more being trained and added to the team each month, the insurance company was investing heavily in secure corporate locked-down laptops.

These enabled the agents to securely protect credit and debit card information submitted by online customers and meet with the scrutiny of PCI DSS regulations.

The company wanted to find a way to lower its spend on new devices, which were costing approximately $1000 each, while ensuring security and crucially, meeting compliance.

The Solution

The organisation adopted a BYOD strategy for its extensive team of agents to tackle the cost issue. It deployed a VDI system alongside Azure Cloud, however in doing this, it opened itself up to compliance risk on the endpoint. To solve this, SentryBay's Armored Client was deployed to secure the VDI client and meet the requirements of PCI DSS regulations.

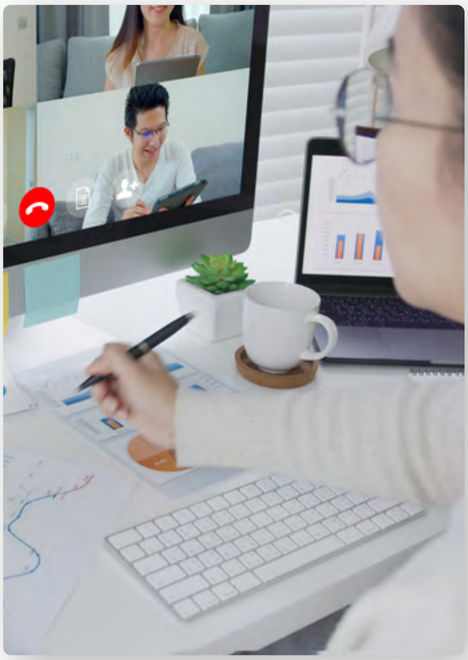
The Armored Client was installed quickly and easily through the SentryBay portal using the 'single sign-on' function. Ensuring agents downloaded the software was achieved through a certificate-based device validation process as the VDI sessions were launched, which provided demonstrable evidence of compliance with PCI.

The Outcome

Deploying the Armored Client software to multiple endpoints was carried out with ease, transforming an unmanaged network of devices into secure endpoints that could interact with the corporate systems without risk.

The insurance company dramatically reduced its CAPEX – and the overheads of managing corporate devices – by adopting a BYOD strategy and that was only possible because the Armored Client can be downloaded in one-click to create an armoured shield on any unmanaged device.

As well as meeting internal infosec requirements, SentryBay helped the company to meet its obligations to PCI DSS and could be confident that customer data is fully protected moving forward.



Case Study

Global investment bank & financial services firm

The Challenge

The bank's existing security solution, designed to protect thousands of globally distributed workers accessing its corporate network, failed to meet the necessary financial compliance regulations.

The organisation needed software that filled the security gap, was easy to deploy and manage, and developed with compliancy built-in.

Against a backdrop of growing BYOD usage, the bank had to cut the escalating costs of deploying – and managing - corporate laptops to employees.

The Solution

SentryBay Armored Client replaced the previous solution which did not meet infosec and audit standards and was causing high amounts of support calls. The solution brought a highly customised security profile to an initial 7,000 remote endpoints, which has now grown to around 20,000, helping to deliver full compliance with the necessary global financial authorities.

The Outcome

Seamless deployment of Armored Client brought rapid protection for remote employees globally.

The bank saved substantial CAPEX costs by no longer funding new corporate laptops to ensure secure connections. A BYOD model can now be more fully embraced across the company.

Patented protection at the kernel level against keylogging and screen capture ensures endpoints are fully compliant with financial regulations.

The earmarked deployment of the Armored Client to a further 10,000-20,000 endpoints over the next two years is testament to the success and efficacy of the solution since it was originally deployed four years ago.

Conclusion

All organisations, regardless of size, face ongoing and important decisions when it comes to technology and cybersecurity. They all have a duty of care to their customers, clients, suppliers and stakeholders. Delivering baseline security for devices, applications and data is fundamental, particularly when the concept of the corporate network has changed beyond recognition.

Understanding what is needed when deploying a BYOD policy and zero trust approach is crucial to a successful outcome. Unless data is protected as it is entered from the keyboard or onto the screen, a gap in the corporate armour is opened which renders the company vulnerable, not just to a damaging and potentially costly security breach, but also to non-compliance with regulations.

BYOD is increasingly the route of choice for many businesses as they negotiate the path ahead and it can lead to cost savings, but at no point should these be at the expense of lower security standards.

SentryBay®

Headquarters

UK 20 Little Britain
London EC1A 7DH

+44 (0)203 478 1300
+1 949 394 4902 1300

info@sentrybay.com
sentrybay.com