Endpoint connectivity

Prepared by:
Blake Markham, Security Consultant

Table of contents

1. Introduction

The need to protect IT assets from a cyber attack is paramount and from a physical endpoint perspective, this presents a challenging dynamic when wanting to prevent a data breach via the myriad of USB mass storage devices.

The popularity of USB usage has grown and it has become a common vehicle for spreading malware. One study showed that out of approximately 300 USB memory sticks dropped around a university campus, 98 per cent were picked up and almost 50 per cent plugged in to a computing device [1]. Furthermore, the Department of Homeland Security (DHS) staged a series of tests which showed that 60 per cent of people who picked up random USB memory sticks that had been scattered in government buildings and car parks plugged them into networked office computers. More significantly, this increased to 90 per cent if the USB device had an official and convincing departmental logo displayed [2].

The popularity and convenience provided by USB devices means that they are likely to be used for the foreseeable future. Therefore, it is vital to manage USB in a secure manner. Many organisations implement network security through the use of firewalls, intrusion prevention and detection with access controls and various levels of authentication. However, these fundamental controls are not always able to mitigate against simple plug-and-play USB devices which can also be used to simply bypass air-gapped architectures, either for data exfiltration or the infiltration of malware.

USB storage devices make exporting data extremely easy for an individual. This could result in severe reputational and financial (regulatory fines) damage for an organisation should the data be sensitive. To this day, there are still many organisations that do not include USB storage devices in their security policies and few IT security managers actively monitor USB usage by their employees.

As a result, when working with USB endpoints, organisations need to adopt a strategy that can provide flexibility and has the ability to adapt to technological advances while not compromising on the security of the underlying IT infrastructure. This flexible approach would not only include direct mitigation, utilising security software among other solutions, but would also address the wider issue of USB memory device usage by monitoring endpoints through Data Loss Prevention (DLP) techniques.

Nevertheless, the threat posed is only amplified with the increasing complexity of undetectable malware as well as mass storage devices that can also emulate Human Interactive Devices (HIDs) and Ethernet (network) ports. As a result, organisations need to further scrutinise and control what devices are allowed access to their networks. Additionally, popular topologies, such as Bring-Your-Own-Device (BYOD), make securing the modern IT environment increasingly difficult.

There are steps that can be taken to reduce and prevent data loss and malware infection. This can be done by implementing a suitable endpoint use policy and taking a layered approach by introducing hardware and software-based solutions. Furthermore, as physical access is a key component through such plug-and-play devices, educating users of the security risks posed by USB is vital.

This whitepaper aims to identify the security risks posed by USB and address the associated concerns by looking at the available strategies and solutions that can be used to deliver effective USB endpoint access control.

2. What is endpoint connectivity?

Endpoint connectivity can be looked at holistically as any device that can accept a connection by either a virtual or physical port. This whitepaper will specifically examine those devices that provide a physical connection through USB connectivity, something that many businesses now rely on. It will look at USB storage devices and how these have evolved to emulate many peripherals that connect to these types of endpoints.

As technology has evolved, USB devices have grown in popularity due to the convenience and performance they offer and the significant reduction in cost for large amounts of peripheral storage capacity. It is important to acknowledge that although the focus of this whitepaper is on USB connectivity, multiple threats still exist in other forms of removable media including:

- Optical discs (Blue-ray, DVD and CDs)
- Memory card slots (SD and Micro SD)
- Hard Disks (eSATA)
- FireWire

However, as USB continues to be the choice of many in order to share data fast and efficiently, new and more sophisticated methods have developed to exploit a user's endpoint device. Devices like the USB Rubber Ducky [3] offer data exfiltration in an instant through the automation of malicious payloads by mimicking HIDs. The USB LAN Turtle [4] is another new device offering man-in-the-middle type of attacks or network reconnaissance through a network adapter.

Nonetheless, USB endpoint connectivity is essential and mandatory for many businesses to be able to operate. This is because they are needed in order to connect peripherals such as printers, mice and keyboards. Simply disabling USB in, for example, the Windows group policy does not always offer the required granularity of control and rendering broad control is practically useless for most entities. Therefore, newer and smarter ways of managing USB endpoints are needed.

3. Risks introduced by endpoint connectivity

When examining the risks posed by the use of USB endpoints, there are some core threats that exist. As a result, organisations are under constant pressure to improve the way they manage and secure corporate and personal data. According to the SANS Institute, massive amounts of resources are invested in protecting confidential information with some of the most critical issues being data leaks, malware and overall access control [5].

In this section of the paper we will cover the key threats to consider relating to USB and the possible negative outcomes that may arise if controls are not put in place.

3.1 Data leakage

Modern USB mass storage devices offer affordability, compactness, increased transfer speeds and are incredibly valuable for productivity in the workplace. However, what initially might appear to be beneficial does in turn present greater risks as movement of data is made seemingly effortless.

USB usage: USB mass storage devices impose increased security risks due to their relatively small size. They are easily misplaced and as a result are prone to getting lost or being stolen. Similarly, the device can be used in a covert manner to siphon large quantities of sensitive information. All that is required is to be able to plug in the device to the USB endpoint in order to start copying data. The severity of this simple method of data movement was exposed when masses of confidential documents of the National Security Agency (NSA) were leaked to the public in 2013 [6].

USB movement: It can be a hard task for an organisation to track the whereabouts of USB devices. As a result of this, data can be lost or stolen without any inclination as to who owned the USB device and what data might have been stored on it. Even with stringent use policies in place, this will not necessarily stop employees from copying confidential information onto USB devices, perhaps simply for their convenience as opposed to any nefarious reasons.

Data leakage brings real risks and substantial financial costs if handled incorrectly. Sensitive data might include credit card details, Personal Health Information (PHI), Intellectual Property (IP) and trade secrets or Personal Identifiable Information (PII). It has become increasingly common to learn about major data breaches of these sorts and it can be very costly, not just financially but also to an organisation's reputation. According to IBM and the Ponemon Institute, a recent study of 383 companies in 12 countries revealed that the average cost of a data breach is in the region of $4 million [7].

3.2 Malware infections

Due to the potential costly impacts of data leakage, organisations can easily focus purely on what data could be exfiltrated through USB. Therefore, what the USB devices can bring into the IT environment can be easily overlooked. A study carried out by Sophos found that out of 50 USB devices bought at an authority's lost property auction, 66% of them were infected with some form of malware [8]. This percentage would have likely been even higher in more recent years due to the introduction of more sophisticated methods of malware deployment and the online availability of malicious code.

Mass spreading of malware can also be rapid and pandemic across Microsoft Windows networks, whereby the malware might automatically execute upon insertion of a USB device due to Microsoft's Autorun feature. This feature has since been disabled by default in modern Windows operating systems but does highlight the disastrous effect malware can have if not handled correctly.

Furthermore, in 2010 the infamous Stuxnet highlighted just how serious propagated malware can be. Stuxnet was found to be primarily spread through the use of USB drives which were plugged into connected network infrastructure endpoints. Interestingly, the malware did not exploit the Autorun feature but instead a vulnerability in shortcut (.lnk) files was placed on the infected USB device. As a result, a user would only have to browse to the USB drive and let the files render, allowing the malware to hijack the running process and initiate infection without the need to manually execute a file [9].

Although Stuxnet targeted Industrial Control Systems (ICS), it is clear how malware can adapt to exploit new vulnerabilities, bypassing controls put in place such as Microsoft's disabling of the Autorun feature. It also provides insight into what to expect from future malware propagated through USB mass storage. It is important to note that malware is used as an umbrella term for many different types of malicious code that result in undesired outcomes. A brief list and description of common types of malware threats via USB connectivity include:

- Virus and worms: These types of malicious infections are very similar. A virus will attach itself to a piece of software in order for it to spread and reproduce itself when the software is executed. Worms on the other hand do not need to infect a program on the system as they are able to move independently across a network.
- Spyware: Spyware is a type of malware that monitors a user's activities without their consent or knowledge. This type of malware will typically include keystroke logging and gathering various types of data. It can disguise itself with legitimate software and interfere with system settings.
- Trojans: Trojans are among the most dangerous types of malware and act more covertly than a typical virus. They appear as regular software but hidden within is malicious code that can introduce persistent backdoors to a system, resulting in unauthorised access. They can target highly sensitive data and result in Denial of Service (DoS) attacks by exhausting system resources.

3.3 Malicious firmware

USB endpoint devices have proven to be a useful tool for the IT environment and more peripherals utilise the convenience and universality of USB for connection than would have been expected. The risk posed by USB devices is, therefore, not always related to malware and its propagation; but rather, an implicit trust in USB has increased owing to the wealth of USB peripherals that exist.

Examples of peripheral USB endpoints include:

- Keyboards
- Mice
- Audio headsets
- Network adapters
- Printers

USB connectable devices being used as an attack vector are a favoured choice of cyber criminals for spreading malicious software or malware, but they can also contain malicious firmware. In order for all of the above to function for their intended purpose, they run a type of firmware. This firmware will of course vary depending on the type of USB device. For instance, when using a USB memory stick the firmware will allow the transfer of data or files.

When it comes to HIDs, such as keyboards, the firmware allows the conversion of physical key presses by a user to digital key presses, which is in-turn sent over the USB connection to the computer. This is where the threat lies as firmware is not a typical piece of software a computer would have access to, so it cannot necessarily check to see if its intention is malicious or not. Code is executed on the USB device and there is no easy way to verify if the USB firmware is safe. The malicious code is simply invisible to available security tools and modern operating systems because there is no need to store the malware on the USB storage device's memory where it could be detected by anti-virus (AV), but instead is hidden in the firmware.

To prove the concept, there are multiple USB-type devices such as the USB Rubber Ducky [5] that tricks a computer into believing that a USB keyboard has been connected. It is then able to emulate the device entering key presses, surpassing human speeds as though it were from a trusted user. Essentially, this is the same as someone accessing another's computer without permission to execute commands that could then compromise that system and subsequently the network.

To put this into context, almost any USB device could be used to act in a malicious way, this can again be highlighted with the LAN Turtle example [4]. This device emulates an Ethernet port allowing an attacker to intercept network traffic and, in some configurations, gain a remote shell on the system it has been plugged into. The methods that are explained above are not entirely new. However, security research has revealed that many USB drives firmware can be re-programmed without any controls to contain malware [10].

BadUSB [11] has been proven by security researchers where a regular USB drive, or stick used to store data, is re-programmed to behave as the devices described above, further reducing the likelihood of detection. This highlights the fundamental design flaw in USB devices and the lack of security they really offer. Finally, a recent venture called USB Killer claims to be able to deliver a 220-volt surge which physically kills the computer it was connected to [12], further indicating the seriousness of endpoint exposure to USB.

The diagram below provides a visual representation of how an attack is structured from these types of devices:

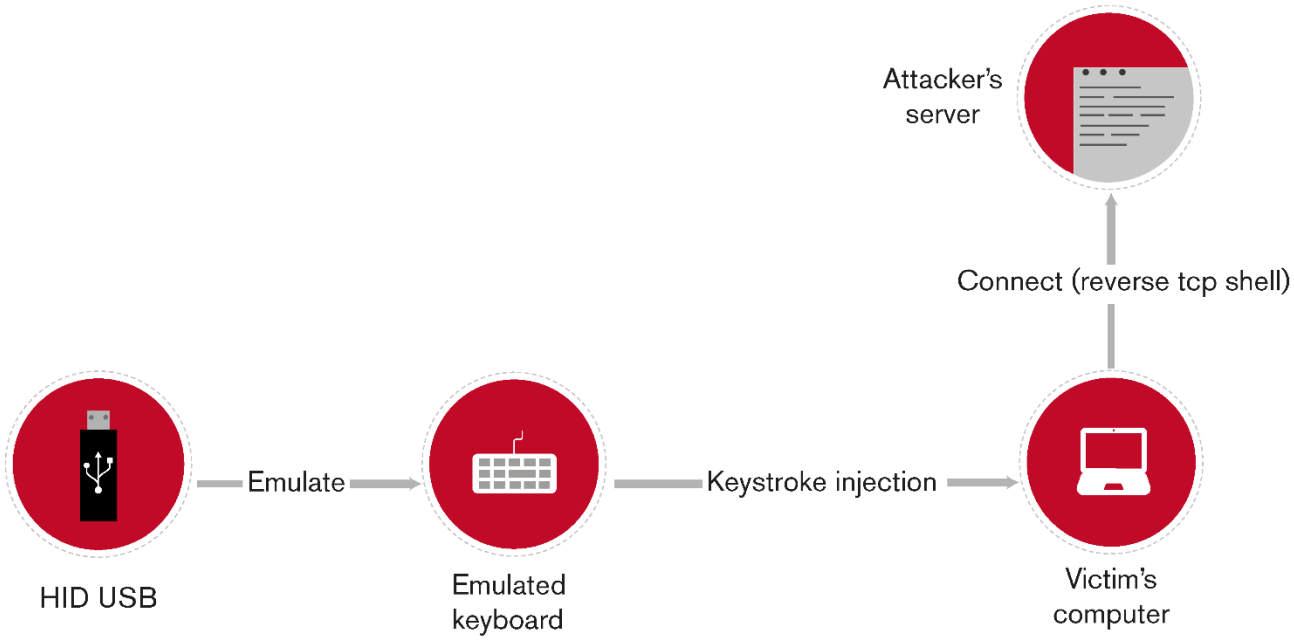

Figure 1. Diagram of a malicious USB firmware attack [1]

It is important to acknowledge that devices that have been manipulated like this render conventional security methods useless. AV and formatting of the USB sticks will do nothing because the malicious code resides in the firmware. Interestingly, this is now drastically changing the way organisations respond to compromises.

In the past, it would be assumed that malware would be present somewhere on an infected machine or network and that various AV and malware scanners would be required to detect the infection. Now, it must be assumed that the peripherals connected to the network could also be infected.

4. Importance of endpoint security (USB)

When approaching USB devices from a security perspective, there are various aspects to consider. This will vary depending on the organisation, its size, operations and requirements. This means there will not necessarily be a ‘one-size-fits-all’ solution but instead a best-fit approach for specific needs. Organisations will have to address endpoint connectivity proactively because disabling USB outright in, for example, Windows Group Policy will not work as it offers little granular control. This is because USB is the only option for many connected devices that are required for business operation.

USB provides only a single physical attack vector through the USB port itself. Historically, it was thought that this threat could be mitigated by simply blocking the port, perhaps through application of epoxy resin (or similar) to physically block the USB ports. There are more sophisticated methods of blocking USB endpoints, such as commercially available USB port locks, which would not risk physically damaging the endpoints. However, this solution might be impractical as it might not always be feasible to block every endpoint. Therefore, the idea is to strike a balance between the usefulness of USB and protection that minimises the risk by implementing a USB access control strategy. A combination of both policy and technological solutions will be required to protect corporate assets from future attacks.

5. A guide to acceptable USB usage

Implementing endpoint security can be difficult. The following points highlight areas that an organisation should consider when approaching USB usage:

- Limit USB devices allowed to connect and the file types that can be executed based on user roles.
- For USB storage devices issued to employees, excessive storage capacities should be avoided in order to minimise the impact from a lost device. E.g. issuing devices with an upper limit of 500Mb would be preferable to provisioning memory devices with capacities of ten Gb or more.
- There should be a centrally-managed database for all USB devices issued by the organisation so that a maintained asset register can be created and used to track USB devices.
- The data stored on corporate issued-USB drives should be regularly audited.
- IT managers should issue notices to employees highlighting acceptable USB usage and highlighting the associated risks.
- Following an external business trip where a USB device has been used or where an employee has left the company, devices should be checked and quarantined until deemed safe to be re-issued and used on the corporate network. Depending on the outcome, this may require secure erasure and/or destruction of devices.
- USB devices that are not issued by an organisation should either not be allowed to connect to the network or be scrutinised and approved by the IT department.
- Organisations should procure USB devices from trusted sources, ensure security in the supply chain and look to use only approved or certified products that offer baseline levels of assurance in terms of encryption levels supported, independent security testing etc.
- Users must adhere to the password and encryption polices set when using USB drives. This would involve using a strong encryption algorithm and a complex password.
- Where necessary or possible, employees should securely attach or chain USB devices in order to prevent loss or theft.
- Laptops and corporate devices should be routinely patched and all security software maintained with the latest updates.

6. Endpoint solutions

Mitigating the risks associated with USB endpoints is difficult and consideration has to be given to all types of solutions. A holistic approach is recommended when implementing a USB endpoint strategy.

Encryption

Among the most obvious of technology solutions is encryption. Despite this many companies still fail to use encryption on their USB storage devices. In the UK, a survey revealed that just 37 per cent of respondents encrypted data when leaving the office [13]. Encryption secures all data on an endpoint and USB drive, preventing data leakage and any unauthorised user from executing malware that may be stored on the device. It should therefore be mandatory for all USB devices deployed by a company to have strong encryption and require a complex password.

Recommendations for password policies:

- Set minimum character limit depending on the account type (nine - 14 characters).
- Enforce a suitable lockout policy (five attempts).
- Passwords should contain upper and lower case letters with digits and special characters.
- Passwords should be unique and not a word that can be guessed with dictionary attacks.
- Password blacklisting can be used to disallow common password choices.

Choosing a strong encryption algorithm is important for protecting data. AES-256 is highly recommended as it is widely accepted to be secure and is broadly supported. Automatic encryption solutions that encrypt data once it has been transferred from one device to another are also available. Furthermore, USB hardware encryption should be considered, if deemed necessary, to add an additional layer of security on top of any software solutions.

There are other alternatives to using conventional passwords as a means to authenticate a USB. Fingerprint biometrics offer convenient and easy methods of unlocking a device and this eliminates the hassle of having to remember a password. In some cases, should there be a poor password policy in place, this is why users set weak passwords. It is important to note that, although convenient, fingerprints may pose more of a security risk despite how attractive they may seem. As we typically leave residual fingerprints on most surfaces that we touch, this renders those latent prints potentially vulnerable to copying. This means that the password is never a secret and one cannot simply revoke a fingerprint, as can be done with a typical password. Furthermore, simple and cheap methods can be used to recreate the fingerprint once lifted from a surface, therefore increasing the likelihood of a compromise. However, biometrics combined with other authentication factors (e.g. with password) might facilitate improved assurance of user authentication for data decryption.

Endpoint security (firewall & AV)

Incorporating a software-based firewall, AV and application control solution on company endpoints should be another basic step to reduce risk. However, this should be maintained with automatic updates to ensure the full effectiveness of the solution. This combined with application control mechanisms will prevent the execution of unauthorised applications or files on endpoints threatened by USB connected devices. Furthermore, some application control measures are capable of actively examining running processes for dangerous activity without having to rely on constant updates of the latest virus or malware signatures [14]. Therefore, these more advanced methods of system monitoring should be considered where budgets allow for them. Some third-party solutions that address application control directly are discussed later in this document.

Education & awareness

Organisations spend substantial amounts on technology in order to keep their infrastructure safe but sometimes forget to address the source of the problem. Employee education and awareness around the threats that USB devices pose is commonly overlooked. If employees were provided with education and awareness training around the dangers that endpoint connectivity poses and the repercussions of plugging in an infected USB, they would likely re-think and seriously consider policies that had been implemented. The goal of an organisation should be to change the overall culture around USB connectivity so that employees, for instance, would not use USB devices that they have found and would always follow procedures put in place. However, it appears that many organisations still lack efficient security awareness training, or where they do offer such training, there may be no mandate on users to participate [15].

To encourage this practice corporate spear phishing simulations can be introduced. This will provide a real-world scenario for employees without the risk of financial and reputational damage. USBs which have been added to an asset register prior to the exercise can be distributed and placed across company offices. Endpoints can then be monitored and connection attempts logged for employees who have plugged them in. Those that decide to hand them in can be presented with a reward as an incentive to continue to do the same in the future should a USB be found. Those that do not, may need training to further highlight the seriousness of the damage that rogue USBs can do. If re-offences occur then disciplinary warnings may be needed to ensure employees act on the training given.

To support educating users, insider risk needs to be considered for both accidental and intentional situations. This is why training is important, however, with those whose intentions are malicious this can increase the risk to the business. To reduce the chances of an employee inflicting damage to an organisation, prospective employees should be screened with background checks prior to undertaking their employment. If necessary, screening of employees could continue annually or where suspicions are raised.

Disabling USB for high assurance environments

It is important to recognise that USB may not be considered an option at all for some sectors, both public and private. For instance, in high assurance environments which handle highly sensitive and classified information such as government departments. Disabling USB support in the BIOS as well as enabling the BIOS password to prevent these settings from being altered will provide protection prior to implementing steps at the operating system (OS) level. Furthermore, locking in the boot priority sequence to the internal hard drive so that it only boots from the selected allowed drive will further harden this approach. Should these steps become compromised further provisioning may be required at the OS level. This can be achieved through modifying the registry so that USB devices will not be recognised when connected. Additionally, uninstalling USB device drivers on the specific OS will prevent USB from launching.

DLP

The risks can be reduced further where sensitive data is exchanged through USB using DLP techniques. DLP simply uses tools to track data and ensures it does not become lost or stolen.

DLP can achieve this by using the following methods:

- Scanning data in transit, in use and at rest.
- Identifying sensitive data that requires protection.
- Remedial actions – alert prompts, quarantines and encryption.
- Provide reporting for compliance, audits, forensics and incident response.

6.1 Malicious firmware prevention

Modified USB firmware escalates the risks of malicious devices because of a fundamental design flaw. It was never envisaged that USB could be abused and exploited in such ways. Therefore, most USB firmware can be replaced without any form of cryptographic signing, resulting in the acceptance of any firmware update the device is offered. However, there are measures that can be followed to mitigate this type of risk.

Firstly, some fundamental initiatives need to be taken by organisations to actively pursue USB vendors in order to build security by design into their devices in order to prevent unauthorised changing of USB drive firmware. This would be achieved in the form of cryptographic key verification to ensure the updates can only be done by approved vendors. However, this does present its own problems as code signing keys can be stolen, thus compromising the device.

Additionally, following best practice through updating and regularly patching in combination with the solutions previously highlighted may not stop the code on the USB's firmware from executing. However, it will reduce the chances of a compromise once the malware has been executed. One solution offered is known as IronKey and this protects against the BadUSB malware which attacks the device itself instead of the data on the device. As revealed at the Black Hat conference in 2016, BadUSB changes the firmware that controls the behaviour of the device turning it into a malicious piece of hardware.

The mitigation here works by digitally signing firmware updates. If the firmware is modified it cannot then authenticate the new firmware and the device will not work, preventing the infected USB from launching the attack. However, this does leave the device unusable but the following steps highlight how this problem is mitigated:

- Digitally signed controller firmware immunising the malicious firmware threat, preventing unverified firmware updates.
- Hardware-based security keys are used to protect the firmware update process, preventing prior firmware tampering which can lock the device.

Both of these measures are backed up with additional security features, some of which include secure AES-256 encryption, multi-factor authentication and built-in password protection policies.

Ultimately, the result of combining an effective usage policy that audits and monitors USB devices and associated endpoints with the solutions discussed provides an overall stronger management solution.

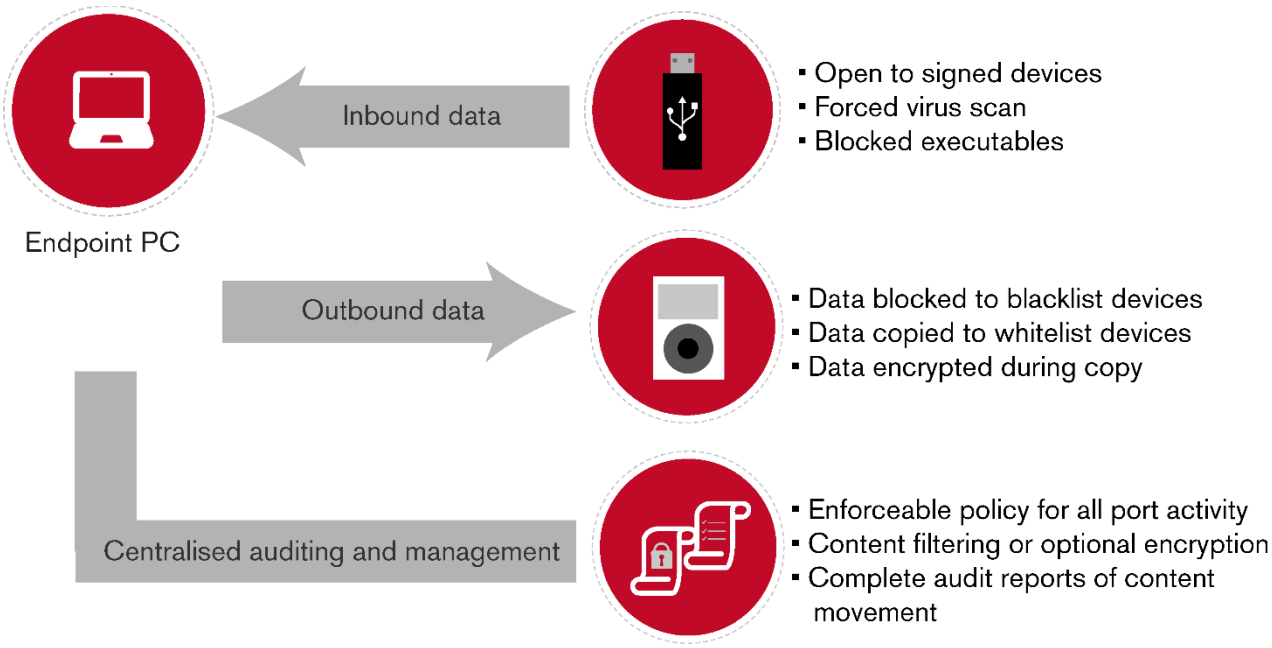

Figure 2. An example of endpoint management [16]

The illustration above highlights the overall goal. However, there should always be revisions to any solution and awareness around the potential issues that could still arise. For example relating to black and white-listing devices, these solutions are not always bullet-proof and might be bypassed by spoofing the ID of a device.

6.2 Third party software solutions (multiple operating system solutions)

Securing endpoints has evolved. Now, the more conventional methods need to evolve in order to continue the fight against sophisticated attacks. This is where Next Generation AV (NGAV) and Endpoint Detection and Response (EDR) play their part. NGAV is having the ability to be able to detect and prevent a threat without any prior knowledge. This is achieved primarily by using exploit prevention, machine learning and behavioural analysis.

However, individually these techniques are not sufficient and it is important to adopt all options available. For example, a NGAV solution that relies on machine learning is not effective against fileless malware that exploits software vulnerabilities using macros and memory-based attacks to expose the endpoint [17]. EDR on the other hand relies more on collecting data in relation to file and registry changes, network connections and various configuration alternations. This then allows the data collected to be used to detect an attack that does not use malware. This then becomes even more valuable as NGAV improves at detecting malicious programs.

Organisations should assess potential third party software solutions, in terms of the functionality that they offer, the platforms that they support versus the organisational policies and requirements, in order to understand the solutions that would best fit their requirements.

7. Conclusions

Endpoint connectivity is, for the most part, mandatory in order for an organisation to function. Connected devices such as printers and keyboards, or mass storage devices used to share information, are fundamental for maximising productivity. Furthermore, endpoints that need connected devices for them to be useable present an increased risk as foreign connected devices can contain malware which may result in data loss, therefore potentially leading to huge financial and reputational damages.

The below table provides a summary of the approaches an organisation can use to protect against the USB threat. It provides a practical overview of current technology solutions as well as the more obvious user education that can be used to help tackle the threats at all levels.

USB endpoint control	Control description	USB appetite
Disabling USB for high assurance environments	Designed for high assurance environments where USB is not an option. Disabling USB in the BIOS and setting a BIOS password will prevent any change to these settings. Locking in the boot priority and disabling/uninstalling USB drivers at the OS level provides a layered approach to locking down USB.	None
Encryption	Point-to-point encryption protects data when transferred between different devices and where removable media is used. This plays a role in DLP as data that is lost will now be somewhat protected.	Some
Endpoint security (firewall/AV)	Installing an established firewall and AV solution on an organisation's endpoints offers further control as to what can access an individual's host. This offers an additional layer of protection should any hardware firewall be bypassed. It is important to ensure updates are automated to protect against the latest known viruses.	Some
Education & awareness	Technology alone should not be the only mitigation to be considered. Staff training provides employees with a level of awareness when educated regarding risks associated with USB connectivity. Attack scenarios can be simulated to test employees to see if they are likely to open an email attachment or plug-in a rogue USB left scattered in the car park or office.	Some

Malicious firmware prevention	Protecting against the BadUSB threat is incredibly difficult as it attacks the firmware that controls the device. However, this can be prevented by digitally signing the firmware on the USB. This prevents unverified updates to the controller firmware and will render the device useless if unverified updates are attempted. Hardware-based security keys can also be used to protect the firmware update process preventing any prior firmware tampering.	Minimal
Third-party software solutions	Endpoint security software offers a well-rounded solution that tightly locks down and tracks data. This is offered through incorporating AV, patch automation and content tracking techniques. This may be preferred to a stand-alone firewall and AV solution but would likely be more costly. This stringent approach is ideal for organisations who are serious about protecting their data but want to continue to utilise their endpoints effectively.	Some

8. References & further reading

[1] Armasu, L. (2016, August 4). Spreading Malware Through Dropped USB Sticks Could Be Highly Effective, Research Finds. Retrieved from Tom's Hardware: http://www.tomshardware.co.uk/dropped-usb-sticks-spreads-malware,news-53590.html

[2] Grauer, Y. (2015, October 30). Should You Plug That USB Drive Into Your Computer? (Beware Of Malware). Retrieved from Forbes: https://www.forbes.com/sites/ygrauer/2015/10/30/usb-drive-malware-security-homeland-security-cybersecurity

[3] Hak5. (2017). USB Rubber Ducky Deluxe. Retrieved from HakShop by Hak5: https://hakshop.com/products/usb-rubber-ducky-deluxe

[4] Hak5. (2017). Lan Turtle. Retrieved from HakShop by Hak5: https://hakshop.com/products/lan-turtle

[5] Eckstein, C. (2015). Preventing data leakage: A risk based approach for The SANS Institute
.

[6] Privacy International. (2015, June). Two Years After Snowden. London. Retrieved from https://www.privacyinternational.org/sites/default/files/Two%20Years%20After%20Snowden_Final%20Report_EN.pdf

[7] IBM and Ponemon. (2016). 2016 Cost of Data Breach Study: Global Analysis

[8] Sophos. (2011, Decemeber 7). Lost USB keys have 66% chance of malware. Retrieved from naked security by Sophos: https://nakedsecurity.sophos.com/2011/12/07/lost-usb-keys-have-66-percent-chance-of-malware/

[9] Paganini, P. (2015, March). Retrieved from Security Affairs: http://securityaffairs.co/wordpress/34810/malware/microsoft-fix-flaw-stuxnet.html

[10] Cluley, G. (2014, August 1). Danger USB! Could a flash drive's firmware be hiding undetectable malware? Retrieved from Tripwire: https://www.tripwire.com/state-of-security/security-data-protection/danger-usb/

[11] Ducklin, P. (2014, October 6). BadUSB - Now With Do-It-Yourself Instructions. Retrieved from Naked Security: https://nakedsecurity.sophos.com/2014/10/06/badusb-now-with-do-it-yourself-instructions/

[12] Goodin, D. (2015, October 14). "USB Killer" flash drive can fry your computer's innards in seconds. Retrieved from ArsTechnica: https://arstechnica.com/security/2015/10/usb-killer-flash-drive-can-fry-your-computers-innards-in-seconds/

[13] Banks, N. (2015, August 24). Secure USB Best Practices Uncovered. Retrieved from Computer Business Review: http://www.cbronline.com/blogs/cbr-rolling-blog/secure-usb-best-practices-uncovered/

[14] Stormshield. (2017). Protect Your Terminals With Signatureless Solutions

[15] Paganini, P. (2015, May 31). An overview of the principal issues related to the 3 general categories that security controls fall under; physical, technical, and operational controls. Retrieved from Security Affairs: http://securityaffairs.co/wordpress/37368/security/operational-securit-user-education.html

[16] Check Point Security Technologies. (n.d). Preventing Data Leaks on USB Ports

8.1 Figure Table