Endpoint Protection

Authors: Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

A quick google search will reveal that it "is an approach to the protection of computer networks that are remotely bridged to client devices"[1]. To put it simply, it is the practice of ensuring that devices connected to your network are protected against malicious activity, which typically translates to deployment of malware and/or exploitation of exiting vulnerabilities.

1. Guiding principles

The business landscape has evolved significantly over the last few years, determined, of course, by the rapid development of new technologies. It is not uncommon in today's business to have people using laptops, smartphones or tablets – either from the office premises or from home or while on the road. Recently, with the wide adoption of IoT devices, the landscape has become even more complex, as these "gadgets" are included into the scenery – if not connected to your network, then at least connected to a device that is connected to your network (just to give a simple example, a smartwatch connected to the company provided phone of tablet). And this are just the new additions. While making use of these "feats of technology", we still have the traditional office network, with servers, network equipment, and end user computers. Not to mention perhaps old, deprecated devices that might still linger on the network due to some important tasks they might be performing.

As one can observe, the scene is complex and protecting it entails a fair amount of effort, creativity and, most probably, a decent budget (to put it mildly). While we cannot cover effort and specific designs, nor can we cover budgets, we will try to list some of the most used and known endpoint protection solutions out there.

Given the complex nature of the environment and the shift towards mobility, it is required that we introduce several concepts at this point:

- Defense in depth
- Zero Trust Model

[1] https://en.wikipedia.org/wiki/Endpoint_security

1.1. Defense in depth

Defense in depth principle refers, in a nutshell, to the practice of ensuring the security of a network/asset through the deployment of multiple independent controls, the logic behind it being that if one control fails, the next one will continue to protect the asset(s). It is a wide known principle and typically should be considered in all security aspects.

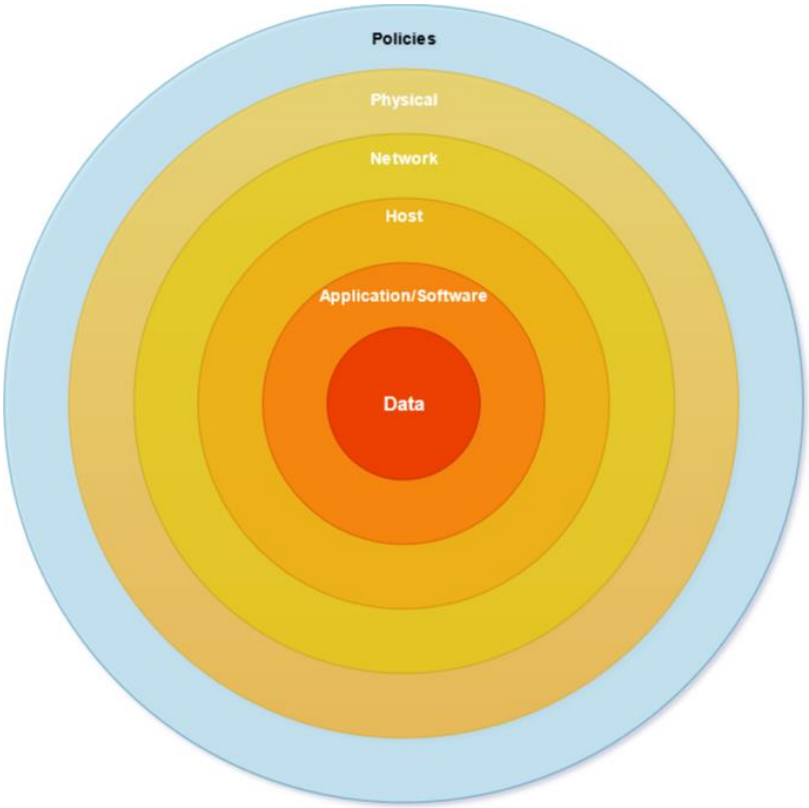

Fig.1 – Defense in Depth principle

1.2. Zero Trust Model

"Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything *inside* or *outside* its perimeters and instead must verify anything and everything trying to connect to its systems before granting access."[2]. The concept is rather a new one and differs significantly from the traditional approach studied for decades in which

[2] https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

you had a network and whatever was outside was malicious while the inside was to be protected. At a high level, of course. You would still have the various internal network areas with varying degrees of security requirements, but overall, that was the idea. You would have the outside zone, the DMZ and the inside network. The Zero Trust Model entails that you trust nothing and verify everything, including internal or own resources. That's the mantra. And it is rapidly gaining popularity due to the complex nature of the present-day business landscape we've just described in our introduction in terms of technology deployed.

Vendors and organizations have their own proposals and architectures for zero trust implementations. Some of the common aspects to all implementations, and that should be considered are:

- Authenticating the user
- Authenticating the host
- Definition and enforcement of access control policies for subjects, objects and data
- Enterprise Public Key Infrastructure – for managing digital certificates issues by the organization to subjects, objects, services and applications which typically are used to authenticate them and grant access to resources
- Identity Management system – creating and managing user accounts.
- Diagnostics and mitigation systems – gathering information about the assets and applying updates to configuration and software components[3]

One thing to note here is that regardless if you go for the traditional models or the zero-trust model, the defense in depth principle should still be considered and applied.

2. Endpoint Protection Strategies

Now that we have covered some of the main principles and protection strategies (and overall differences between them), we'll take a more closed look at the actual endpoint protection strategies available. These can be used independently, in any number of combinations and, why not, in whole, depending on budget.

2.1. Active Directory Policies

Although you might not find these in many of the lists, we consider that starting with the basics is the way to go. Any discussion regarding nextGen AV, SIEMs, DLP and others is

[3] NIST Special Publication 800-207 – Zero Trust Architecture - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

useless if we don't get the basics right. Especially if mobile computing is a part of your day-to-day business life. Active Directory group policies are a good starting point to ensure basic security such as user access and rights management (considering you do not employ a more complex access management solution). Besides this, there are some good basic protection strategies that every business should make use of. Just to name a few of the most well-known ones:

- Password policy (complexity, history)
- Failed logins allowed
- Local Admin account disable
- Audit policies enabled (account management, object access, logon/logoff, system, etc.)
- Restrict access to local resources such as registry editor, configurations, etc.
- Enforce multi factor authentication – at least for admin accounts
- Lockdown service accounts or disable unused ones
- Disable SMB, if possible – or at least SMBv1
- Restrict USB/IO port access

For a more comprehensive security stance, using security benchmarks is a good starting point for defining your AD security policies. Security benchmarks are created by independent organizations, well known in the industry. These represent recommendations or best practices of how different operating systems or software should be configured. Some of the recommendations made in the benchmarks may be conflicting with your needs in terms of functionality. However, consulting them is a good way to ensure a starting point in securing your environment. You can, of course, tailor the recommended profiles to your needs. And, as always, document the deviations for future reference.

2.2. Multi Factor Authentication

Multi Factor Authentication (MFA) has already been mentioned in chapter 2.1 above. With that in mind, we believe this should have its own chapter as well. With the wide adoption of cloud technologies and remote work, MFA should be considered for a company-wide implementation, rather than ensuring such practices only for admin accounts.

Gone are the days in which the workforce needed to come into the office to have access to resources. Nowadays, most of them are just a click away from accessing internal resources, sometimes even confidential data that resides in the company cloud instance. Attacks targeting the cloud environment, such as brute force attacks or password spray attacks are a regular thing. This setup, combined with perhaps not so secure user passwords may lead to unauthorized

access to resources such as email or collaboration spaces such as sharepoint online or, even worse, to malware attacks and compromise.

The principle for multi factor authentication is simple: the users must pass multiple authentication steps in order to gain access to resources. It is important to note that two passwords are not considered a form of multi factor authentication. For the purpose of completeness, let's review some forms of authentication and what they entail:

- One factor: something you know – typically a password
- Two-factor: something you know + something you have – a password and a token, access card, etc.
- Three-factor: something you know + something you have + something you are – a password + a token/access card + biometric verification (retina scan, fingerprint, palm scan, face recognition)

Probably the most widespread MFA form is the two-factor authentication. This is usually employed through the use of a password in combination with some kind of token that will generate an additional access code to use in conjunction with your password (usually requires input or validation of a code after the password has been provided). Tokens may be hardware tokens or software tokens. In recent years, software tokens have been used more and more due to their practicality – they may be installed on your smartphone, without the need to carry around a hardware token. Authentication software such as Google or Microsoft Authenticator are widespread in usage. For company-wide implementation, covering all users, these are some of the solutions that may be considered for implementation.

2.3. Antivirus

Next point on the list is, of course, the antivirus. Not the home use or "free" type, definitely. Organizations of all sizes should consider deploying enterprise level antivirus solutions. They offer central management capabilities and definitely will ease administration tasks. Antivirus solutions are software designed to detect and remove malware such as viruses, trojans, worms, rootkits, keyloggers etc. Traditional antivirus solutions typically employ signatures as detection mechanisms. Although these solutions may protect against a wide array of malware, they are not bullet-proof. They may be less effective against polymorphic or armored viruses which are designed to encrypt parts of themselves, create differing copies of themselves or, as in the case of the latter, deploying various methods to avoid detection.

For this purpose, in recent years the shift has been towards nextGen AV solutions which are rather signature-less. "Numerous approaches to address these new forms of threats have appeared, including behavioral detection, artificial intelligence, machine learning, and cloud-

based file detonation."[4]. The afore-mentioned are some of the newer techniques employed to detect malicious software and, potentially, even zero-day attacks.

To note that with the growing complexity and number of threats, new security solutions have been developed in the endpoint security space. It is worth going through each of them to define them and understand their use.

EPP – Endpoint Protection Platform

Endpoint Protection Platforms have the role of preventing endpoints from threats such as malware, zero-days, etc. EPPs are typically the antivirus solutions we've just covered.

EDR – Endpoint Detection and Response

EDR solutions come into play when an incident has occurred. While EPPs are rather more…passive if you will, EDR tools are designed to help analysts respond to incidents. They will help analysts during response activities to identify IoCs, provide real time alerts, etc. They also have the ability to trigger automated responses such as host isolation or reimaging or manual responses.

To note that modern EPP solutions nowadays typically contain an EDR solution as well.

XDR – Extended Detection and Response

XDR is a term that was coined rather recently and defines complex platforms that have the ability to ingest and correlate log data from various sources such as servers, network equipment, and various security solutions including EEPs and EDRs and endpoints. The goal is to provide a unified view of the security stance of your environment. "Gartner defines XDR as *"a SaaS-based, vendor-specific, security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components."* Improved protection, detection capabilities, productivity, and lower ownership costs are the primary advantages of XDR."[5]

[4] https://en.wikipedia.org/wiki/Antivirus_software
[5] https://en.wikipedia.org/wiki/Extended_detection_and_response

2.4. DLP – Data Loss Prevention

Data loss prevention solutions are another option to protect your endpoints. This time it is not to protect against an infection, but rather to prevent potential data breaches or data exfiltration attempts. DLP solutions have several characteristics

- Ability to label data based on predefined classification levels
- Data discovery
- Ability to scan outgoing traffic (network, email)
- Block potential data exfiltration attempts based on defined policies

Enterprise level DLP solutions are typically deployed on hosts in the form of an agent that monitors endpoint traffic.

2.5. Encryption

Another important aspect of endpoint security is encryption – specifically disk encryption. Usually employed through the use of native applications such as Bitlocker on Windows systems or dedicated software specifically built for this purpose by various vendors. To note that disk encryption will not protect against malware or other software-based attacks – it rather mitigates the risk of device loss by blocking access to the data stored on it.

2.6. Mobile Device Management

Mobile Device Management solutions, MDM for short, should not miss from any organization's arsenal if they make use of significant numbers of mobile devices (smartphones, tablets or laptops). These are usually special-purpose built software created for such tasks. Some of the most encountered MDM characteristics are as follows:

- Ensure a configuration standard for all devices
- Managing updates for devices, applications, and applied policies
- Monitoring and tracking of equipment
- Remote troubleshooting and administration in a consistent manner

2.7. Vulnerability Management & Patch Management

Last, but not least, a sound vulnerability management and patch management program is a must have for all organization. Vulnerability management is the continuous work of

identification, classification and remediation of known software vulnerabilities. The program should cover all assets under your management, regardless whether they are located in a data center or devices being used by your mobile workforce.

To note that some vulnerability management solutions nowadays also have the ability to scan your endpoints not only for known vulnerabilities, but also for configuration flaws. This may be achieved by using benchmarks and special built scanning profiles based on those benchmarks to identify deviations from the standard (remember, we have mentioned the use of benchmarks is the beginning, when talking about security configurations).

Vulnerability management and patch management programs, at the very least, should consider:

- Including all assets in scanning
- Define regular vulnerability scans and reporting on findings
- Regular application of security patches and software updates
- Applying security patches or updates based on the risk level to your organization. While all vulnerability scanners will provide a rating for the vulnerabilities they have found, an assessment that takes into account the environment and network configuration is needed to ensure that the most relevant updates are applied first. For example, an internal assessment might determine that a vulnerability that was marked as “high” by the scanners is actually of medium priority, based on the specific environment, while a “medium” marked vulnerability might take precedence as it has been determined by your internal assessment that it is of critical importance

3. Closing thoughts

There is a variety of solutions out there that will help protect endpoints in an organization. We’ve just covered a few of the most important ones. However, we want to underline that there is no bulletproof solution and none of the ones we have discussed, nor many others, will ensure security by itself. As we’ve already noted, defense in depth is an absolute guiding principle in all aspects security related and deploying as many of these as possible and covering as many layers as possible will ensure a more robust security stance.