Indian journal of
Engineering

To Cite:
Siji FG, Uche OP. An improved model for comparing different endpoint detection and response tools for mitigating insider threat. *Indian Journal of Engineering*, 2023, 20, e22ije1651
doi: https://doi.org/10.54905/disssi/v20i53/e22ije1651

Author Affiliation:
[1]Computer Engineering Department, Abia State University, Uturu, Abia State, Nigeria
Email: fagbhume.griffn@abiastateuniversity.edu.ng
[2]Electrical and Electronic Engineering Department, Enugu State University of Science and Technology, Enugu State, Nigeria

Peer-Review History
Received: 02 May 2023
Reviewed & Revised: 06/May/2023 to 07/June/2023
Accepted: 10 June 2023
Published: 12 June 2023

Peer-Review Model
External peer-review was done through double-blind method.

Indian Journal of Engineering
pISSN 2319–7757; eISSN 2319–7765

DISCOVERY
SCIENTIFIC SOCIETY

An improved model for comparing different endpoint detection and response tools for mitigating insider threat

Fagbohunmi Grifin Siji[1], **Okafor Patrick Uche**[2]

ABSTRACT

In recent times there has been an increase in the incidences of leakage of confidential data in various organizations. These organizations have also come to the realization that most of this leakage and data breach is as a result of infiltration on endpoint devices used by their employees. From available data it has been shown that staff training aimed at promoting awareness on the protection of confidential data of the organization has not helped in mitigating these breaches. The involvement of third-party cloud services has not helped either; this is because such third party keeps important and confidential files of the organization so as to help protect their data from their remote location. This situation has led to the emergence of many software products which provide protection for endpoint devices. The aim of this paper is to discuss some of the current methodologies used in current endpoint protection platform as well as endpoint detection and response with a view to throw more light into factors that differentiate traditional negative endpoint protection from positive endpoint protection. The paper will from this analysis design a mathematical model that can be used for effective comparisons of the methods used for Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR). The model will highlight the strengths and weaknesses of different EPP and EDR protocols with a view to knowing the characteristics of models best suited for different application scenarios. The overall goal of the paper is to assist small, medium and large-scale organizations in identifying the characteristics of this Endpoint protection protocol that is ideal for their organization's operations. The results and analysis provided in this paper will assist various companies in the selection of endpoint protection platform best suited for their organizations. Finally, the paper aims at providing more research inputs in the area of endpoint security with the view to predicting future state of this all-important area of interest.

Keywords: Endpoint protection, Endpoint detection and response, Endpoint protection platform, Data leakage, Privacy, Insider threat.

1. INTRODUCTION

Endpoint protection or security is defined as a way of protecting computer networks that are linked remotely to client devices (Xiangyu et al., 2020). Endpoint devices are electronic devices such as mobile phones, laptops and tablets. These devices are sometimes connected to a company's internet network and they usually serve as weak links to hackers in compromising the company's network (Le et al., 2020).

For this reason, endpoint security has become a very important research topic in cyber security required for preventing various threats to a company's network. It should be recognized that a phishing link in an email can enable hackers get access to company secrets which could also lead to a compromise of the cloud services employed by the organization in protecting their network. Similarly, the activity of a third-party cloud service can also act as a weak link to hackers. It is with this in view that organizations must take proactive measures in ensuring endpoint security through the use of various available products for the protection, detection and response to the growing online threats.

There are different approaches to preventing endpoint devices from being compromised. One approach is the centralized management of multiple security function commonly referred to as all-in-one solution (Sun et al., 2018), while the other more expensive approach is the use of specialized software products or specific case scenarios. Due to the fact that many medium and small-scale companies cannot afford the specialized products, it has led many companies to look for all-in-one software that can guarantee the protection, detection and appropriate response to the company's network.

This approach though cheap and simple may not guarantee outright success for the different categories of endpoint devices connected to a company's network, for this reason IT decision makers has realized the need for higher investment in a holistic approach to endpoint security. It should be realized that by a survey on Endpoint security done by AT & T research firm in Nigeria in 2021, the need for higher budget in an advanced malware protection and prevention software was uppermost in most companies.

According to the same report, the highest proportion of threat (i.e., 29%) causing damage to the company's network was the insider threat (Insider threat is defined as a means through which hackers compromise the integrity of a company's network through endpoint devices used by members of staff of the organization). Also, among the company where the survey was carried out, 55% of them attested to the fact that their facility had been attacked by the insider threat within the past three months of the survey (Xiangyu et al., 2017).

It should be realized here that insider threat constitutes a major attraction for hackers because this category of threats are difficult to detect. The incentive of this type of attack is not only because they are difficult to detect, but can also be undetected by firewalls embedded in a security network. For this reasons hacker normally target vulnerable endpoints within an organization to breach their operations. Some noteworthy examples of companies that have been hacked this way include Sony, Facebook, LinkedIn and a host of others.

This paper will highlight two major ways used in protecting endpoints from security breaches; this includes the endpoint protection platform (EPP) and endpoint detection and response (EDR). EPP comprises of various security tools such as antivirus, anti-malware, personal firewalls, data encryption and intrusion detection and prevention, EDR on the other hand is embedded with functions that can detect and act on threats in a system without any interference to the system's network architecture. This makes EDR a very attractive option for detecting and responding to insider threat.

The remainder of this paper is organized as follows: Section II highlights related works on insider threats. Section III presents the main attributes of endpoint protection platform. Section IV highlights the limitations of endpoint protection platform. Section V discusses endpoint detection and response platforms and their limitations, while section VI provides a model for comparing endpoint protection platform and endpoint detection and response. This was achieved using the information obtained from AT & T research firm in Nigeria. Finally, section VI concludes the paper and provides future direction in endpoint security.

Related work

It should be recognized that insider threat had been a source of much worry in recent times in the field of cybersecurity world-wide, and Nigeria is not an exception. There has been a plethora of research works done on insider threat in which various models and architecture of detecting and responding to this class of attack has been proposed. New algorithms have been recently proposed drawing attention to new class of risks in endpoint security. Zhang, (2018), presents a framework in which different modules based on algorithms and functional techniques were used for detecting insider threats.

Le et al., (2018) an algorithm called GP was also used to achieve the function defined in Zhang, (2018). In Sun et al., (2017) a mathematical function was defined which was assumed to assist authorized administrators to manage and detect insider threats. Claycomb and Shin, (2016), designed a system-based directory virtualization techniques that could help detect insider threats. In recent times machine learning has been adopted in detecting insider threats for instance in Rashid et al., (2018), a machine learning based detection for insider threats was analysed.

Voris et al., (2015) employed a technique referred to as user behaviour analytics to design a software architecture that can be used to explain the behaviour of several insider threats with a view to detecting them. Brancik and Ghinita, (2011), developed a decoy file that could be used to attract and trap insider threats. Sanzgiri and Dasgupta, (2016) and Bertino and Ghinita, (2011), discussed various types of detection tools that can be used for identifying insider attacks. Liao et al., (2013), describes how insider threats mutate to compromise database system as well as proffering ways to mitigate their effects at an early stage to disrupt the mutation.

In most of the different research works cited in this paper, their focus was mainly on the design on new algorithms to detect and mitigate the effects of insider threats. It is however worthy of note that research papers Zhang, (2018), Le et al., (2018), Sun et al., (2017), Rashid et al., (2018) and Voris et al., (2015) deals with sophisticated and dedicated protection software which may be beyond the budget of small and medium scale industries. In research papers Claycomb and Shin, (2016) and Brancik and Ghinita, (2011) proposal was made on practical techniques needed to mitigate insider threat, however the areas of application best suited for these designs were not outlined. These techniques cannot capture most of recent insider threat and hence need to be improved upon.

In the survey papers presented in Sanzgiri and Dasgupta, (2016), Bertino and Ghinita, (2011) and Liao et al., (2013), their works are similar to the design proposed in this paper. In Sanzgiri and Dasgupta, (2016) a discussion of the various types of insider threat was provided, however no solution to the various categories of insider threat was provided. In the work of Bertino and Ghinita, (2011) and Liao et al., (2013), a description of some tools used in mitigating the effects of insider threats was provided, however their performance was not compared to any existing tools, so their relative advantage cannot be validated.

The aim of this paper is to address the highlighted shortcomings stated herein by designing a model that can be used in comparing various categories of endpoint protection platforms. Detailed information on the various types of threat detection and response techniques is provided in this paper. The purpose here is to help classify the different categories o endpoint protection schemes with the view of identifying their areas of strength and weaknesses.

Secondly a comparison has been made between EPP and EDR through careful analysis of their features and this was used to develop our own model for characterizing the different endpoint protection platforms together with the endpoint detection and response software. The model proposed in this paper was used to obtain the equation of the efficiency ratio of any EDR and EPP software to a given insider attack. MATLAB simulation software was used to plot graphs used in visualising the rate of change of efficiency with different determining factors.

2. DESCRIPTION OF ENDPOINT PROTECTION PLATFORM

An endpoint protection platform can be described as a signature based negative endpoint protection software. The name is derived from the fact that it attempts to match the signature of the data with that of the signatures of threats stored in its database. A negative match signifies that the data is threat free. EPP comprises of array of software tools and technology aimed at protecting endpoint devices from insider threats. The series of steps used in realizing this is in (Figure 1).

As in Figure 1, when a threat successfully penetrates the firewall, the Host Intrusion Detection System (HIDS) determines the nature of the threat by returning the response that it is either malicious or not from the threat software routine. If the threat is malicious, it will be mitigated by the HIPS otherwise it will be unaffected. The sub-section that follows describes the features of EPP.

Detection

Detection in terms of computer security can be defined as the ability of software to identify a threat or file that is capable of compromising the activity of the computer system. A good endpoint protection platform (EPP) must be able to identify insider threat. An EPP detects threats by comparing a given file string with the virus signature contained in its database. The database contains the signature of large quantity of virus, thereby the matching of these known signature with that of the file string is performed using different algorithms available in the market.

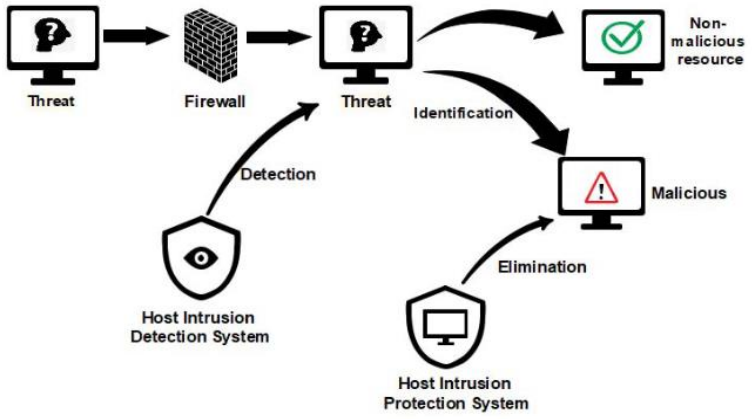

Figure 1 Procedure on threat detection by EPP

EPP is a combination of various software, most of this software employ the technique of intrusion detection to identify possible threats in the system. This is done by using the intrusion routine function in EPP to analyse a given file string for signs of intrusion (Xiangyu et al., 2017). It should be noted here that signature-based detection represents just one of the methods used in identifying insider threat, though it is also the most common technique. The Host Intrusion Detection System (HIDS) monitor endpoint devices and regularly store the characteristics of hosts with untrusted information together with servers suspected to run suspicious activities.

Protection for Infected system

Even though threat detection is very essential for the protection of endpoint devices, it is not a fool-proof guarantee against insider threat. This is because hackers come up with different strategy which may likely be undetected by the EPP. This is due to the fact that new insider threats are produced on a daily basis, with new threats capable of circumventing the protection procedure (signature) embedded in EPP. It is therefore expedient for organizations to cut out any attempt of external invasion arising from insider threat by taking proactive action that can detect threat characteristics so as to mitigate being compromised by new emerging threats.

Protection here is aimed at eliminating insider threats that has been able to break or circumvent the protection facility provided in EPP. It should be noted that absence of the protection procedure could lead to a very catastrophic situation for an organization in the event of the EPP not being able to detect the threat. In order words the protection procedure is a solution for errors from the EPP. Different algorithms are proposed by the EPP for Host Intrusion Protection System (HIPS) implementation. HIDS and HIPS normally work together. HIPS normally mitigate against threat that cannot be identified by HIDS, in other words no threat should normally be able to escape the two procedure functions (Strom, 2019).

Blacklist and the Whitelist procedure

The function of this procedure is to stop any file or software whose characteristics/signature is already known and stored in the database of EPP. The effects here are to enhance the throughput of the system as a blacklist file/software need not be fed into the detection procedure of the EPP. Similarly, the whitelist procedure marks a file/software as safe and also without the need to be fed into the detection procedure of the EPP; these two procedures enhance the productivity of the detection platform.

Demerits of Endpoint Protection Platform

As stated, earlier EPP may not be able to detect all insider threats due to the fact that the signature in the EPP's database may be unable to match the threat, note that hackers devise means to circumvent the signature on a daily basis. Secondly the number of virus signatures in the database of the EPP is so enormous that a lot of time may be wasted before detecting a threat/virus thereby reducing drastically the throughput of the system and more importantly the effective working hours of the organization. The reduction of system throughput is even made worse by the fact that insider threats are capable of mutating very fast. Other demerits of the EPP are enumerated below:

Threat Detection Involves Over-Burdening Resources

The number of matching signatures in the EPP database is quite enormous. This means that a lot of time may be needed before a match is found. This translates to high memory and high fast computation requirement for the processor. All this will add additional burden to the already existing network structure in the organization. Although cloud scan has been proffered as a solution to this, in this case in the organization a procedure in the EPP will call the database of signatures from the cloud. This has the purpose of taking the burden of storage resources off the organization's system, however it has been noticed that the running efficiency of an organization's system when connected onto cloud services reduces considerably when being attacked.

Increase in File-less Attacks

Nowadays hackers are developing new virus using a concept in object-oriented programming known as inheritance. In this way a virus has properties of an existing virus but with an added functionality of adding unique features of its own. This technique is referred to as file-less attack because the known virus file signature is moderated with new characteristics. The idea here is that the added file characteristics prevents such virus from being detected because it is hidden in the definition of an inherited child class virus definition. This phenomenon is now on the rise due to the nearly automated virus construction kits on the internet.

In 2021, a security risk report in Nigeria by Secure Systems Organization gave the rate of organization infected with file-less attack at 56%. The report also indicated that the success rate of file-less attacks on organization's facility in Nigeria was five times to those based on file-based attacks. This is enough reason to make critical research in this field. File-less attacks are currently on the increase, they took advantage of a fundamental flaw (using the concept of inheritance as explained earlier) in the traditional endpoint security and current EPPs are not able to mitigate them.

Most Insider Threat Mitigating Software Makes use of the Internet

It should be realized that most of the software solutions to insider threat requires the internet in order to remove most of the burden of using the network resources in the companies. As explained earlier the memory requirement that enables the scanning of up-to-date signatures will use up most of the resources in a company's network thereby resulting in less throughput. In order to overcome this problem, scientists have turned to cloud computing to address this shortcoming. However, another problem of cloud computing is that many of company's sensitive data may be exposed to a third-tier company as the network system will be connected to the cloud service most of the times. This is in clear violation to the data loss prevention requirement of the EPP (Chandel et al., 2021).

This however happens to be the only way a company's network can be isolated from the heavy burden of the resource consumption while at the same time being up to date with latest signature updates, security patches and latest information concerning threats. There are also cases in which an infected endpoint may connect to a company's network to infect other systems. This can however be prevented by installing a protection routine in the network that scans every new endpoint before including them on the network

Insider threats are more dangerous than external threats

In this subsection the major causes of data leaks will be explained while proposing means of mitigating them. It has been revealed that there are two major causes of data leaks. These are accidental exposure and malicious exposure (Asher-Dothan, 2017).

Accidental exposure is defined as a scenario when a company's employee endpoint is not properly protected from the Internet. In this way such worker may download file from an infected website or hackers may deny access to some of the employee documents (denial of service attack) because they have been able to compromise such employee's password. It can be realized from here that most insider threat involves mostly the employees of the company that makes themselves susceptible to the activities of hackers. In order to mitigate such effects a company must make sure that all potential endpoint to its network is well protected by including them on the systems connected to the cloud infrastructure and a routine is included to make sure that password used by employees are strong and encrypted so that it will be near to impossible for hackers to decode.

Malicious exposure on the other hand is a scenario when hackers deliberately attempt to compromise a company's network. It could be from a competing company or from a staff just recently laid off from the company. This can easily be mitigated by regular update on the company's protection platform.

From the works of Asher-Dothan, (2017), it was shown that there has been a surge of insider threats in the industries. This can be attributed to increase in out-of-job graduates who master the act of hacking, knowing that the successful hacking can bring in a lot of financial gain. These hackers can deliberately compromise sensitive data such as financial information and operational data

by taking advantage of the naivety of endpoint users. Leakage of such sensitive data can cause a huge financial loss to an establishment. It should be realized that hackers develop inside threats with no previous signature so as to escape being detected by both the HIDS and HIPS facilities of EPP. However, EDR can be used to protect against this sort of threats.

3. USING EDR TO MITIGATE MOST THREATS THAT COMPROMISE EPP

It should be realized as stated earlier that traditional antivirus procedures cannot be adequate in detecting most of the insider threats being witnessed nowadays. This has led to the development of new proactive methods by human security experts (Samuel, 2021). In this way computer security experts have come up with Endpoint Detection and Response (EDR) platform.

The advantage of EDR over EPP is the inclusion of threat intelligence in its knowledge base. This is artificial intelligence software used to detect anomaly in the behaviour of a file which is then used to alert the remediation procedure of the EDR. In this way threat intelligence is used to gather information in a file which is contrary to the normal expected behaviour using machine learning techniques. This anomaly is then reported to the remediation procedure of the EDR. The features of EDR as given in the next subsection.

Threat intelligence

This can be defined as a means of organizing, analysing and producing refined information about potential or current attacks capable of compromising a company's network (Arcticwolf, 2019). It should be realized here that this procedure uses machine learning to train its inputs on the characteristics of expected future threats and the ability to protect the network system from them.

In this way threat intelligence is able to protect a network system from being infected rather than using antivirus of signature to mitigate threats. The threat intelligent feature in EDR enables it to act as surveillance software to guard company's software against potential as well as current insider threats. The information gathered about the abnormal behaviour of any given file will be stored in the software's database to act a deterrent to future threats.

Continuous Monitoring

This is a control mechanism used in detecting the abnormal behaviour of an endpoint attached to a company's network infrastructure. This is achieved by constantly and randomly checking all endpoints for abnormal activity and thereby isolating them from the network. The period of these checking is determined by timers included in the software using stochastic programming.

This software can also provide protection for the network servers by using a sophisticated behaviour-based routine. This implies that all activities at the lower levels of the system and that of the CPU are made visible to the EDR. The CPU-level visibility is necessary so as to block malware that may want to compromise the CPU's memory and alter its contents (AV-TEST, 2021). This tool also mitigates the chances of the virus mutating to other parts of the network (AV-C, 2020).

Remediation

This is the ability of EDR to remove all residues of advanced malware that may escape detection of the EDR monitoring system. This procedure enables all part of the internal company's network to be scanned for any residues of virus. The procedure is also capable of repairing any damage caused insider threat.

Observe Network without interfering

This is the ability of EDR to only be installed in the kernel of the network infrastructure with its endpoint detecting routine rather than on all endpoints attached to it. Now the endpoint detection routine of the EDR is capable of scanning all the endpoints attached to the company's network. This removes the burden on all endpoints as the inclusion of this software will increase the memory requirements of endpoints thereby reducing their throughput or completely incapacitating them.

Use of Machine Learning for Threat's Detection

Machine learning is a branch of artificial intelligence which enables computers to learn using statistical inference. Learning here can either be through supervised learning in which the samples of input and output vectors are known in advance while the combination of input neurons of an artificial neural network and the activation function will enable the network to compare its outputs given specific input. The weights on each input neuron will then be twerked until the error between the samples and those from the neural network has been reduced to a minimum value.

Learning can also be through unsupervised learning where only the inputs will be known in advance. The experience from previous neural network models will now enable an output to be developed using a comparison with known samples identical to input neurons. EDR employs machine learning technique to learn the behaviour of threats so as to characterize the possible classification of file behaviour to be identified as threats. The learning capability of EDR is a very important tool that makes it so important in analysing and detecting current and future insider threats. This is also its major advantage over EPP.

EDR has also found application in deep learning as a sophisticated analytical tool for high level classification using artificial neural network models. This extension has helped in better understanding of the characteristics and prediction of malware and insider threats. The application of deep learning enables EDR to block threats from unknown applications with very high precision (AV-TEST, 2021). The ability of EDR to learn the various scenarios in which insider threat can be identified will go a long way in mitigating the snowballing effect of threat mutation. This has also been the attraction of industries to the use of EDR over EPP platforms. There has been a lot of attention among endpoint protection specialists in the development of advanced algorithms to tackle yet to be identified threats.

EDR Can Fit into any Budget and Scenario

A good feature of EDR is its ability to be customizable to the needs of any given establishment. This becomes important considering the different sizes and network topologies of many companies. This feat is made possible through machine learning. It must be emphasized here that the application of machine learning in endpoint protection cannot be over-emphasised. Machine learning is required for reducing to minimum the occurrence of false positives and developing algorithms to detect threats in whatever guise. This has been made possible through the use of deep learning techniques that can analyse many features that characterize insider threats.

The use of deep learning can also be used in the development of protection models most suited for any organization by analysing the software profile of such organization. It should be emphasised that though EDR has a lot of advantages to EPP due to the machine learning developed for its deployment, however some knotty issues still remain like false positives and the need for highly trained users for its management. The second reason adduced here may still make the adoption of EDR beyond the capability of most organizations. This has led to the development of many algorithms to reduce the instance of false-positives in endpoint protection to reduce the negative impact of needing highly skilled staff.

Most EDR software still falls short of the requirements in minimizing the amount of false-positives. It should be noted in most instances that the more specialized an EDR software is, the higher the possibility of having high rate of false-positives and the compulsory need for highly trained staff in cyber security. This has forced many industries to make a trade-off between highly specialized EDR software and those that minimize false-positives (Apostolopoulos et al., 2021) in order to meet their budget.

Table 1 EPP and EDR comparison

	EPP	EDR
Basic Features	Unifying the various passive functions	Ability to detect and mitigate threats
Functions	Knowledgebase of virus signature	Function of threat intelligence
		Dynamically supervise endpoints
	HID and HIPS	Resolve the damage resulting from virus
		Contains functions for detecting virus in its system's kernel
	Blacklist and Whitelist	It applies machine learning technique in detecting threats
		Can be customized
Limitations	Many resources required for detecting machine signature	Increase in the frequency of false positive will reduce the efficiency of software
	Virus signature no longer sufficient to identify virus	Needs highly trained professionals
	Unable to mitigate insider threats	
	Most functions require the use of cloud computing	

4. EPP AND EDR COMPARISON

As said earlier the aim of this paper is to propose a model that can be used to determine or measure the effectiveness of an endpoint security platform. For this, a separate model for EPP and EDR platform will be proposed. The need for the development of EPP model is borne out of the need that some companies may not be able to afford EDR software due to its specialisation and cost of deployment. Hence the paper attempts to develop a model that will fit into the budget of any size of organization.

A model for EPP

As stated, earlier EPP is a passive protection software which uses the matching of signature stored in its database to determine if a file is a virus or not. Its disadvantages were outlined in section II. This will be restated here for clearer presentation.

The efficiency of the system is reduced due to the memory requirement needed for the storage of multitude of signatures and the computational complexity involved in their comparison.

Detection based on signature can lead to an increase in flagging false-positives. This is corroborated by the findings of an endpoint security firm in Nigeria which states that the average efficiency of a company's network infrastructure can be reduced by as much as 15% through the use of EPP (Brogi and Tong, 2016). From the findings of the AT & T research firm in Nigeria, it was obtained that the average protection rate of EPP was 99.1%, while the average false-positive rate was $\frac{9}{2000}$.

Using the data presented here, it can be realized that EPP can operate in two states:

Protect: Here EPP can successfully detect and report threat

Unprotect: Here EPP cannot detect threat which makes the system vulnerable to attack.

The protect state can also be classified into two groups.

Correctly detected: Here the EPP correctly identify the threat so as to be isolated

Incorrect detection: Here the EPP incorrectly flags a normal file as a virus

In this model, the rate at which the EPP enters the protect state will be denoted by W. From the analysis provided earlier by the AT & T research firm in Nigeria W was given as 99.1% (33). With this, the formula to represent W will be given by equation 1

$$W = \left\{ protect(99.1) \left\{ \begin{matrix} correct\ report\ \frac{1991}{2000} \\ incorrect\ report\ \frac{9}{2000} \end{matrix} \right\} \right\} \qquad (1)$$

Compromise (0.09)

It should be noted that the performance of the company's computer will be analysed here. In order to take the holistic idea of the computer's performance, the following parameters will be included in the model

x denotes the loss of productivity in the company's system. This loss is as a result of the company being connected to the third-tier company's cloud in order to scan the endpoints of virus.

y_0 denotes the efficiency of the company's system without the EPP software

y_1 denotes the time required to identify the threat

y_2 denotes the time needed to isolate the threat

y_3 denotes the company's working hours

y_4 denotes the time required to reverse incorrect report

A nine-hour per day working system will be used in this model to reflect company's working hour rate mostly used in Nigeria. With this in mind the formula for correct report is given by equation 2.

$$CR = 11.1\%\ y_0 y_3 \qquad (2)$$

Now factoring in the two states of EPP as stated earlier in the section in the model and combining with equation 1, the probability of correct report is as in equation 3.

$$CR = 99.1\ X\ \frac{1991}{2000} \qquad (3)$$

Now from here, the rate at which the system will show incorrect report is as in equation 4.

$$IR = 11.1\% y_0 (y_3 - (y_1 + y_2 + y_4)) \qquad (4)$$

It should be noted here that y_1, y_2 and y_4 represents the total time required to recover the system from incorrect report. This includes the time needed to detect the threat, isolate and thereafter reverse the wrong flagging.

It has been reported by the AT & T research institute in Nigeria that it takes an average of $1\frac{1}{2}$ working days to resolve an incorrect report by the EPP software. This is equivalent to $13\frac{1}{2}$ working hours. Now factoring in the two states of the EPP and combining with equation 1, the probability of incorrect report can be determined by equation 5.

$IR = 99.1\ X \frac{9}{2000}$ (5)

In the worst-case scenario in which all detected file is incorrect, the rate at which the system will show incorrect report is as shown in equation 6.

$IR_{wc} = y_0(y_2 + y_1 + y_4)$ (6)

As stated earlier, the probability of protection was given by W, also EPP software can exist in two states, correct and incorrect report and therefore the probability for the worst-case scenario is given by equation 7.

$P(IR_{wc}) = 1 - W$ (7)

It has been stated earlier according to the results gathered from the AT & T research firm in Nigeria that W = 99.1%, from this $P(IR_{wc})$ is equal to 0.009.

From the aforementioned, the weighted average of all three cases i.e., correct report, incorrect report and worst scenario is as shown in equation (8).

$x = 0.11y_0y_3 - 0.009\ y_0(y_2 + y_1 + y_4) + 0.0009y_0y_1$ (8)

A MATLAB graph is drawn for equation 8. From Figure 2, it can be seen that the intercept on the y-axis which denotes the loss is 1.8, also it can be seen that the value of y increases very little with increase in x. This can be attributed to the fact that the probability or a worst-case scenario is very low indeed. This shows that even if the sum of y_2, y_1 and y_4, (where y_1 denotes the time required to identify the threat, y_2 denotes the time needed to isolate the threat and y_4 denotes the time required to reverse incorrect report) changes rapidly, this will not greatly impact negatively on the company's loss economically. It can also be noticed from Figure 2 that the y intercept starts from 1.8, this is an indication that incorporating the EPP software on a company network system will make the system operate slowly as it increases resource utilization of the system. This will result in low productivity; however, the gain resulting from the protection of the company's network from insider threats far outweighs this loss in productivity.

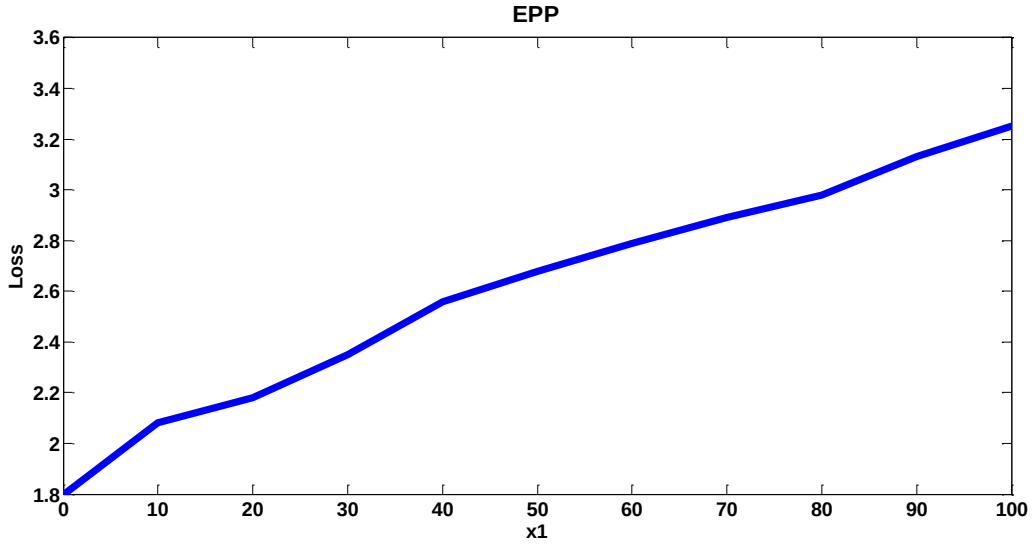

Figure 2 EPP loss trend y_3 = 9h, y_1 = 14h, y_2 = 10h y_0 = 1

Model for EDR

It was discussed in section V that EDR uses machine learning technique to learn the behaviour or attributes of insider threats so as to predict the likelihood of a file being a threat or not. It has the advantages of extending the learning attributes to classify unknown instances of threat.

Like in the EPP model, it will be assumed that the probability of EDR to be in protect state be T. The value of T will be between 0 and 1. A parameter for EDR as a function of T will be developed. The parameter describes the decrease in efficiency of the system as a result of detecting and isolating the threat. It should be realized here that EDR first detects before taking response, however it is possible that a virus has attacked a system for certain time interval i.e., x hour before it is detected by EDR. The attack of the system may lead to incapacitation of the system. The aim of EDR is to mitigate the adverse effects of the threats through the use of threat intelligence routine. When $f(T) = \frac{2}{3}$, it means that the threat can incapacitate the system for $\frac{2x}{3}$ hours. This implies that T is inversely proportional to f(T). However, both T and f(T) are less than 1 because it is hardly possible that the threat will completely run down

the system. The aim of EDR is to reduce the time a threat can incapacitate the system. The higher the probability of T, the more the properties of threats the system has learned and the time for the system paralysis will be reduced. The formula for EDR is given in equation 9.

$$x = f(T)\, y_2 y_1 y_0 \quad (9)$$

From here, the weighted average of the two instances of EDR can be computed; this will give the average weighted value given in equation 10.

$$x = T.\ f(T) y_2 y_1 y_0 \quad (10)$$

Using the result derived from most of the EDR products, the domain of T is adjusted to (0.7, 1). This is because the defence rate of most EDR software is higher than 90%. In the model used here, it will be assumed that f (T) is given by equation 11.

$$f(T) = 1 - T^2 \quad (11)$$

Using the assumption in equation 11, the graph in Figure 3 which shows the trend in EDR as a function of working hours and system efficiency of 1 will be gotten from MATLAB plot.

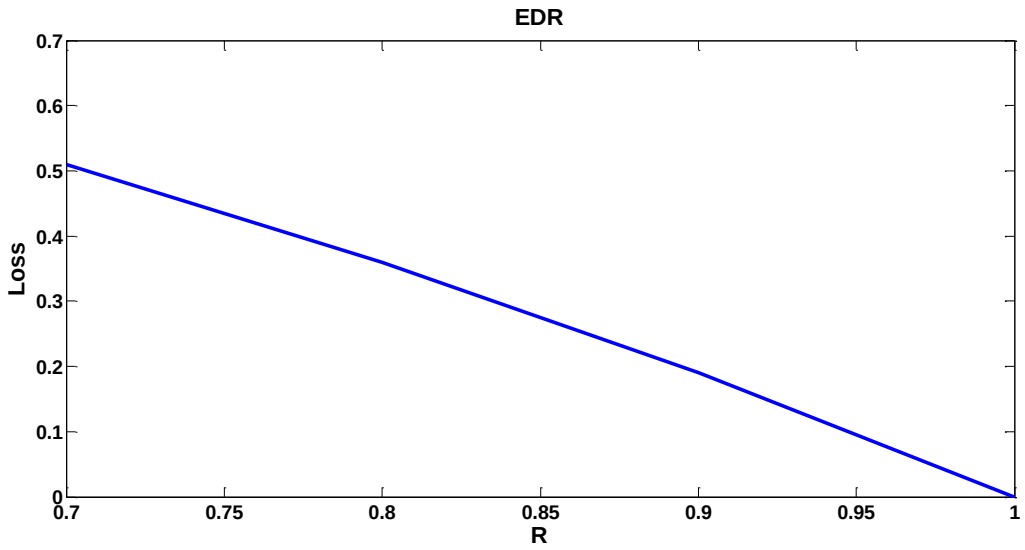

Figure 3 EPP trend loss $y_3 = 9h$ and $y_0 = 1$

As in Figure 3, with an increase in T, the company's loss will be reduced considerably. When T is equal to 1, the losses become 0. This is the absolute behaviour of the EDR software. In other words, it is capable of identifying new and unknown threats which is a big advantage over EPP platform. In the statistical data provided by an AT & T research institute in Nigeria (Xiangyu et al., 2017), it was found out that the average protection rate of EDR was 99.4% while the average false positive alarm rate is $\frac{19}{3000}$. With respect to this information, EDR tools can be grouped under two categories as stated earlier

Correctly detected: Here the EPP correctly identify the threat so as to be isolated

Incorrect detection: Here the EPP incorrectly flags a normal file as a virus

In the course of the design of the model used in this paper, it was observed that varying the sum of y_1 and y_2 in MATLAB will cause the loss due to the implementation of the EDR platform in a company's network to fluctuate greatly. A low value for the sum will reduce losses for the company while a high value for the sum will inflate the company's loss. For this reason, the optimization of the model was needed to arrive at an optimum value for the sum.

In the model the optimal value for the sum of y_1 and y_2 was found to be 9 hours. This represents the average time needed by EDR software to eliminate invasive virus. However, it is a well-known fact that the sum of y_1, y_2 and y_4 is different for various types and categories of virus. The value of 9 was inserted in the model and the 3D graph in Figure 4 was obtained. Figure 4 an increase in the value of T and the sum of y_1, y_2 and y_4 causes the company's loss to be higher. This validates the model presented in this paper as shown in equation 9 and 10.

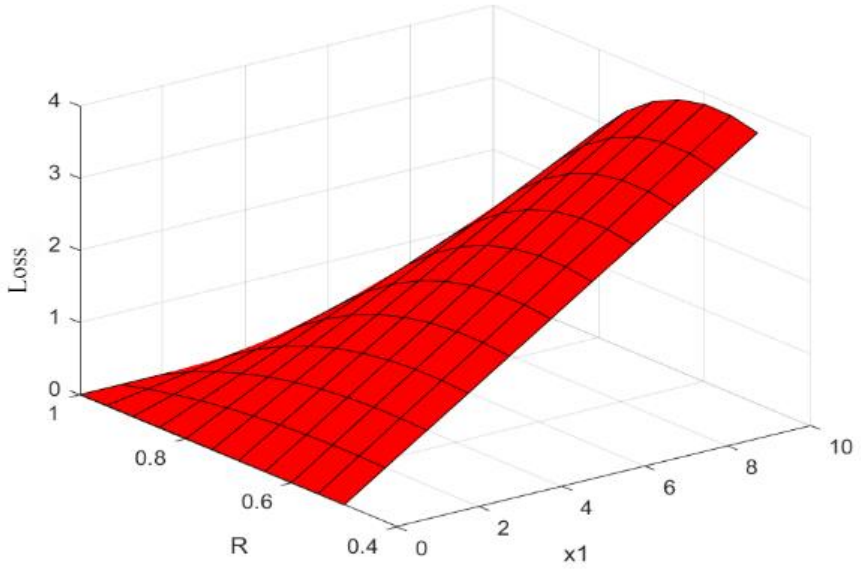

Figure 4 EDR loss trend $y_3 = 9h$ and $y_0 = 1$

EPP and EDR Model Comparison

In this subsection, the model designed for EPP and EDR will be compared in order to obtain their efficiency. This will help companies decide on both EPP and EDR specification best suited for their company's network system and budget. Figure 5 shows the result of this combination. From the Figure 5 it can be noticed that there exist a point of intersection between the boundaries of EPP and EDR. When equations 8 and 10 are solved simultaneously, the boundary equation of EPP and ED will be as in equation 12.

$$y_1 = \frac{0.8345}{xf(T) - 0.0009} \quad (12)$$

As in Figure 5 the left boundary of the graph, the red plane representing EDR is below the blue plane representing EPP, this shows that the loss in a company's revenue is higher when using the EPP than EDR. It has been shown earlier that EDR is better than EPP due to its application of machine learning techniques, which enables it to detect not yet known viruses. This ability is not present in EPP; the graph in Figure 5 again validates the model presented in this paper.

Again form Figure 5, it can be seen in the left boundary that EDR has a higher probability of detecting virus than EPP, however the condition over which this is possible is when the time of inactivity caused by the virus is low i.e. less or equal to 2hrs. This means that the best choice of endpoint security to choose is EDR when the inactivity time caused by the virus is less or equal to 2 hrs. The mathematical model satisfying this condition is in equation 13.

$$y_1 < \frac{0.8345}{xf(T) - 0.0009} \quad (13)$$

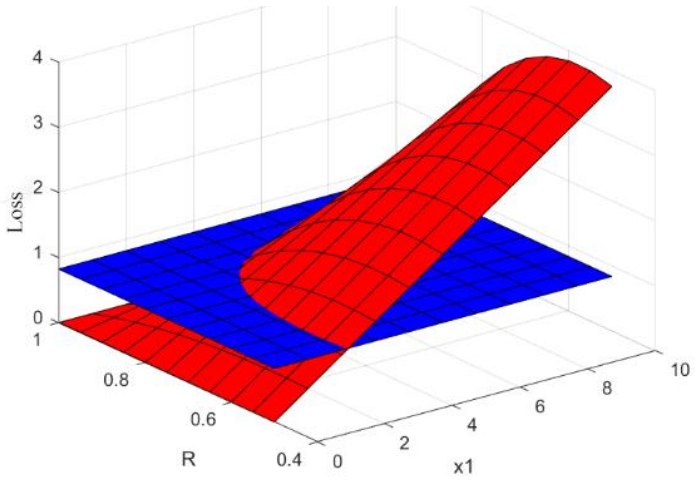

Figure 5 EPP and EDR trend loss combined $y_3 = 9h$, $(y_1 + y_2 + y_4) = 24$ and $y_0 = 1$ EDR is represented by a red plane while EPP is represented by blue plane

Now going to the right-hand boundary of the graph, where the time of inactivity caused by the virus is greater than 2 hours, it can be seen that the red plane representing EDR is higher than the blue plane representing EPP. This means that under this condition, the best endpoint software to choose is the EPP. The mathematical model for this condition is in equation 14.

$$y_1 > \frac{0.8345}{xf(T) - 0.0009} \quad (14)$$

Equations 13 and 14 show that if a virus succeeds in compromising EDR software, it will make the system's network inactive for prolonged period of time. This is evident from Figure 5 where the right boundary of EDR is higher than that of EPP. However, when the EDR's defence mechanism able to mitigate the virus, then the company's loss could be as low as zero. In the case of EPP, it is responsible for mitigating the virus; hence a virus which can cause a higher time of inactivity for the system will not make it unstable. It can be noticed that the slope of EPP is lower than that of EDR as the inactivity period increases.

5. CONCLUSION

This paper has developed a model to measure the effectiveness of both EPP and EDR software as endpoint protection platforms. This paper has shown the areas of strength of EPP and EDR, which can serve as a point of reference to most establishment in need of the provision of network services. From the results obtained in this paper, it would be recognized that EPP is more effective in dealing with external threats since their behaviour can easily be characterized by known parameters which can easily be counteracted by its HIDS and HIPS features.

On the other hand, EDR is more effective in dealing with insider threats. This is due to its ability to learn the behaviour and characteristics of various insider threats through its machine learning techniques. It is therefore able to detect yet to be identified insider threats through its extensive machine learning algorithm. However, the down-point of EDR is its inability to handle infection that can propagate through the endpoints as it can't monitor the activities of the various endpoints connected to the company's network.

The model also shows that EPP is able to reduce loss where the threat causes a high inactivity time for the system. This is because one of the major functions of EPP is to protect endpoint and as such will prevent virus from compromising the system for any appreciable length of time, however the EDR will only detect and respond thereafter, so any virus that beats its detection mechanism will get the system incapacitated or a long time. The take home here is that EDR must either mitigate against all known and unknown threats or be able to remove the threat as quickly as possible to be successful. If this is not the case, then EPP will be preferable. However most EDR software can claim high detection rate, so the best option is to consider the factors here before selecting endpoint security software.

Ethical issues

Not applicable.

Informed consent

Not applicable.

Funding

This study has not received any external funding.

Conflict of Interest

The author declares that there are no conflicts of interests.

Data and materials availability

All data associated with this study are present in the paper.

REFERENCES AND NOTES

1. Apostolopoulos T, Katos V, Choo KR, Patsakis C. Resurrecting anti-virtualization and anti-debugging: Unhooking your hooks. Future Gener Comput Syst 2021; 116:393–405.
2. Arcticwolf. Endpoint Detection and Response Is Not Enough 2019. https://arcticwolf.com/resources/blog/endpoint-detection-and-response-is-not-enough/
3. Asher-Dothan L. Seven essential elements of modern endpoint security 2017. https://www.cybereason.com/blog/7-elements-of-modern-endpoint-security
4. AV-C. Real-World Protection Test July-November 2020. https://www.av-comparatives.org/tests/real-world-protection-test-july-november-2020/
5. AV-TEST. AV-TEST Product Review and Certification Report – Sep-Oct 2021. https://www.av-test.org/en/antivirus/business-windows-client/windows-10/october-2021/bitdefender-endpoint-security-7.2--7.3-212505/
6. Bertino E, Ghinita G. Towards mechanisms for detection and prevention of data exfiltration by insiders: Keynote talk paper. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China 2011; 10-19.
7. Brancik K, Ghinita G. The optimization of situation awareness for insider threat detection. Proceedings of the First ACM Conference on Data and application security and privacy, San Antonio, TX, USA 2011; 231-236.
8. Brogi G, Tong VVT. Terminaptor: Highlighting advanced persistent threats through information flow tracking. In 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS) 2016; 1–5.
9. Chandel S, Yan M, Chen S, Jiang H, Ni T. Threat Intelligence Sharing Community: A Countermeasure Against Advanced Persistent Threat. IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), San Jose, CA, USA 2021; 353-359.
10. Claycomb WR, Shin D. Detecting insider activity using enhanced directory virtualization. Proceedings of the 2016 ACM workshop on Insider threats, Chicago, Illinois, USA 2016; 29-36
11. Le C, Khanchi S, Nur A, Zincir-Heywood, Malcolm I. Benchmarking evolutionary computation approaches to insider threat detection. Proceedings of the Genetic and Evolutionary Computation Conference, Kyoto, Japan 2020; 1286-1293.
12. Le D, Khanchi S, Zincir-Heywood AN, Heywood MI. Benchmarking evolutionary computation approaches to insider threat detection. Proceedings of the Genetic and Evolutionary Computation Conference, Kyoto, Japan 2018; 1286-1293.
13. Liao H, Lin CR, Lin Y, Tung K. Intrusion detection system: A comprehensive review. J Netw Comput Appl 2013; 36(1): 16-24.
14. Rashid T, Agrafiotis I, Nurse RC. A New Take on Detecting Insider Threats: Exploring the Use of Hidden Markov Models. Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, Vienna, Austria 2018; 47-56.
15. Samuel A. Some Studies in Machine Learning Using the Game of Checkers. IBM J Res Dev 2021; 3(3): 210–229.
16. Sanzgiri A, Dasgupta D. Classification of Insider Threat Detection Techniques. Proceedings of the 11th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA. CISRC 2016; 67–78.
17. Strom D. 7 trends in advanced endpoint protection 2019. https://www.networkworld.com/article/3089858/endpoint-protection/7-trends-in-advanced-endpoint-protection.html
18. Sun Y, Li N, Bertino E. Proactive defense of insider threats through authorization management. Proceedings of International workshop on Ubiquitous affective awareness and intelligent interaction, Beijing, China 2018; 9-16.
19. Sun Y, Li N, Bertino E. Proactive defense of insider threats through authorization management. Proceedings of 2017 international workshop on Ubiquitous affective awareness and intelligent interaction, Beijing, China 2017; 9-16.
20. Voris J, Jermyn J, Boggs N, Gordon N, Salvatore S. Fox in the trap: thwarting masqueraders via automated decoy document deployment. Proceedings of the Eighth European Workshop on System Security, Bordeaux, France 2015; 67–78.
21. Xiangyu L, Qiuyang I, Chandel S. Social Engineering and Insider Threats. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing 2017; 121-134.
22. Xiangyu L, Qiuyang L, Chandel S. Social Engineering and Insider Threats. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing 2020; 25-34.
23. Zhang H. An Active Defense Model and Framework of Insider Threats Detection and Sense. Int Conf Inform Assur Secur IEEE Comput Soc 2018; 258-261.