Endpoint Security: An Overview and a Look into the Future

Sam Slate
May 7th, 2018

1. Abstract

Endpoint security, the securing of endpoint devices on a large network, is an important piece of company and organizational security. In this paper, I'd like to introduce endpoint security, describe the methods most commonly used, and discuss the future of the field. Additionally, I hope to impress upon the reader the need to adopt comprehensive endpoint security solutions and to take seriously the vulnerabilities inherent in large networks.

2. Introduction

In any modern-day company, it would be near impossible to list every internet connected electronic device used by an employee. There are desktops, laptops, and phones. Perhaps there are also tablets, printers, consumer interfaces, washing machines, cameras, and more. The landscape of devices connected to a company network is large and always growing. How does a modern company attempt to secure all of these devices to any effective degree?

In the security world, any device connected to a company network is called an endpoint.[i] Each endpoint represents a particular security vulnerability to the network, subject to attacks and leakage of information.[ii] The systems set in place to protect these endpoints is called endpoint security, and it encompasses the wide range of tactics, both behavioral and technical, used to secure networks.[iii]

2.2 To the Community

If you are an employee at a large company, most likely you have endpoint security in place. If not, you need to advocate incredibly hard for it to be implemented. Security of company devices is not just a profit problem, it is a privacy and safety problem. As companies handle more and more private, sensitive information, the consequences of security breaches grow in magnitude ten times over. Endpoint vulnerabilities can release millions of private profiles to the world, can lock vital services for ransom, and can bring to a halt governments and healthcare systems. It is imperative that you take ownership of your devices and protect yourself, your company, and the people you serve.

3. What is Endpoint Security

A company network connects endpoints with each other, such as a computer to a printer, and with internal structures, such as servers, databases, intranets, and extranets.[iv] The larger network allows for communal access to files, software, and internet, and provides specialized methods of communication and organization.[v] A user will access a network by connecting to an endpoint, either in person or remotely. Depending on the setup of the network, they will then have access to part or all of the network.

The vulnerabilities of endpoints seem endless. By the nature of the network, a compromised endpoint can gain access to almost every other point in the network. Many of the attacks targeting endpoints are similar to those that target an unconnected computer, but the stakes are much, much higher. According to one source, 70% of successful corporate exploits target endpoints, rather than servers or other internal infrastructures.[vi] Notable breeches of well-known companies in the past five years, such as one involving point-of-sale endpoints at Target, drive this point home.[vii]

3.2 Unique Difficulties of Endpoint Security

What is so unique about endpoints that make them particularly difficult to secure? For one, the variety of possible endpoint devices makes it incredibly challenging to institute a one-size-fits-all system for securing them.[viii] Their numbers in large company networks also increases the chance of exploitation, and the interaction between users and endpoints brings in behavioral and security culture concerns.[ix] Finally, as with many other security weaknesses, much less attention is paid to endpoints than to other operations in a company.

New developments in company networks increase the difficulty as well. The surge in BYOD (bring your own device) policies ushers in a whole host of threats, including a lack of oversight and standardization of endpoints, not to mention the unique vulnerabilities of the wide variety of endpoints BYOD encourages.[x] The migration to the cloud introduces cloud-based attacks,[xi] and, as always, innovations in black-hat methods require innovations in protection.

3.3 Tradeoffs of Endpoint Security

As with any other technical security concern, addressing endpoint vulnerabilities requires trade-offs. A company must balance the comprehensiveness of the security plan with cost-effectiveness, effort required to implement, and consequences in efficiency and productivity. There must also be a balance in focus between behavioral and technical approaches and a balance between what is desired and what is achievable. At the end of the day, no company can ensure 100% security of their endpoints; a company must determine the minimum protection needed in order to minimize the most dangerous of vulnerabilities.[xii]

4. Endpoint Security Strategies

Any comprehensive endpoint security strategy starts with coordination at the upper level of management. A Change and Control Board, made up of engineers and executives, is usually created to oversee security operations and serve as the centralized hub for information and implementation.[xiii] A strategy is developed by the Change and Control Board to put in place security measures dependent on the organizational structure of the company, including behavioral and technical procedures and structures to support their implementation. Such structures include resources and personal devoted to assisting security implementation, methods for analysis and feedback, and maintenance of security measures.[xiv]

4.2 Behavioral Strategies

When most people think of computer security, they imagine software on a computer that battles with a would-be attacker. The truth is, however, that the majority of vulnerabilities come from the human element of the human-computer relationship. Many endpoint security strategies start at this human side, looking at what risks lie in the behavior of users and interaction with endpoints, as opposed to the endpoints themselves.[xv]

According to a study from Data Breach Today, the most common vulnerability of endpoints in the healthcare sector is improperly configured devices and default admin credentials.[xvi] Poor password security is a problem that haunts every company and continues to deliver exploit after exploit.[xvii] The solution on a company level is instating policies and accountability for password security company-wide, and integrating security measures, such as two-factor authentication, into standard practice.

Other behavioral security measures related to endpoints include requiring the updating and patching of software, recommendations on how to physically secure devices, and protocols on how to avoid social engineering and phishing attacks.[xviii] Endpoints are particularly vulnerable to behavioral exploits because a user directly interacts with the device and may be lulled into a false sense of security due to their familiarity with the device, especially with BYOD. For example, an employee using their own laptop may forgo usual security measures because of the merger of personal and work security standards.

4.3 Technical Strategies

The technical strategies of endpoint security consist of many of the strategies an individual would use to secure their own computer, with the increased dimensions of scale and device variance. Firewalls, for example, are commonly used to ensure safe web access within a network.[xix] VPNs and proxies are also common to secure web traffic, and device whitelists and blacklists protect against attackers.[xx]

Along with the usual suspects, there are quite a few endpoint-specific vulnerabilities. For example, a large network is susceptible to rogue hosts, that is devices that pretend to be an

endpoint in order to access the network. Endpoint security strategies will often include rogue host detection, which alerts if an unidentified device attempts to connect.[xxi]

One of the main difficulties in implementing technical solutions is compatibility across devices and configurations needed for specific applications.[xxii] Some devices may have older versions of software by necessity that is incompatible, and others may have hardware that limits the use of certain security software. Those in command of endpoint security must keep track of a wide range of possible devices and maintain a threshold of security across the network as a whole.

As endpoint security encompasses a wide range of complex applications and quickly scales out of control, many companies invest in endpoint security products from security companies that specialize in company networks. These companies will provide a suite of protection tools, as well as a command interface, advanced analytics, and updates as new vulnerabilities are discovered.[xxiii] The 2016 market size for endpoint security companies was over four billion dollars, and is expected to double by 2021.[xxiv]

5. Future of Endpoint Security

Endpoint security companies are often on the frontline of innovating endpoint security solutions. One such innovation is the use of artificial intelligence and the cloud to better identify threats.[xxv] Basic security tools such as antivirus software can only scan malware for known patterns. Artificial intelligence however can be used to predict possible modifications of malware that would otherwise pass common AV, as well as determine deeper patterns in malware that cannot be determined by the human eye.[xxvi] If we think of the battle between attackers and defenders as a back and forth where the attacker exploits a vulnerability, the defender updates their security to prevent it, and then the attacker creating something new, artificial intelligence is using advanced algorithms on millions of attack cases to predict what the attacker will develop before they do so and defend against it.[xxvii]

The cloud provides the computer processing power needed to run artificial intelligence algorithms. In addition, cloud based endpoint security allows for real-time analysis and monitoring, as well as location-independence protection and fast alert systems.[xxviii] Many of the endpoint security companies that label themselves as “next generation,” such as Promisec, Carbon Black, Cisco, Kaspersky, and Symantec, provide cloud-based security products. A popular new category of tools offered by many of these companies, called Endpoint Detection and Response software, combines antivirus software with centralized malware databases in the cloud and triggered responses to identified malware attacks.[xxix]

5.2 Shared Data

Of particular interest to me is the use of shared malware databases to aggregate data for artificial intelligence. As of now, endpoint security companies use the cloud to share data among their clients, but I wonder if someday in the future companies will share data between themselves to enrich the greater cybersecurity community. A report from the National Institute of Standards

and Technology articulates in detail how exchanging cybersecurity threats within an industry can benefit the security of everyone.[xxx] Research on machine learning and artificial intelligence has similarly proven that the more data used to feed into algorithms, the better the results.[xxxi]

A limit to this type of exchange within the industry is the financial consequences of releasing datasets. At what point does it become financial beneficial to endpoint security companies to share data between themselves? What is the balance of protecting company resources and providing the best security to customers?

As new threats arise with more complex techniques, such as ransomware, these questions will become more and more essential to the overall security community. In the field of diseases and public health, international organizations such as the World Health Organization focus on creating networks around the world to share data on new diseases, immunizations, and vaccinations. Common sense says that countries should not keep important disease information to themselves, even if it might be used by an enemy nation. Similarly, a time may come when the public good of sharing malware information across companies and organizations will surpass the desire for profit from private cybersecurity companies. The need for larger data sets to better artificial intelligence for endpoint security is one such example of needed communication and coordination.

The future of the endpoint security field will depend on if and when major crises in endpoint security occur, such as an entire company or country held for ransom, and what radical shifts in security frameworks and mindsets will be needed to move forward. I imagine a time when open source sharing of endpoint security information and techniques will be a necessity to fight growing international security threats.

6. Action Items

If you are in charge of implementing endpoint security for your company or organization, follow this eight step plan to get started. You can also find an infographic with this information here.

1. **Coordinate your people:**
   Get together engineers, executives, and management. Proper Endpoint Security requires coordination on all fronts, so it's best to get everyone in a room together.

2. **Understand what you have:**
   Do a comprehensive study of what devices you wish to protect and how they fit into your network.

3. **Understand what you need:**
   Think about how you wish to protect your devices and to what degree.

4. **Think about tradeoffs:**
   Decide on where you want to fall on tradeoffs like security versus price, security versus effort to implement, and behavioral focus versus technical focus.

5. **Decide on your strategy:**
   One of the biggest questions you need to answer is whether you outsource your endpoint security to a security company or do it yourself. Make decisions on this question and all others.

6. **Do your research:**
   Once you decide on your strategy, use resources such as this paper to narrow down your choice of tools and techniques.

7. **Create a plan and follow through:**
   Develop a plan with your leadership team that encompasses all aspects of endpoint security, including internal support structures and methods for analysis and feedback.

8. **Evaluate and evolve:**
   Proper endpoint security is a process! Evaluate your progress and evolve your techniques.

7. Conclusion

Endpoint security literacy is important at all levels of a company, from the leadership that designs strategies to the average employee who implements them. While not everyone may have the in depth technical understanding of endpoint security tools, everyone must understand what it means to keep their devices secure on a day-to-day basis. This includes the behavioral strategies, use of technical tools when needed, and perhaps most importantly, the ability to reach out to a support network at any time to ask endpoint security related questions.

As endpoint security threats continue to grow in frequency and lethality, endpoint security solutions must evolve as well. Companies must prepare themselves for the changing tides of vulnerabilities and exploits, and must look ahead to possible crises and future threats. Creating and implementing endpoint security strategies is just the starting point; endpoint security is a continuous process that requires attention, resources, and preparation. At the end of the day, the safety and security of consumers are at risk.

Works Cited

Beal, Vangie. "Endpoint Security." *The Five Generations of Computers - Webopedia Reference*, www.webopedia.com/TERM/E/endpoint_security.html.

Ahl, Ian. "The Relevance of Endpoint Security in Enterprise Networks." *Cyber-Development, Cyber-Democracy and Cyber-Defense*, 2014, pp. 337–354., doi:10.1007/978-1-4939-1028-1_14.

Mitchell, Bradley. "Introduction to Business Computer Networks." *Lifewire*, www.lifewire.com/business computer-networks-817883.

"Advantages of Setting Up a Business Computer Network." *Tranquilnet | 858-259-9388 | Del Mar 92014 | Carmel Valley 92130 | San Diego CA*, tranquilnet.com/resources/advantages-of-setting-up-a computer-network-for-your-business.html#.

Kirsch, Christian. "IDC Says 70% of Successful Breaches Originate on the Endpoint." *Rapid7 Blog*, Rapid7 Blog, 31 Aug. 2017, blog.rapid7.com/2016/03/31/idc-says-70-of-successful-breaches-originate-on the-endpoint/.

Williams, Jacob. "The Case for Endpoint Visibility, A SANS Analyst Survey." Mar. 2014.

"Endpoint Security: Preventing Threats on Devices Connected to Your Network." *Types of Malware and How to Defend Against Them*, www.esecurityplanet.com/network-security/endpoint-security.html.

Kolba, David. "How Does Endpoint Security Change in a BYOD World?" *CIO*, CIO, 4 Nov. 2014, www.cio.com/article/2842899/mobile/how-does-endpoint-security-change-in-a-byod-world.html.

Roemer, Kurt. "Securing the Cloud Endpoint." *Network World*, Network World, 4 Nov. 2016, www.networkworld.com/article/3138540/cloud-computing/securing-the-cloud-endpoint.html.

"Study: Endpoint Vulnerabilities Common." *Data Breach Today*, www.databreachtoday.asia/study-endpoint vulnerabilities-common-a-6514.

Ogden, Jacqueline von. "The 6 Most Common Network Vulnerabilities Haunting CSOs in 2017." *Cimcor, Inc.*, www.cimcor.com/blog/6-common-network-vulnerabilities-cso-2017.

Garside, Debbie, and IDG Contributor Network. "The Future of AI and Endpoint Security."*CSO Online*, InfoWorld, 18 Jan. 2018, www.csoonline.com/article/3249093/endpoint-protection/the-future-of-ai and-endpoint-security.html.

"Best Endpoint Protection Software in 2018." *G2 Crowd*, www.g2crowd.com/categories/endpoint-protection.

"Endpoint Security Market Size 2014-2020 | Statistic." *Statista*, www.statista.com/statistics/497965/endpoint security-market/.

"Why Artificial Intelligence Is the Future for Endpoint Security – SparkCognition Inc."*SparkCognition Inc*, 5 Jan. 2018, www.sparkcognition.com/2017/11/artificial-intelligence-future-endpoint-security-2/.

Sharma, Sugandha. "FIGHTING VIRUS AND MALWARE WITH ARTIFICIAL INTELLIGENCE."*Insights Success*, 16 Jan. 2016, www.insightssuccess.com/fighting-virus-and-malware-with-artificial intelligence/.

"Antivirus Is Dead: How AI and Machine Learning Will Drive Cybersecurity." *TechBeacon*, techbeacon.com/antivirus-dead-how-ai-machine-learning-will-drive-cybersecurity.

Siemons, Frank. "5 Benefits of Cloud-Based End-Point Security Products." *Infosec Institute*, 7 Dec. 2016, resources.infosecinstitute.com/5-benefits-of-cloud-based-end-point-security-products/.

Walker, Aaron. "What Is Endpoint Protection? Breaking Down Next-Gen Security." *G2 Crowd*, 16 Feb. 2018, blog.g2crowd.com/blog/endpoint-protection/endpoint-protection-breaking-down-next-gen-security/.

Johnson, Christopher S., et al. "Guide to Cyber Threat Information Sharing." *National Institute of Standards and Technology*, 2016, doi:10.6028/nist.sp.800-150.

Domingos, Pedro. "A Few Useful Things to Know about Machine Learning." *Communications of the ACM*, vol. 55, no. 10, 2012, p. 78., doi:10.1145/2347736.2347755.

---

[i] Beal
[ii] Ahl, 339
[iii] Beal
[iv] Mitchell
[v] Advantages
[vi] Kirsch
[vii] Williams
[viii] Ahl, 339
[ix] Endpoint Security
[x] Kolba
[xi] Roemer
[xii] Ahl, 353
[xiii] Ahl, 340
[xiv] Ahl, 342
[xv] Endpoint Security
[xvi] Study
[xvii] Ogden
[xviii] Garside
[xix] Ahl, 347
[xx] Ahl, 349
[xxi] Ahl, 350
[xxii] Ahl, 339
[xxiii] Best Endpoint
[xxiv] Endpoint Security Market
[xxv] Why Artificial Intelligence
[xxvi] Sharma
[xxvii] Antivirus is Dead
[xxviii] Siemons
[xxix] Walker
[xxx] Johnson
[xxxi] Domingos