**ISSN:** 2583-9888
**DOI:** doi.org/10.51219/JAIMLD/Jaya-Sehgal/483

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 1

*Research Article*

# Layered Security Meets Defense in Depth: A Dual Approach to Threat Miti-gation

**Jaya Sehgal***

**Citation:** Sehgal J. Layered Security Meets Defense in Depth: A Dual Approach to Threat Miti-gation. *J Artif Intell Mach Learn & Data Sci 2023*, 1(1), 2208-2210. DOI: doi.org/10.51219/JAIMLD/Jaya-Sehgal/483

**Received:** 02 March, 2023; **Accepted:** 18 March, 2023; **Published:** 20 March, 2023

***Corresponding author:** Jaya Sehgal, Jersey City, New Jersey, USA, E-mail: jaya.sehgaloo1@gmail.com



## ABSTRACT

With the advent of technology, cybersecurity has become part of day-to-day lives, where security threats, identity theft and network attacks are more common than ever imagined. Information security aims to sustain and defend three critical security properties of information: confidentiality, integrity and availability2. The motivation behind these attacks can be cyber-terrorism, political espionage, financial gain or anything else. To address the ongoing threats to systems and networks, various security strategies can be employed, such as Defense in Depth and Layered Security. These two approaches can complement each other to strengthen cybersecurity, thus reducing risks across the entire attack surface. This paper aims to focus on the elements of these two strategies, synergies, advantages and disadvantages of each framework and summarize how organizations can build and reduce reliance on a single point of failure. The Defense in Depth and Layered Security are interchangeably used, but their applications are different, although the context is identical. According to SOPHOS Security5, "Modern malware is all about stealth". In a larger context, a Layered Security or Defense in Depth can safeguard organizations' networks using multiple security practices or products or, at the very least, mitigate the impact.

**Keywords:** Layered security, Defense in depth, DiD, Cybersecurity, Multi-factor authentication. MFA, Zero ac-cess, Network security, Threat mitigation, Zero trust, Information security

## 1. Defense in Depth (DiD)

The Defense in Depth (DiD) originated as a strategy in the military to slow down the progression of attacks and have a single defensive line with all the resources deployed in layers to protect the population. The National Security Agency (NSA) originally designed DiD as a best practices strategy for achieving information assurance"[6]. Similarly, Defense in Depth in networking is a strategy to have multiple levels or layers of security to protect data and malicious attacks on the network. The intent of having multiple layers is to build a backup against the failure of one layer for the security threats originating from multiple origins. This strategy has a multi-dimensional approach to security where security controls are deployed at physical, technical and administrative layers. At the physical layer, data centers and physical assets on the network shall be provided with surveillance, scanners, biometric IDs and facial recognition systems. Technology control is applied to ensure all the hardware and software are secure by using firewalls, antivirus software, intrusion detection and prevention systems (IDS/IPS), etc. The administrative security control is deployed to control access to internal systems, resources, data and information. Internal information is often classified as confidential or for internal use only. In addition to the controls, certain security practices are used in Defense in Depth.

Some of them are listed below:

Multi-factor authentication (MFA is a security practice to add extra layer of authentication. For example, an organization's network can be accessed using a VPN, but authentication

happens using an MFA token provided by Google or Microsoft for extra security. Following strong passwords along with identity verification for getting is covered under multi-factor authentication. It is used heavily not only at the organizational level but for personal use, such as emails or website logins.

Traffic Analysis to identify abnormal patterns or usage is a great way to prevent attacks. However, it is a continuous process as attackers keep evolving and building new methods to threaten security; these patterns will also have to evolve along with the monitoring tools. Tools like "SolarWinds NetFlow Traffic Analyzer" can be significant assets to the organization and help analyze the anomalies in real time.

Zero Access or least privilege access should be the first and foremost security practice to be adopted by any organization. This means giving zero access to those who do not need it and limiting access to those who do. It is a concept where role-based permissions are granted to everyone in the team. With cloud adoption across the board, these security practices are becoming much easier than ever.

### 1.1. Advantages

Defense in Depth strategy can reduce the risk of a very expensive security breach. Due to multiple layers of Defense, if one layer fails to detect or prevent, the other layer can. The redundancy is the primary advantage of Defense in Depth. The other aspect as mentioned above is the multi-dimension where this strategy can protect a firm from all sides and at all levels.

### 1.2. Disadvantages

The primary disadvantages are the implementation cost and overall management of the security constructs such as firewalls, IDS/IPS systems, traffic monitoring tools, access control mechanisms, role-based permissions and network virtualization. The other disadvantage is that it is a complex strategy as it must ensure it is adopted in multi-dimensions. Hence, the network design at one dimension must complement the other to safeguard all the resources.

### 1.3. Layered security

Layered security is part of a larger strategy known as "Defense in Depth[8]. Conceptually, layered security also has multiple layers, such as that of Defense in Depth. However, it is often implemented at one of the controls, primarily technology. The multiple layers are not of the same kind; Layered Security focuses on network perimeter defense, application defense, host defense, data defense, etc. Layered security can simultaneously tackle multiple security vulnerabilities through multiple layers. It is divided into three main categories - prevention, detection and response. Layered Security has a layer of defense for each security gap in the system, such as firewalls, encryption, authentication, etc. Layered Security strategy has a primary objective of preventing an attack at the very origin of the threat by virtue of multiple layers of security protocols. The following defines a few layers of security in a layered security strategy:

Security Policy is the first step to secure the network. This can vary according to an organization's business functions.

Perimeter defense can be a firewall, IPS/ IDS or malware monitoring tool. This is to secure a perimeter and Endpoint protection is to protect the authorized users from security vulnerabilities. Software like Symantec provide features of advanced security by using a firewall, endpoint protection and many other layers.

Web Content filtering provides additional protection to authorized users against phishing emails and spam that can gain access to the network through their personal data.

**1.3.1. Advantages:** One can see redundant use of security protocols as a disadvantage as well but that is the benefit that offers multiple lines of Defense. Layered security is a flexible and scalable solution for providing security to an organization's network. Layered security can be as simple or as elaborate as an organization wants however a balance between security, cost and operability needs to be defined[4].

**1.3.2. Disadvantages:** One of the disadvantages of layered security is redundancy. Multiple layers can provide security services for the same attack, which is an advantage during specific attacks as well. However, this involves data overhead and processing, which causes additional cost, maintenance and operational overhead, which can be controlled to some extent if accurate security protocols are used at each layer. The other disadvantage is the performance of the network using multiple firewalls, virtual networks and extra security protocols that can cause a bad user experience for internal as well as external users. The other disadvantage is the single point of failure at technology or network control despite multiple layers within the system.

### 1.4. Synergies between defense in depth and layered security

Defense in Depth and Layered Security together can deliver an advanced threat mitigation strategy by addressing their individual limitations:

**Enhanced resilience:** The redundancy of DiD ensures continuity, while the diversity of Layered Security addresses specific vulnerabilities.

**Improved detection and response:** DiD slows attackers, providing more time for the diverse mechanisms of Layered Security to detect and respond.

**Reduced single points of failure:** DiD mitigates risks associated with sequential attacks, while Layered Security ensures independence of controls.

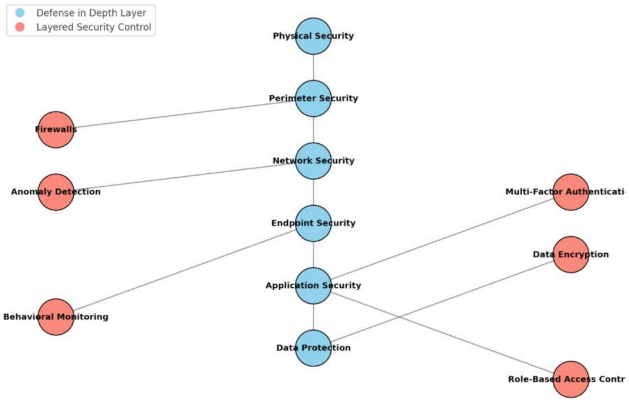


**Figure 1:** Synergies between Defense in Depth (DiD)and Layered Security.

- **Blue color nodes represent defense in depth layers:** These represent the hierarchical layers of security, starting from "Physical Security" and extending to "Data Protection".

- **Red color nodes represent layered security controls:** These highlight specific, independent security mechanisms like Firewalls, Multi-Factor Authentication and Data Encryption mapped to their relevant layers.

Layers of Defense in Depth can be sequentially structured, as shown in Figure 1. Red nodes are linked to blue nodes to depict how specific layered security controls integrate with each layer. This combined approach ensures redundancy, diversity and comprehensive threat mitigation.

## 2. Conclusion

A defense in Depth security widens the scope of attention to security and encourages flexible policy that responds well to new conditions, helping ensure you are not blindsided by unexpected threats[3]. Layered Security is one dimension of the defense in Depth strategy adopted as a technology control with multiple controls within. In contrast to layered security, the Defense in Depth strategy can prevent the attack before it enters the network. Overall, cost is a significant factor to be considered while implementing the security strategy. Defense in Depth is expensive as compared to layered security and organizations cannot afford to not implement the security at all levels -physical, technology and administrative despite the cost. Considering the continued malicious activities and security threats, network security has become a primary concern for any organization, among others.

Integrating Defense in Depth (DiD) and Layered Security strategies provides a robust framework for mitigating modern cybersecurity threats. Defense in Depth builds resilience through multiple sequential layers of protection, each serving as a barrier that delays, detects or neutralizes attacks. Layered security enhances protection by using various independent measures to prevent a single failure from jeopardizing the system. Additionally, multi-factor authentication (MFA) strengthens access control, while data encryption safeguards sensitive data, even in the event of a breach in other layers.

Despite their merits, implementing these strategies together presents challenges, including increased complexity, resource allocation and the need for seamless interoperability between diverse controls. Organizations can ensure greater resilience and faster response times by addressing threats across multiple layers and leveraging diverse controls. The adoption of this dual strategy represents a shift from reactive to proactive cybersecurity, enabling organizations to stay ahead of sophisticated adversaries.

Furthermore, there is a lot of scope for future research to focus on streamlining the implementation of these strategies, leveraging emerging technologies to reduce complexity and adopting adaptive measures to address evolving threats. As organizations continue to digitize and embrace hybrid environments, the synergy between Defense in Depth and Layered Security will remain an essential component of resilient and scalable cybersecurity architectures.

## 3. References


1. Saltzer JH, Schroeder MD. The Protection of Information in Computer Systems. Proceedings of the IEEE, 1975;63: 1278-1308.
2. https://resources.sei.cmu.edu/asset_files/handbook/2006_002_001_14633.pdf.
3. http://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/
4. https://www.ijcit.com/archives/volume3/issue5/Paper030518.pdf
5. http://www.sophos.com/enus/medialibrary/PDFs/other/sophos-security-threat-report2014.pdf
6. Weaver R, et al. Guide to Network Defense and Countermeasures (3rd ed.). Boston, MA: Cengage Learning, 2014.
7. https://www.researchgate.net/publication/291075332_Critical_analysis_of_Cross-layer_approach
8. https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/security-in-depth
9. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education, 2018.
10. NIST. Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology, 2020.
11. Garuba M, Liu G, Eyiti T. Cybersecurity Defense in Depth: A Strategic Perspective. Journal of Cybersecurity Research, 2021;8: 45-56.
12. https://www.wati.com/the-dilemma-of-saas-companies-in-cybersecurity-where-to-begin/