BROADCOM

Executive Summary

Defense in Depth—A Layered Approach to Cybersecurity

In today's complex digital environments, no single security measure is sufficient to protect against persistent and evolving threats. Defense in Depth (DiD) is a cybersecurity strategy that leverages multiple overlapping layers of security controls—ranging from firewalls and encryption to monitoring and response tools—to protect systems, networks, and data. This layered approach ensures that even if one control fails, others remain in place to prevent, detect, and respond to threats effectively.

Why Defense in Depth Matters

Modern enterprises face a wide array of threats across increasingly distributed networks, cloud infrastructures, and endpoint devices. As a result, total prevention of breaches is no longer a realistic goal. The guiding principle of DiD is simple: "Prevention is ideal, but detection is a must—and response is essential." A successful DiD strategy accepts that breaches may occur and ensures the ability to detect, contain, and recover from them swiftly.

Foundational Principles

DiD operates within the broader framework of risk management, aiming to reduce risk to an acceptable level rather than eliminating it entirely. It aligns closely with the CIA triad—Confidentiality, Integrity, and Availability—which guides the selection and implementation of security controls:

Confidentiality
Restrict access to sensitive data.

Integrity
Ensure data and systems are accurate and unaltered.

Availability
Guarantee authorized access to systems when needed.

Each DiD layer supports at least one of these core objectives.

The Zero Trust Connection

DiD shares conceptual ground with Zero Trust, which holds that no user or device should be inherently trusted, even if located within the network perimeter. Zero Trust takes DiD to its logical extreme: continuous verification of all identities, devices, and access requests, with pervasive monitoring and adaptive access controls.

Strategies and Implementation

Organizations can tailor DiD strategies to their specific environments. Common approaches include:

Uniform Protection

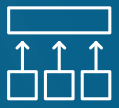
Consistent controls (e.g., firewalls, secure web gateways) across all systems.

Protected Enclaves

Segmenting networks to isolate high-value assets.

Information-Centric Security

Protecting the data itself, regardless of where it resides.



Threat Vector Analysis

Identifying and reinforcing likely avenues of attack (e.g., phishing mitigation through email filtering).

These strategies are often used in combination to build a resilient security architecture.

Types of Security Controls

Controls within a DiD model fall into three main categories:

Preventive
Block attacks before they succeed. Examples of preventive controls include access controls, encryption, and firewalls.

Detective
Identify and alert on suspicious activity. Examples of detective controls include logging, intrusion detection systems, and Security Information and Event Management systems (SIEMs).

Corrective/Response
Contain and remediate incidents after detection. Examples of corrective/response controls include endpoint isolation, password resets, and incident response protocols.

Controls can also be classified by function: technical (e.g., DLP tools), physical (e.g., surveillance), and administrative (e.g., security awareness training).

Importance of Detection and Response

Because breaches are inevitable, timely detection and effective response are essential. Organizations must implement:

Detective Controls
Logging, SIEMs, Intrusion Detection Systems (IDSes), Data Loss Prevention (DLP) systems, and penetration testing to spot anomalies and vulnerabilities

Response Controls
Incident response plans, EDR tools, and SOAR platforms to automate and coordinate containment and remediation

The Cyber Kill Chain

Understanding the attacker's process—outlined in the Lockheed Martin Cyber Kill Chain—helps inform DiD strategies. Each phase of an attack, from reconnaissance to data exfiltration, presents opportunities for DiD controls to disrupt or mitigate the threat.

Conclusion

Defense in Depth offers a pragmatic and resilient approach to cybersecurity by layering preventive, detective, and corrective controls across all vectors—networks, cloud, endpoints, and identity. By acknowledging that no system is impenetrable, DiD equips organizations to detect threats early, respond quickly, and minimize harm—creating a security posture built for today's dynamic threat landscape.

SANS | Research Program

Endpoint Security Challenges

Today's endpoints—ranging from laptops to mobile devices—are often remote, mobile, and not owned by the organization. This shift increases risk and requires tools such as:

Mobile Device Management (MDM)
Enforce policies, separate personal/corporate data, ensure updates.

Application Control
Only allow authorized software to run.

Multifactor Authentication (MFA)
Critical for reducing credential-based attacks.