WHY
LAYERED SECURITY
IS LIKE AIRPORT TRAVEL

OVERVIEW

- ✓ KNOW THE CURRENT THREATSCAPE
- ✓ LAYERED SECURITY AND DEFENSE IN DEPTH (DiD) CAN HELP
- ✓ ELEMENTS OF LAYERED SECURITY AND ITS IMPORTANCE
- ✓ THE 7 LAYERS OF LAYERED SECURITY
- ✓ LAYERED SECURITY AND AIRPORT TRAVEL

– KNOW THE CURRENT THREATSCAPE

- Cybercrime damages are expected to cost $6 trillion per year by 2021.[1]
- Human error is responsible for 90% of cyber data breaches.[2]
- Phishing, a popular attack vector, took advantage of the pandemic to increase its prevalence from 25% last year to 36% this year.[3]
- Ransomware has doubled its frequency since last year, appearing in 10% of verified breaches.[3]

LAYERED SECURITY AND DEFENSE IN DEPTH (DiD) CAN HELP

- Multiple sophisticated threats can attempt to crack into an organization’s network at the same time.
- As a result, relying on a single basic security solution will be ineffective.
- This is where Layered Security and Defense in Depth find their relevance.

LAYERED SECURITY AND DEFENSE IN DEPTH (DiD) CAN HELP

Layered security and **DiD** are two similar yet distinct concepts.

DiD aims to deploy **multiple security measures** to address various threats related to the entire IT infrastructure.

Layered security uses **different security products** to address a particular security aspect, such as email filtering.

ELEMENTS OF LAYERED SECURITY

The **THREE ELEMENTS** of layered security are:

PREVENTION

DETECTION

RESPONSE

WHY THE ELEMENTS OF LAYERED SECURITY ARE IMPORTANT

PREVENTION:

- Cybercrime has shot up by almost 300% since the start of the pandemic.[4]
- Can you afford to be the next victim?

DECTECTION:

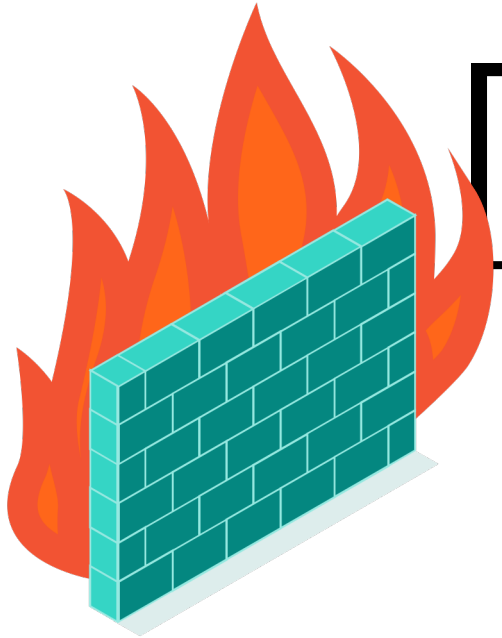
- The average time to identify a breach in 2020 was 228 days.[5]
- Reducing detection time is critical for limiting damage.

RESPONSE:

- In 2020, the average time to contain a breach was 80 days.[5]
- The longer the response time, the greater the impact.

THE 7 LAYERS OF LAYERED SECURITY

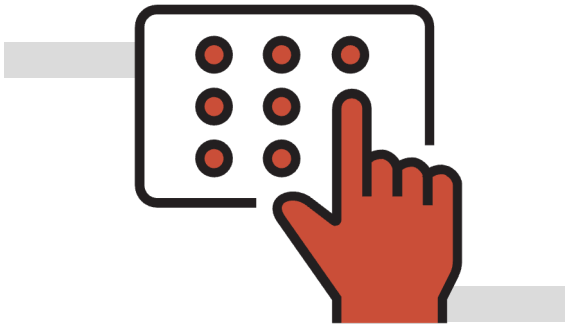
Layered security is divided into seven layers by security experts.



Hackers seeking to get into a system must break through each layer to gain access.

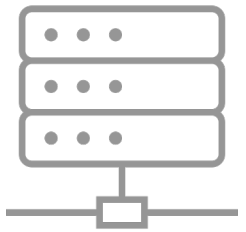
As a result, every information security expert should concentrate on improving these seven layers.

THE 7 LAYERS OF LAYERED SECURITY

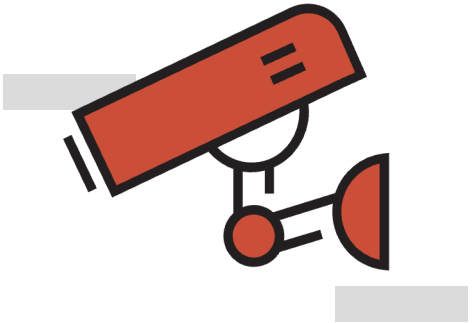


1 Information Security Policies

- Organizations must adopt security policies that prevent unauthorized access.
- Having robust security policies help avoid data breaches and raises security awareness within your organization.



THE 7 LAYERS OF LAYERED SECURITY



2

Physical Security

- Physical security measures, such as fences and cameras, are critical to prevent cybercriminals from breaking in.
- It also helps in the monitoring of employees with access to sensitive systems.

THE 7 LAYERS OF LAYERED SECURITY

3 Network Security

- Only one vulnerability is needed for hackers to get access to the network.
- Hackers can easily break into computers and servers after they have gained access to the network.
- As a result, establishing effective network security measures is essential.

THE 7 LAYERS OF LAYERED SECURITY

4 Vulnerability Scanning

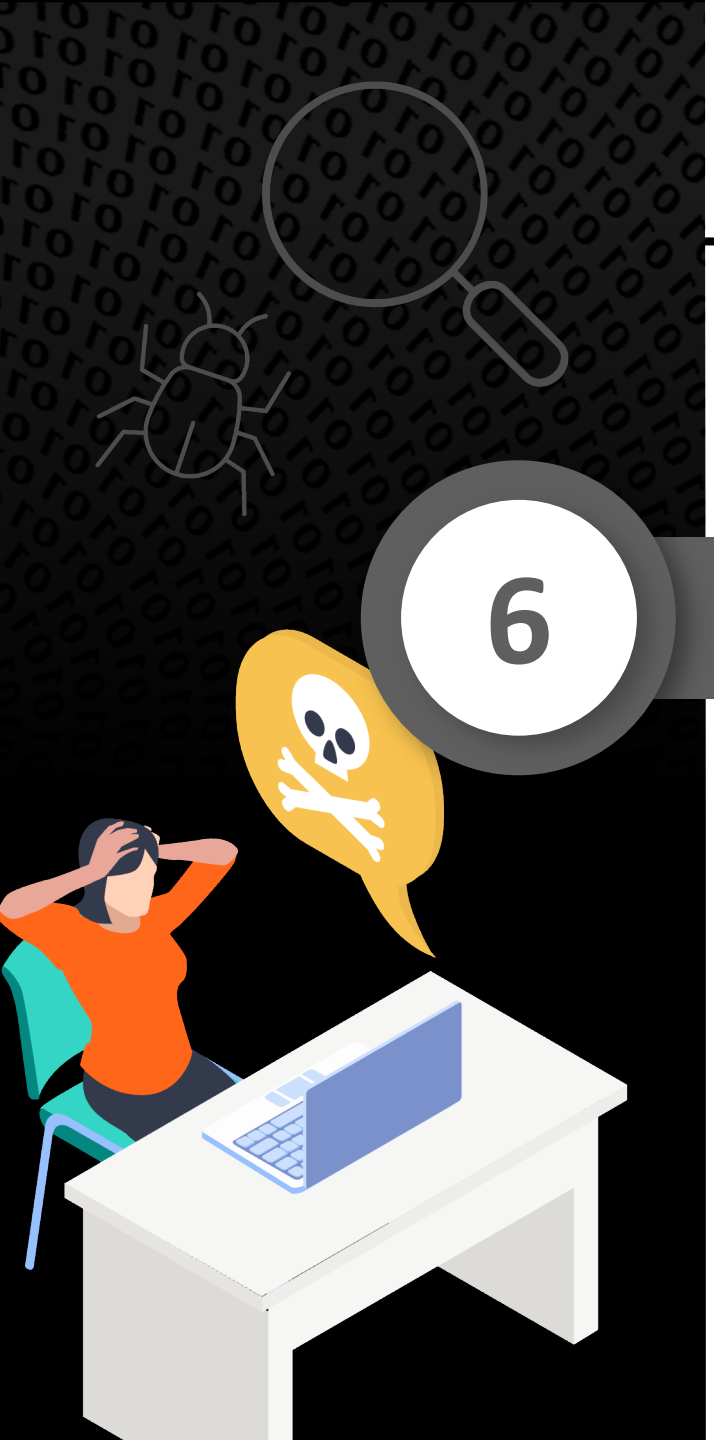
- Vulnerabilities that occur because of factors such as inadequate patch management and misconfigurations open the door for cybercriminals.
- Vulnerability scans help detect missed patches and improper configurations.

THE 7 LAYERS OF LAYERED SECURITY

5 Strong Identity and Access Management (IAM)

- Because of technological advancements, acquiring passwords and hacking into networks is easier than ever.
- IAM restricts access to critical data and applications to certain workers, making unauthorized access hard.

THE 7 LAYERS OF LAYERED SECURITY



6

Proactive Protection & Reactive Backup and Recovery

- Proactive protection detects and fixes security risks before they lead to a full-blown breach.
- The goal of reactive backup and recovery is to recover quickly after an attack.

THE 7 LAYERS OF LAYERED SECURITY

7 Continual Monitoring and Testing

- Failure to regularly monitor and test your backup and disaster recovery strategy is a major oversight.

WHY LAYERED SECURITY IS LIKE AIRPORT TRAVEL

Airport Travel

- At the airport your destination is your terminal.
- After checking in for your flight, you go through security.

Layered Security

- In layered security, the destination is your computer.

- After an email is sent to you, the email goes through your email or system filtering/scanner.

WHY LAYERED SECURITY IS LIKE AIRPORT TRAVEL

Airport Travel

- If what's in your suitcase looks good, it passes through security, and you make your way to your terminal.

Layered Security

- If the email sender and content don't look suspicious, the email makes it to your inbox.

WHY LAYERED SECURITY IS LIKE AIRPORT TRAVEL

Airport Travel

If there's something suspicious or concerning in your suitcase, a bag checker will take another look and review your suitcase's contents.

Layered Security

The bag checker in layered security is your antivirus. Security operations center pulls aside items that look suspicious from the antivirus scan for quarantine until further review.

Q&A

Though layered security is what your organization needs, handling it alone can be challenging.

By collaborating with a partner like us, you can focus on running your organization while we manage your layered security.

Let’s schedule a consultation to move one step closer to a secure future.

THANK YOU