WEB SECURITY

THE BASIC ESSENTIALS

PENTASECURITY.COM

WHY WE NEED
THE BASICS

More than 70 percent of hacking attempts are carried out through the web.

Although it would be ideal if present-day advanced technology and growing IT literacy within the general population meant that successful hacking attempts would decrease, it's just not that easy. Even experts have a hard time implementing an effective web security management strategy because there is no uniform, standardized measure.

Not all companies have an in-house security manager to establish their own security system. This is a pretty difficult task, and without a dedicated security team, companies often outsource the management of parts of the security architecture to third party security solution providers. However even so, few employees without expert security training can configure, operate and maintain a web security product correctly. Without fully understanding web security, it is hard to discern which solution is right for the company's needs in the first place. The result is the introduction of new vulnerabilities due to poor installation and, ultimately, the continuance of attacks.

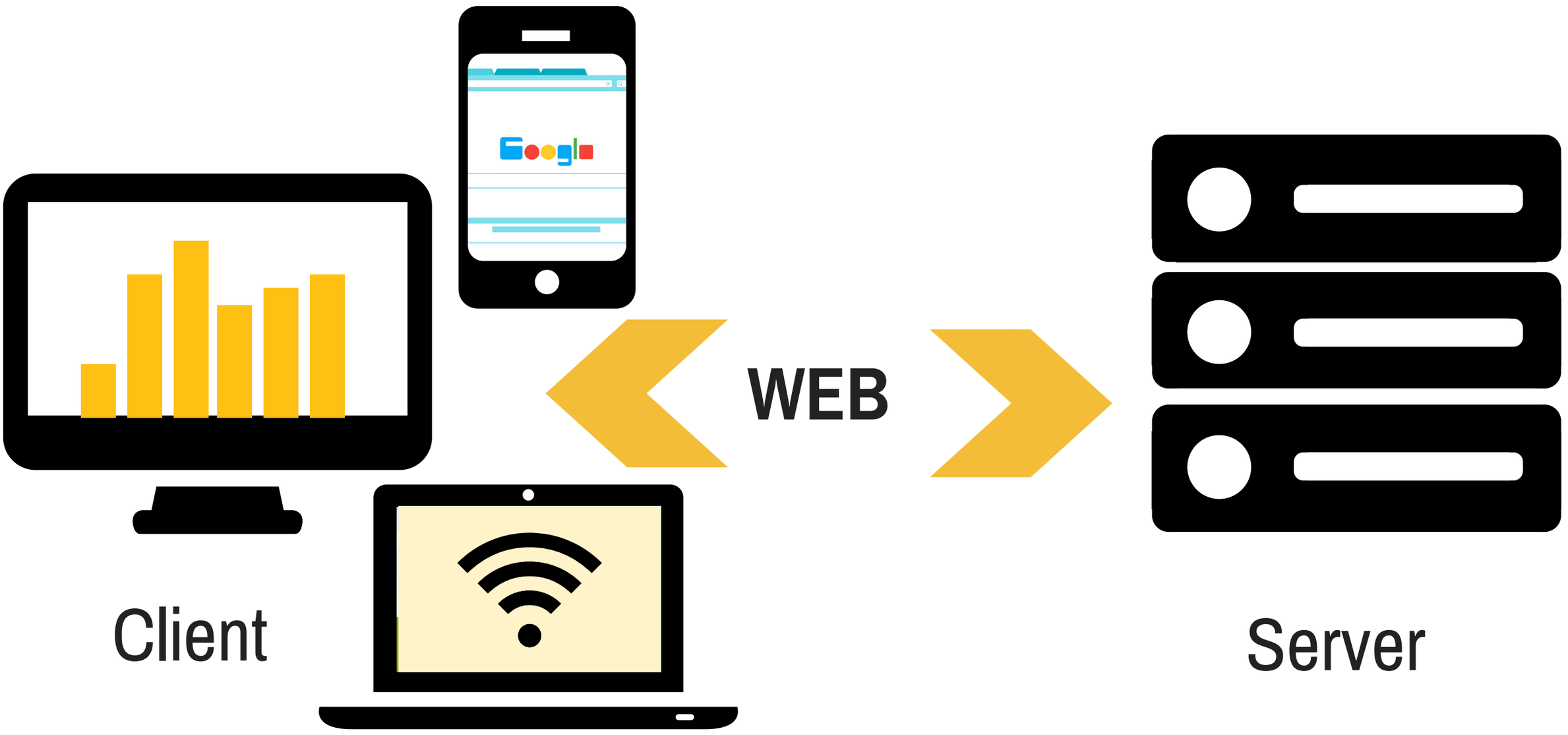
The reality is, to achieve web security,
understanding the IT system is the first – and most essential – step.

HOW WE ACCESS **THE WEB**

While it may seem that we access the web magically, we are simply requesting information and getting information back.

Most of us use desktops, laptops, and mobile devices on a daily basis to access the web. These devices are called “clients.”

The service providers who save web contents like websites and mobile applications, and make them available when clients want to access them are called “servers.”

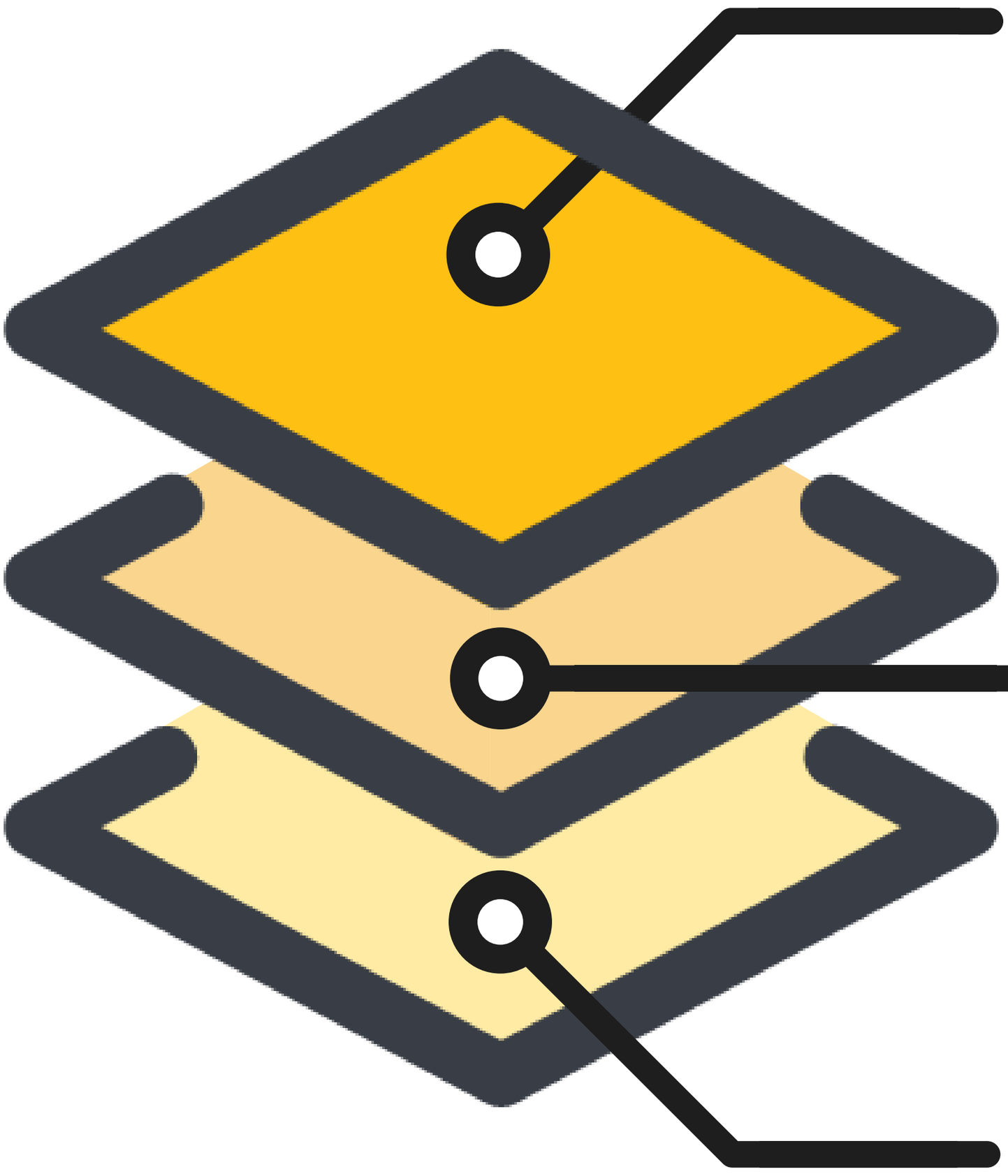


Clients and servers send information back and forth to each other, resulting in what we see as the web.

Simply put, **the web is the network that connects clients and servers.**

THE IT-SYSTEM

STRUCTURE



APPLICATION

Provides protocol (HTTP, FTP) and application services.

SYSTEM

Platform that various applications can run on, like operation systems.

NETWORK

Servers communicate with each other to send and receive data.

An IT system, therefore, consists of a **network** layer, a **system** layer, and an **application** layer. These three layers interact with one another to make IT systems work.*

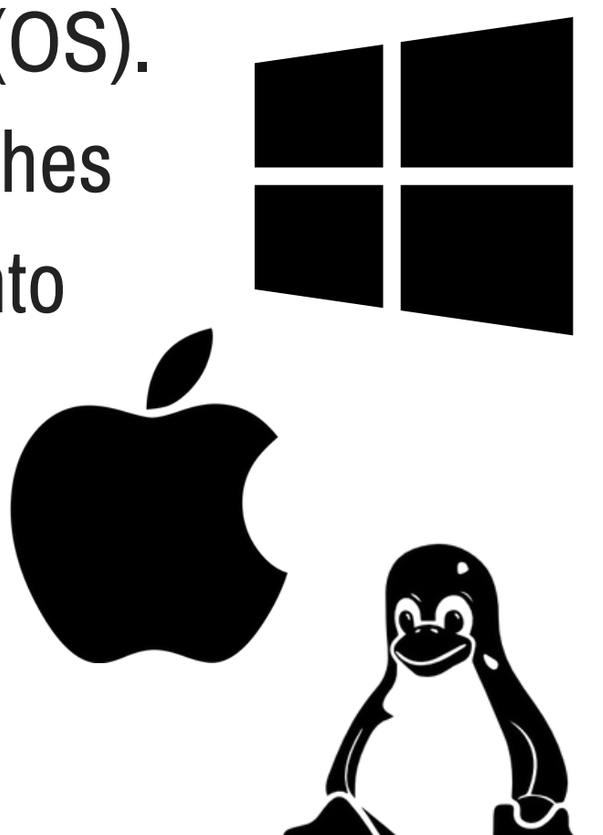
Let's take a closer look at network and system security.

** These three layers break up into more detailed layers, resulting in the 7-layer OSI model*

For network security, IPs and ports that are unsafe have to be secured through access control and proper authorization protocols. Traffic coming through allowed IPs or ports must also be checked.

Hence, many companies install firewalls or intrusion detection/prevention systems (IDS/IPS). However, a firewall can't block attacks from safe IPs and ports, and even IDS/IPS have their limits since they often have no insight into application layer traffic.

System security is mostly related to operating systems (OS). OS manufacturers prepare for threats with security patches and updates. However, malicious code may still enter into the system through unpatched vulnerabilities between updates. Therefore, security managers still have to continuously scan for malicious code.



Companies will usually attempt to mitigate issues by installing anti-virus solutions. But these only work against file-level threats and are unequipped for dealing with custom web application vulnerabilities.

WHAT ABOUT THE APPLICATION LAYER?

The application layer is much more diversified, making securing the different types of applications challenging. Many are weary of dealing with this layer but ironically, the most neglected part of security is actually the most important.

THE CORE OF SECURITY

APPLICATIONS

All of the web that we use is composed of web applications. Websites, mobile apps – these are all web applications.

Attacks on web applications cause the most damage, which is why more than 90% of all attacks are aimed at this layer. If you really want top-notch security, you need to secure the web application.

But because of the difficulty and complex nature of this layer, there aren't too many companies that are installing appropriate security solutions in this area.

Real application security has to start from the development stage all the way to the maintenance stage after the initial building is done.

Building good security, therefore, is much like building a house.

BUILDING THE **SECURITY SYSTEM**

For adequate protection, you need solid bricks. That's why secure coding is crucial to ensure all codes that may be vulnerable are excluded.

Web scanners check the application from outside, like checking the exterior for cracks when a house is finished.

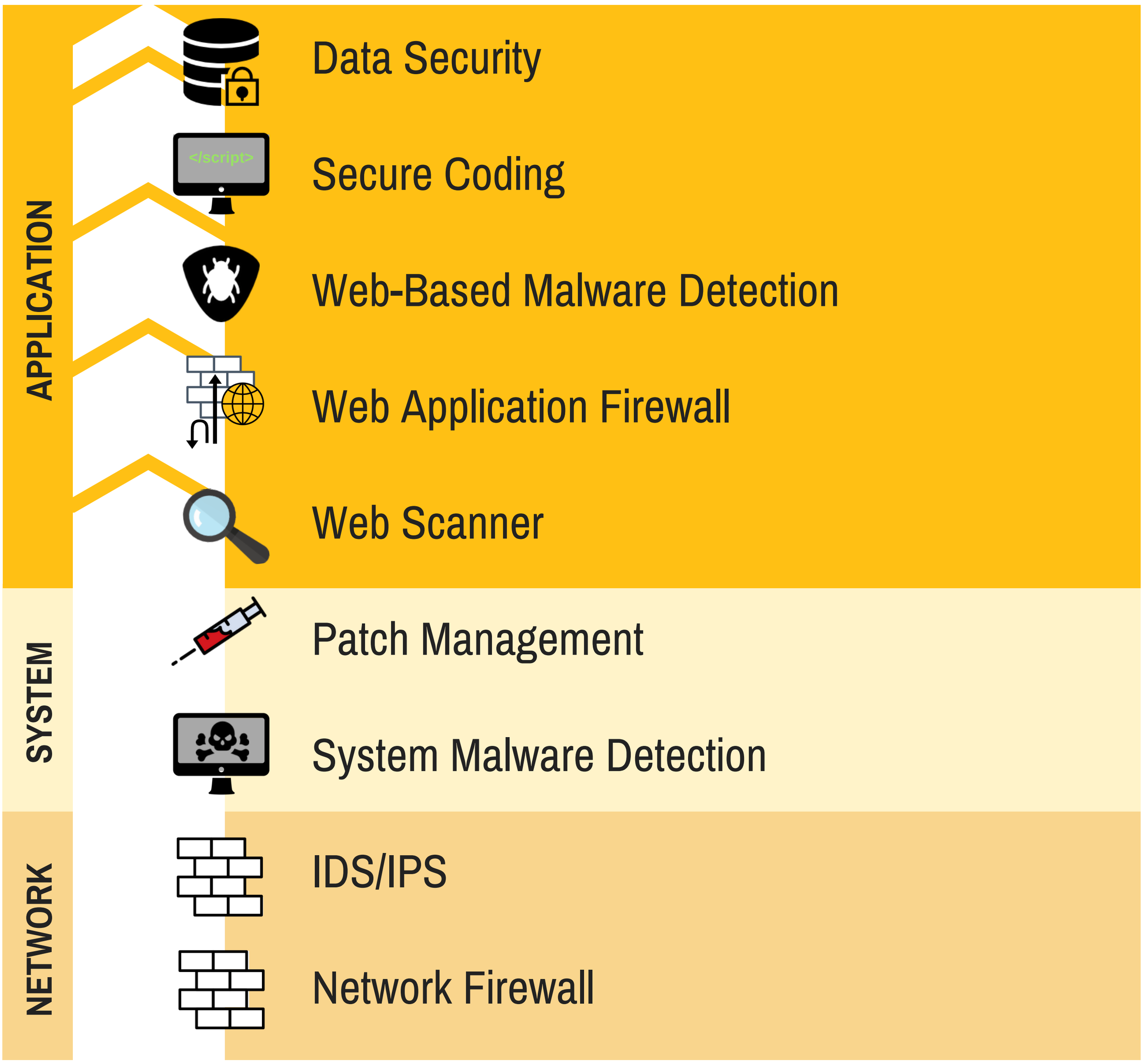
Once inside, you need to check for leaks. Web-based malware detection solutions do internal inspections of applications.

After you're done, you need a fence to keep out intruders. The WAF will keep malicious code out, allowing only safe code.

Finally, valuables inside need to be kept safe. Data security makes sure any sensitive information will be kept in encrypted form.

THE SPAN OF **WEB SECURITY**

As you can see, web security is easy to understand if you divide it up and visualize it in ways that are more accessible. Now, if solutions were put into one image according to the layers, it would look like this:



Each layer is unique, and different solutions pertain to different layers. So where do you start?

GETTING RID OF
THE WEAKEST LINK

While the application layer is the core and should be focused on in terms of implementing solutions, it's important to remember that at the end of the day, an organization's security is only as strong as its weakest link.

> **"AN ORGANIZATION'S SECURITY IS ONLY AS STRONG AS ITS WEAKEST LINK."**

Even with one weak solution within any of the layers, an entire system can go awry. Individuals and enterprises alike need to be aware of the variety of solutions that pertain to specific layers.

As the world continues to become more and more data and web-oriented, our reliance on information will only make us more vulnerable if there are holes in the security system.

But the good news? Comprehensive web security is achievable and should be made a priority, **even if it's just one step at a time.**

RESOURCES

FOR STARTING OUT

Getting started can seem like a chore, but here are a few easy and free ways to get a step ahead on your security:

OBSERVATORY by mozilla

Observatory is a free tool designed for developers, administrators, and security professionals to test their websites for vulnerabilities.

cloudbric

Cloudbric is a cloud-based web security service, offering a Web Application Firewall (WAF), DDoS protection, SSL and CDN in a full-service package. It is free for up to 4GB of traffic each month.

MyDiamo

MyDiamo is an open-source database encryption solution for MySQL, MariaDB, and PerconaDB. Free licenses are available for one month, and are renewable upon request.