Module 5

By

Sunil Kumar S

Cyber Security – Need of the Hour

- It’s a Virus Attack , Literally!
- The word ‘Virus’ is used in a specific context in the world of computers, software, and the internet.
- It is an unwanted set of commands designed to unsettle the operating system of users’ devices.
- No one knows who makes the viruses and what exactly the makers want in return.
- But anyone and everyone using electronic devices are under constant threat of a virus attack.
- Of course, there are several proactive and corrective measures that can be taken to minimise the damage; but none of them can promise a complete protection or complete recovery.

Cyber Security – Need of the Hour

- All of this now sounds relatable like never before. Despite centuries of research and advancement in medical science, humankind is still under the threat of some unknown virus attack.
- The recent outbreak of Coronavirus (COVID-19) has challenged our belief that we can predict the future and plan our own lives.
- This unwanted virus has unsettled the routine operations of every nation across the world.
- Not a single sector is left unaffected, thanks to this global **health crisis**.
- To be specific, all businesses and markets were abruptly shut down after the Government(s) decided to restrict human contact by declaring a nation-wide LockDown!
- Schools, colleges, offices, and all other establishments were closed.
- Travel within and outside the cities, villages, and states was restricted, rather stopped for perhaps the longest duration in history.
- Public transport facilities such as buses, trains, and air travel were discontinued with immediate effect.
- Colonies and areas were sealed to contain the spread of Coronavirus.
- The world, it seems, was not at all prepared for such a virus attack.

Health Crisis & The Internet

- Covid -19 changed the way we use internet
- Pre-Covid
  - E-Mail – were considered as corporate mode of communication
  - Social Media – was considered as Youth's Domain
  - Virtual Meetings for Official Purposes Only (even people were not comfortable)
- Covid-Period & Post-Covid
  - Lockdown Forces
  - People rely on Internet Like never Before
  - Video Calls to Stay in Touch with each other
  - No Hard Copy of NewsPapers due to lockdown
  - Online Portal for News & Social Media for latest updates
    - Risk of Fake News
  - Online Classes
  - Local Grocery Shop started accepting order online via Whatsapp
  - Restaurants switched from Dine-in to Home-Delivery facilitated by third party online platforms (Swigy, Zomato)

Changing Landscape of Cyber Security & Cyber Crimes

- Pre-Covid – corporate were too conscious about data security
- Due to Covid-Lockdown
  - Work from Home Concepts emerges
  - Dependent on Public Internet to access their Organization Private Network
  - More people started use Internet for Personal / Official Purposes
  - People from All age groups were exposed to Cyber World (Internet)
  - No time for proper training for all people before they start using Internet in safe mode
    - Hence Many People became easy target for cyber attacks

Changing Landscape of Cyber Security & Cyber Crimes

- While world was busy in handling unforseen challenges posed by Pandemic
- Cyber Criminals busy in developing and boosting their attacks at alarming rate
- Unstable Social & Economic situation exploited by the Cyber Criminals
- Increasing Online Transactions
  - Crated new opportunities for cyber attacks
  - With many business & Individuals not ensuring their cyber defenses
  - Work from Home model is now becoming an opportunity for the cyber criminals to exploit people through e-mail scams, hacking passwords, phishing, ransom attacks, online harassment

Cyber Crimes to Cyber Warfare – Everybody is at Risk

- Although its difficult to guess the number of ways cyber-crimes are committed
- Few common pattern here to start with
- Example - Cyber Criminals take advantage of unattended bugs to break into the system.
  - When they use new unknown bug, its called zero day attack.
  - In other cases, they break in using known bugs that developers or users have not bothered to patch or fix.
  - Another Example is cyber attacker tricks the people to share their OTP & other login credentials.
  - Another Example – installing Harmful software, known as malware or virus

Cyber Crimes to Cyber Warfare – Everybody is at Risk

- Cyber Criminals usually target individual or companies, with an intention of stealing money or company secrets.
- But in few cases, a cyber attack might be targeted at a larger group – say an **entire country.**
- In such cases, certain information & Privacy are not the only things at risk.
- Some cyber attacks are aimed to destruction & damage at a large scale.
- If some country directs such an attack at another country, it is considered to be an act of **cyber warfare**
- This includes hacking govt websites with an intention to malign the country image globally.
- Cyber warfare also aims at stealing confidential information regarding armed forces & defense strategies of the target county
- Fake News

Cyber Security – Need of the Hour

- Every Industry Govt or Private
  - Highly depending on Internet
- Cyber Security plays an important role in the filed of Information Technology
  - Securing the information & Transactions has emerged as one of the biggest challenges in the current times.
- Use of Internet has increased
  - Online Food
  - Education Sector
  - Entertainment everything has became online.
- In one side technology is good but another end comes with security issues (more vulnerable to cyber attacks).
- Bigger Need for cyber security awareness in order to protect the users from online frauds & cyber crimes.
- Cyber Security professionals are in huge demand & is the most lucrative career options.

What is Cyber Security

- Several Definitions are there
- Cyber Security is the preservation through policy technology & education of the availability, confidentiality and Integrity of Information and its underlying infrastructure so as to Enhance the Security of Person both Offline & Online

CIA TRIAD

- In order to define the Cyber Security one needs to understanding of the significance of the 3 foundational information security principles;
- Confidentiality
- Integrity
- Availability
- Known as CIA TRIAD

CIA TRIAD

- Confidentiality
  - Information is not Disclosed to unauthorized Individuals
- Integrity
  - Ensuring accuracy and Completeness of Data
- Availability
  - Users must have information when they need it

CIA Triad

- The CIA Triad is a central tenant of ISO/IEC 27001:2013 (ISO 27001), the international standard that describes best practice for an ISMS (information security management system).
- ISO 27001 neatly summarizes Information security as the maintenance of confidentially, availability and integrity of the confidential assets of an organization CIA Triad is a model designed to guide policies for information security.
- It provides us with a reference to evaluate and implement secure information systems, independently of the underlying technologies.
- Each one has specific requirements and processes.

CIA Triad

- CIA Triad is aimed at protecting the organization's digital assets against the ever-growing Cyber-attacks.
- This can be ensured by deploying appropriate security controls to provide several security features such as deterrent, prevention, and detection of Cyber-crimes.
- In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.
- Lets look at components of CIA Triad individually.

Confidentiality

- Confidentiality is roughly equivalent to privacy.
- Confidentiality ensures privacy to the sensitive information while it is in transit over a network.
- Proactive measures undertaken to ensure confidentiality are designed to prevent sensitive information from unauthorized people / processes, while making sure that only authorized people and only to the intended parties have access to it.
- The malicious actors must not intercept the data to use it for nefarious purposes.
- It is common for data to be categorized according to the amount and type of damage that could be done should it becomes accessible to authorized people / processes.

Confidentiality

- There are various implementations which can be incorporated to ensure the confidentiality of data.
- Safeguarding data confidentiality involves special trainings for those needs to access and work on sensitive data.
- These training would typically include understanding of security risks that could compromise the Confidentiality.
- Training can help users to get familiarize with risk factors and how to safeguard against common attacks.
- Further aspects of training should include password-related best practices and information about social engineering methods, to prevent users from bending data-handling rules with good intentions and potentially disastrous results.

Confidentiality

- An example of methods used to ensure confidentiality is an account number or token number when banking online.
- Cryptography is the best solution in this regard. Data encryption is one of the most common and robust method of ensuring confidentiality.
- The encryption mainly ensures the confidentiality of sensitive data. It converts the plaintext of data into the Cipher-text, which is an unreadable form for humans. Cipher text can only be understood by the authorized entities.

Confidentiality

- Encryption might involve one of the two vital security controls either Symmetric Encryption or Asymmetric Encryption.
- User IDs and passwords constitute a standard procedure; two-factor authentication is also being implemented in most online banking transactions.
- Other options include biometric verification and security tokens, soft or hardware tokens.
- Users can also take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a transaction.

- Anand Shinde. Introduction to Cyber Security : Guide to the World of Cyber Security (p. 43). Notion Press. Kindle Edition.

Confidentiality

- Extra measures might be taken in the case of extremely sensitive data,
- such as storing only on air gapped computers and networks, disconnected storage devices for highly sensitive information, in hard copy form only.
- In addition, user can also use Steganography to hide data into another type of data such as images, audio, or video files.
- Hidden sensitive data in large media files is much difficult to compromise.
- Confidentiality should ensure that
  - Data should be handled based on their required privacy.
  - Data should be encrypted, with a form of two-factor authentication to reach it.
  - Keeping Access Control Lists and Other File Permissions up to date.

Integrity

- **Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.**
- **Integrity refers to preventing data from being tampered with, modified, or altered in malicious way to achieve malicious goals.**
- **That means data which is sent must be received intact and unaltered by an authorized party.**
- **Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (a breach of confidentiality).**
- **Integrity is essential for data whether it is in transit or it is in a storage media.**
- **Data integrity is crucial for E-commerce and business websites.**

Integrity

- These measures include file permissions and user access controls.
- Version control may be used to prevent erroneous changes or accidental deletion by authorized users from becoming a problem.
- Various attacks that compromise data integrity include a Man-In-the-Middle (MITM) attack, penetrating into the web server, and introducing malicious code in databases.
- In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash.

Integrity

- Use of Hashing Algorithms such as MD5 and SHA1 are normally provided by developers in order to check the integrity of data.
- Other techniques include certificates, digital signatures, and non-repudiation.
- Some data might include checksums, even cryptographic checksums, for verification of integrity.
- Backups or redundancies must be available to restore the affected data to its correct state.

Integrity

- Integrity should ensure that
- 1. Employees are knowledgeable about compliance and regulatory requirements.
- 2. Use a backup and recovery software.
- 3. To ensure integrity, make use of version control, access control, data logs and checksums.

Data Availability

- **Availability is also a security service which ensures the constant availability of resources and services to only authorized parties in a timely manner.**
- **Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts.**
- **Reliable hardware must be maintained in order to provide constant services to a large number of customers in any organization.**
- **There must be less downtime during upgrades and backup of sensitive data in external drives will be helpful in case of data loss.**
- **It's also important to keep up with all necessary system upgrades.**

Data Availability

- Providing adequate communication bandwidth and preventing the occurrence of bottlenecks are equally important.
- Quick disaster recovery plans should be followed in worst case scenarios.
- Other important security controls for availability include data backup, patching, and redundant systems.
- Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues occur.

Data Availability

- Fast and adaptive disaster recovery is essential for the worst-case scenarios; that capacity is reliant on the existence of a comprehensive Disaster Recovery Plan (DRP).
- Redundancy ensures fault tolerance.
- It means, when a primary system fails to perform, the secondary system is available to continue the delivery of functions and services.
- In this case, security analysts redirect all traffic or workload to a backup system.
- Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire.
- To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe.

Data Availability

- Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data blocked by malicious denial-of-service (DoS) attacks and network intrusions.
- Availability
  - Use preventative measures such as redundancy, failover and RAID. Ensure systems and applications stay updated.
  - Use network or server monitoring systems.
  - In case of data loss, ensure a Data Recovery and Business Continuity plan is in place.

Application Security

- Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.
- Application security describes security measures at the application level that aim to prevent data or code within the app from being stolen or hijacked.
- It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect apps after they get deployed.

Application Security

- Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities.
- Application security is important because today's applications are often available over various networks and connected to the cloud, increasing vulnerabilities to security threats and breaches.
- There is increasing pressure and incentive to not only ensure security at the network level but also within applications themselves.

Types of Application Security

- Different types of application security features include
- authentication,
- authorization,
- encryption,
- logging, and
- application security testing.
- Developers are always trying to code applications to reduce security vulnerabilities.
- They achieve this by releasing newer versions of the applications as they find and fix the bugs within the existing applications.

Authentication:

- Authentication: When software developers build procedures into an application to ensure that only authorized users gain access to it.
- Authentication procedures ensure that a user is who they say they are.
- This can be accomplished by requiring the user to provide a user name and password when logging in to an application.
- Multi-factor authentication requires more than one form of authentication—the factors might include
- something user know (a password),
- something user have (a mobile device - OTP), and
- something user is (a thumb print or facial recognition).

Authorization

- Authorization: After a user has been authenticated,
- the user may be authorized to access and use the application.
- The system can validate that a user has permission to access the application by comparing the user's identity with a list of authorized users.
- Authentication must happen before authorization so that the application matches only validated user credentials to the authorized user list.

Encryption

- Encryption: After a user has been authenticated and is using the application, other security measures can protect sensitive data from being seen or even used by a cybercriminal.
- In cloud- based applications, where traffic containing sensitive data travels between the end user and the cloud, that traffic can be encrypted to keep the data safe.

Logging & Application security testing

- Logging: If there is a security breach in an application, logging can help identify who got access to the data and how.
- Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.
- Application security testing: A necessary process to ensure that all of these security controls work properly.

Application security in the cloud

- Application security in the cloud: Application security in the cloud poses some extra challenges.
- Because cloud environments provide shared resources,
- special care must be taken to ensure that users only have access to the data they are authorized to view in their cloud-based applications.
- Sensitive data is also more vulnerable in cloud-based applications because that data is transmitted across the Internet from the user to the application and back.

Mobile application security

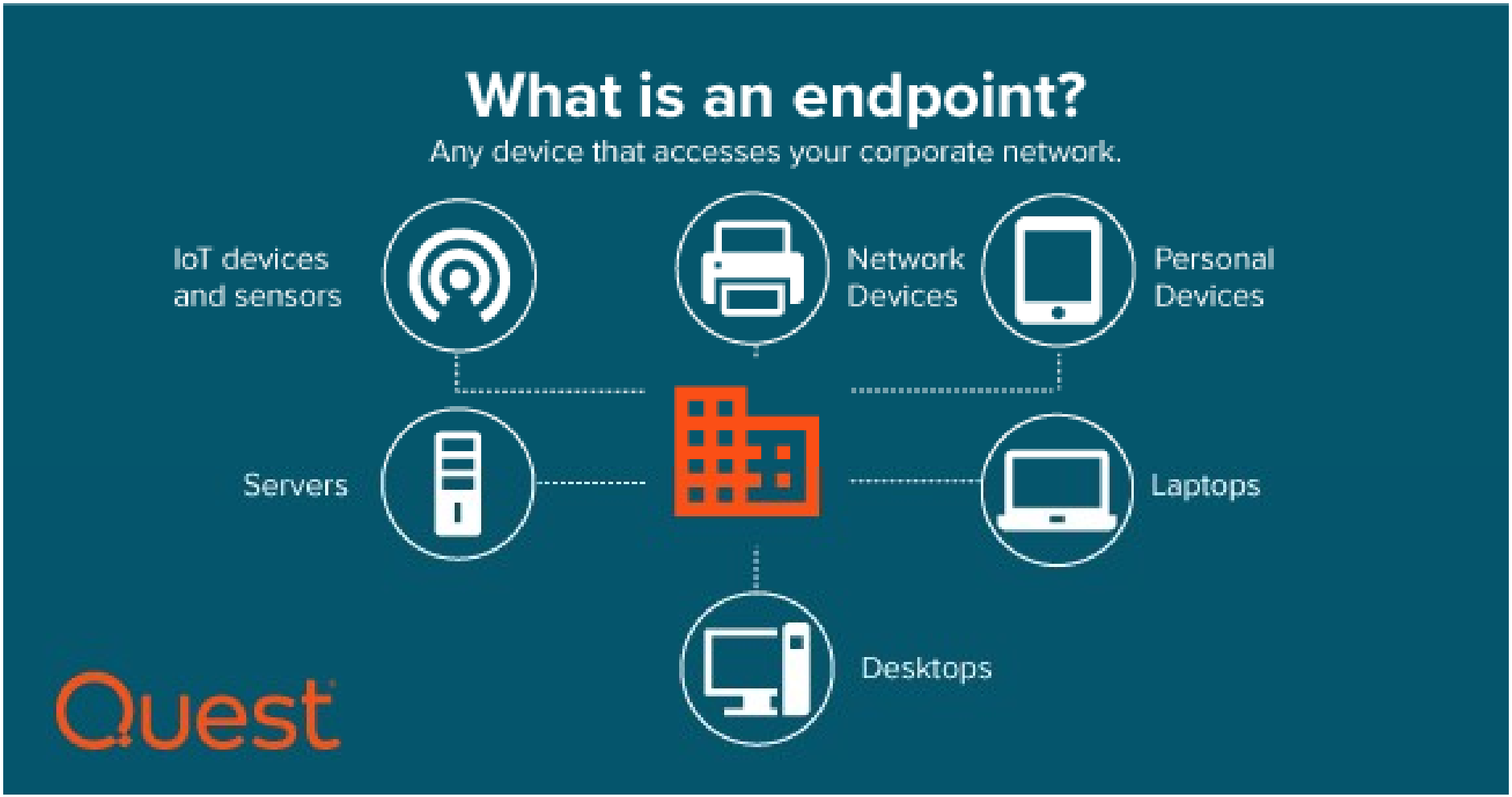
- Mobile application security: Mobile devices also transmit and receive information across the Internet, as opposed to a private network, making them vulnerable to attack.
- Enterprises can use virtual private networks (VPNs) to add a layer of mobile application security for employees who log in to applications remotely.
- IT departments may also decide to vet mobile apps and make sure they conform to company security policies before allowing employees to use them on mobile devices that connect to the corporate network.

Web application security

- Web application security: Web application security applies to web applications—apps or services that users access through a browser interface over the Internet.
- Because web applications live on remote servers, not locally on user machines, information must be transmitted to and from the user over the Internet.
- Web application security is of special concern to businesses that host web applications or provide web services.
- These businesses often choose to protect their network from intrusion with a web application firewall.
- A web application firewall works by inspecting and, if necessary, blocking data packets that are considered harmful.

Endpoint security

- Endpoint security refers to securing endpoints, or end-user devices like desktops, laptops, and mobile devices which are connected to the corporate networks.
- Endpoints serve as points of access to an enterprise network and create points of entry that can be exploited by Cyber Criminals.


What is an endpoint?
Any device that accesses your corporate network.
IoT devices and sensors
Network Devices
Personal Devices
Servers
Laptops
Desktops
Quest

Endpoint security

- **Any device, such as a smartphone, tablet, or laptop, provides an entry point for attacker.**
- **Endpoint security aims to adequately secure every endpoint connecting to organization's network to block access attempts and other risky activity at these points of entry.**
- **As more enterprises adopt practices such as BYOD (Bring Your Own Device) and remote / mobile employees, the enterprise network security perimeter has essentially dissolved.**
- **With the proliferation of mobile devices like laptops, smartphones, tablets, notebooks etc., there has been a sharp increase in the number of devices being lost or stolen as well.**
- **These incidents potentially translate as huge loss of sensitive data for enterprises which allow their employees to bring in these mobile devices (enterprise-provided or otherwise) into their enterprise.**

Endpoint security

- **Endpoint security solutions often use a client-server model of protection, employing both a centrally managed security solution to protect the network as well as client software locally installed on each endpoint used to access that network.**
- **Some work on a SaaS (Software as a Service) model, by which both central and endpoint security solutions are maintained remotely.**
- **It also helps organizations successfully prevent any misuse of their data which they've made available on the employee's mobile devices.**
- **Example: a disgruntled employee trying to cause nuisance to the enterprise or someone who may be a friend of the employee trying to misuse the enterprise data available on the device.**

Endpoint security

- Every device which can connect to a network poses a considerable danger.
- And as these devices are placed outside of the corporate firewall, on the edge of the network using which individuals have to connect to the central network, they are called as endpoints.
- Meaning endpoints of that network.

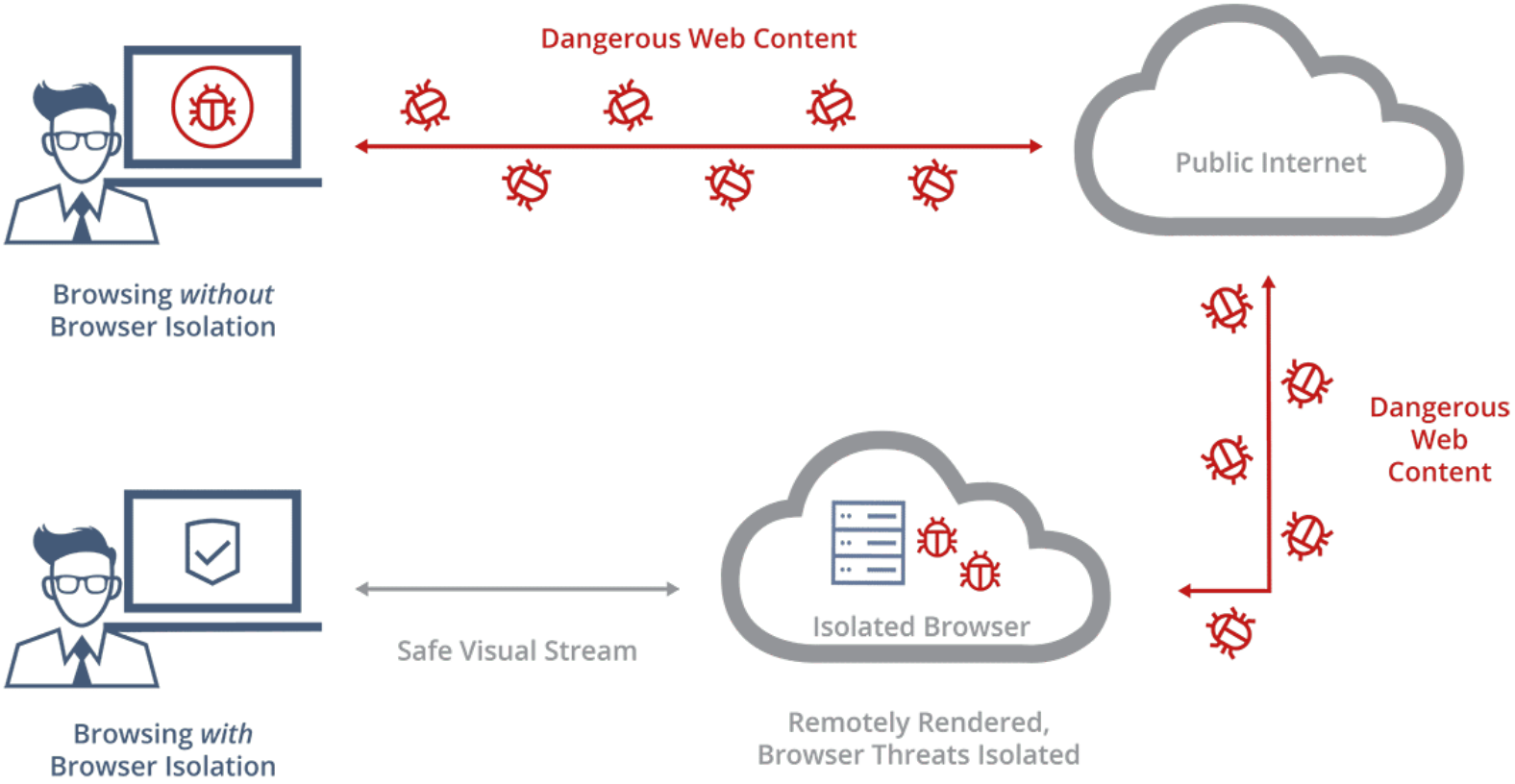
Antivirus vs Endpoint security

- Antivirus
  - Runs on PC or Devices
- Endpoint Security
  - Firewall
  - A host intrusion prevention system (HIPS) is an approach to security that relies on third-party software tools to identify and prevent malicious activities
  - Monitoring Tools

Types of Endpoint Security

- Antivirus Solutions
- Application Control
  - Backlisting
  - Whitlisting
  - What Application can do / can't do
  - APP Permission
- Network Access Control
  - MAC Filter
- EndPoint Firewall
- HIPS
  - Rule Based HIPS
  - Halting application which violates the rules and detect the intrusion
- URL Filtering
- Browser Isolation
  - Deleting Session data after use (Cookies)

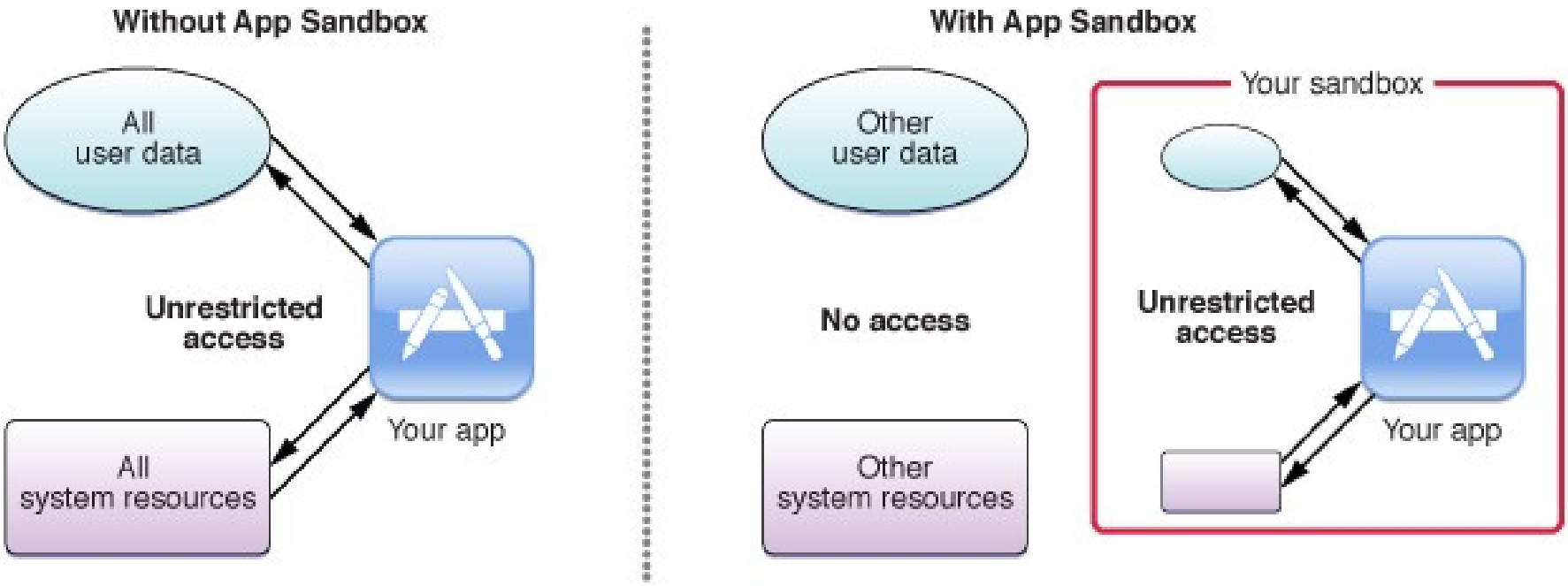
Browser Isolation



Types of Endpoint Security

- Cloud Perimeter Security
- Endpoint Encryption
- Sandboxing
  - Isolated Environment
- Secure Email Gateway
- IoT Security

Sandboxing


Without App Sandbox
All
user data
Unrestricted
access
Your app
All
system resources
With App Sandbox
Other
user data
No access
Other
system resources
Your sandbox
Unrestricted
access
Your app

Mobile Security

- Security threats on mobile devices
  - Device lost or theft
  - Application Security
  - Data leakages
  - Unsecured Wi-Fi
  - Phising Scams
  - Malicious Apps
  - Network Spoofing
  - Spyware
  - Bluetooth security issues
  - Mobile Device Management
    - Goolge familty suite
    - Secure Browser
    - Secure Email
    - Secure Docs
    - Secure APP Catalog

Data Security

- **Biggest challenge for facebook, whatsapp, instagram apps**
- **Data Encryption**
- **Data Masking**
  - **Credit card number first 12 digit masked**
- **Data eraser**
  - **There are times when data that is no longer active or used needs to be erased from all systems. For example, if a customer has requested for their name to be removed.**
- **Data resilience**
  - **Backup**
- **Authentication or Authorization**
  - **Access Control List**
  - **Role based Access Control List**
- **Data Security Standards**
  - **GDPR: General Data Protection Regulation.**
  - **PCI: The Payment Card Industry Data Security Standard**
  - **HIPAA: The Health Insurance Portability and Accountability Act (HIPAA)**
  - **ISO/IEC 27001: ISO/IEC 27001 formally specifies an Information Security Management System**
  - **FIPS**
  - **NERC**
  - **ANSI / ISA 62433**

Authentication

- Authentication is the process of recognizing a user's identity.
- It's the process of determining whether someone or something is, in fact, who or what it declares itself to be.
- It is the mechanism of associating an incoming request with a set of identifying credentials.
- Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.
- User ID – used for identification
- Password – validating the identification

Authentication

- permitted access to a protected resource or system.
- Generally speaking authentication has three tasks:
- Manage the connection between the human (user) and the physical server (computer).
- Verify users' identities. Approve (or decline) the authentication so the system can move to authorizing the user.
- HTTP vs HTTPS – Stateless
- Authentication for each session
- The authenticating system issues a signed authentication token to the end-user application, and that token is appended to every request from the client.

Authentication Server:

- Authentication Server: An authentication server is an application that facilitates authentication of an entity that attempts to access a network.
- Such an entity may be a human user or another server. An authentication server can reside in a dedicated computer, an Ethernet switch, an access point or a network access server.
- An authentication server is a database that stores user credentials—username and password—and typically group and attribute information.

Authentication Server

- Windows NT Domain, Active Directory, RADIUS, LDAP, NIS, RSA ACE/Server, SAML Server, and eTrust SiteMinder, and enables organizations' to create one or more local databases of users who are authenticated.
- In a more sophisticated system called Kerberos, the subscriber must request and receive an encrypted security token

Authentication Factors

- Knowledge:
  - User ID
  - Password
  - Pin
- Possession: This factor consist of anything a user must have in their possession in order to log in; this category includes access cards, one-time password tokens, or smartphone apps, employee ID cards and SIM card-based mobile phones etc.
- Inherence: This include any inherent traits the user has that are confirmed to identity; this category includes the biometrics features of user such as: Retina scans, Iris scans, Fingerprint scans, facial recognition, voice recognition.

Additional Factors - Supplemental Authentication Factors

- Additional Factors - Supplemental Authentication Factors. There are as below.
- **Location:** User location is sometimes considered a fourth factor for authentication. Now days most smartphones are equipped with GPS, enabling reasonable surety confirmation of the login location.
- **Time:** This factor consist of “When user is authenticating.” Like the location factor, the time factor is not sufficient on its own, but it can be a supplemental mechanism for weeding out attackers who attempt to access a resource at a time when that resource is not available to the authorized user.

Additional Factors - Supplemental Authentication Factors

- **Device:** In most organizations' users are given company assets, such as Laptops, desktops, Tablet PCs, Smart phones etc. The users are expected to use these devices only to access the organizations' resources.
- **single sign-on (SSO) :**Forcing user to authenticate at every step can overwhelm and frustrate the user. To avoid this in large organizations, authentication may be accomplished using a single sign-on (SSO)

Single-Factor Authentication (SFA)

- Single-Factor Authentication (SFA): Single-factor authentication is the simplest form of authentication methods.
- With SFA, a person matches one credential to verify himself or herself online.
- The most popular example of this would be a password (credential) to a username. Most verification today uses this type of authentication method. The traditional user authentication process for accessing computer resources.
- Risks of Single-factor Authentication:
  - Weak Password
  - reuse the same password across multiple accounts, which is also known as Password Reuse.

Two-Factor Authentication (TFA)

- Sometimes called 2-step verification or dual factor authentication.

Two-Factor Authentication (TFA)

- OTP
- Biometric

Two-Factor Authentication (TFA)

How does two-factor authentication work? Here's how the process breaks down step-by-step:

1. The user is prompted to log in by the website or application.
2. The user enters what they know. This is usually a traditional username and password combo. The site's server finds a match and recognizes the user. This step relies on the knowledge factor.
3. For processes that don't require passwords, the website generates a unique security key for the user. The authentication tool processes the key, and the authentication server validates it.
4. The site then prompts the user to initiate the second login step. Although this step can take a number of forms, users have to prove that they have something only they would have, such as a security token, ID card, smartphone or other mobile device. This step relies on the possession factor.

Two-Factor Authentication (TFA)

5. Then, the user enters a one-time code that was generated during step four. Some services use additional security measure such as time factor where in the user has to enter the password within 30 seconds or a minute. Failing to do so will take the user back to first step.

6. After providing both factors, the user is authenticated and granted access to the application or website.

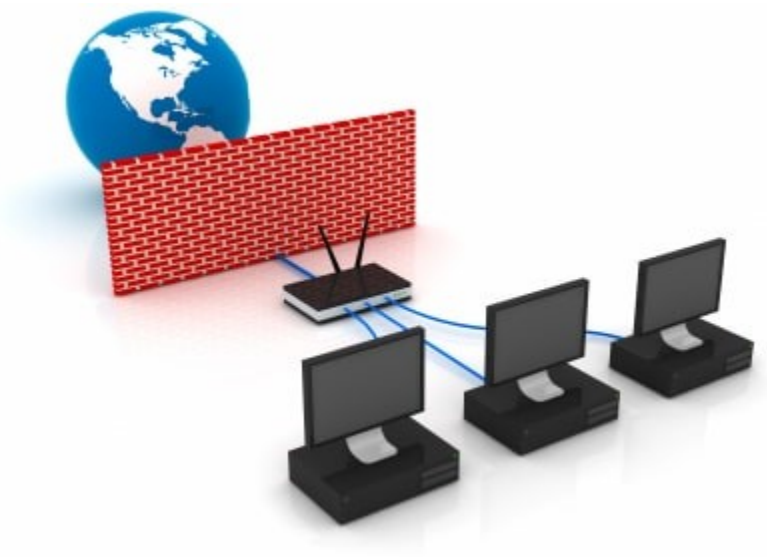
Two-Factor Authentication Products:

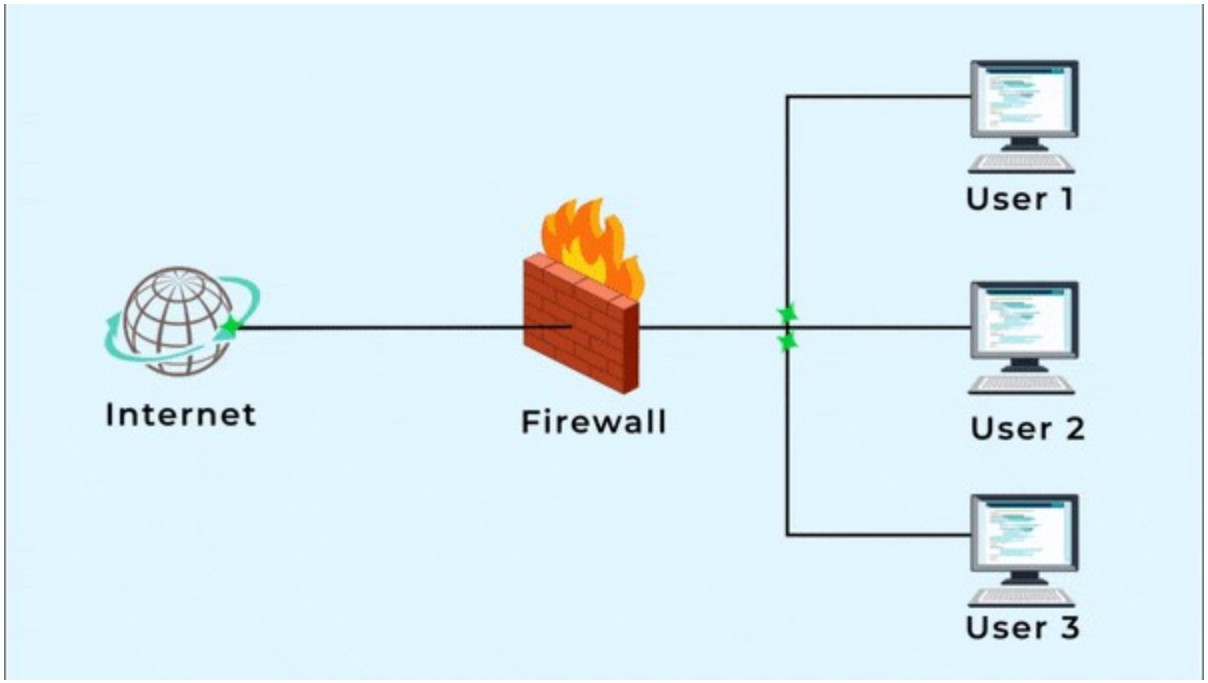
- Hardware Tokens
  - Pen Drive
  - Biometric
  - Access Cards (ATM Cards)
- Software Tokens
  - Google Security Code for gmail login
  - OTP

Multi Factor Authentication

- Something user is – Finger Print, Retina or Iris Scan, Face recognition, voice recognition.
- Something user has – Hard Token, Access / Smart card, USB Authentication token.
- Something user know – Password, Pin number.
- Something user do – Signature, hand writing pattern, wipe stroke on cell phone,
- Somewhere user is – Location (GPS), Time-zone

Firewall





Firewall

- Internet is a Public Network. Being a public network used by people with good intensions and bad intensions.
- To protect computer from people with bad intensions a firewall is used.
- When surfing the internet there are many dangers in the form of malware that are trying to harm computers. Hackers all trying to gain access to every computer connected to Internet.
- Just like a security fence around a building protects home from burglars and intruders; a firewall keeps Cyber criminals and hackers from penetrating computers.

Firewall

- A firewall's purpose is to create a safety barrier between a private network and the public internet.
- A firewall acts as a defense system for a network against viruses, worms, Trojans, brute force attacks and other network attacks or attacks that attempts to compromise a network.
- Firewall can take the form of software such as a security program or hardware such as a physical router.
- Both perform the same function which is scanning incoming network traffic to make sure it doesn't contain blacklisted data.
- Firewall scan each packet of data which are small chunks of the larger hole reduced in size for easy transmission and make sure these packets don't contain anything malicious

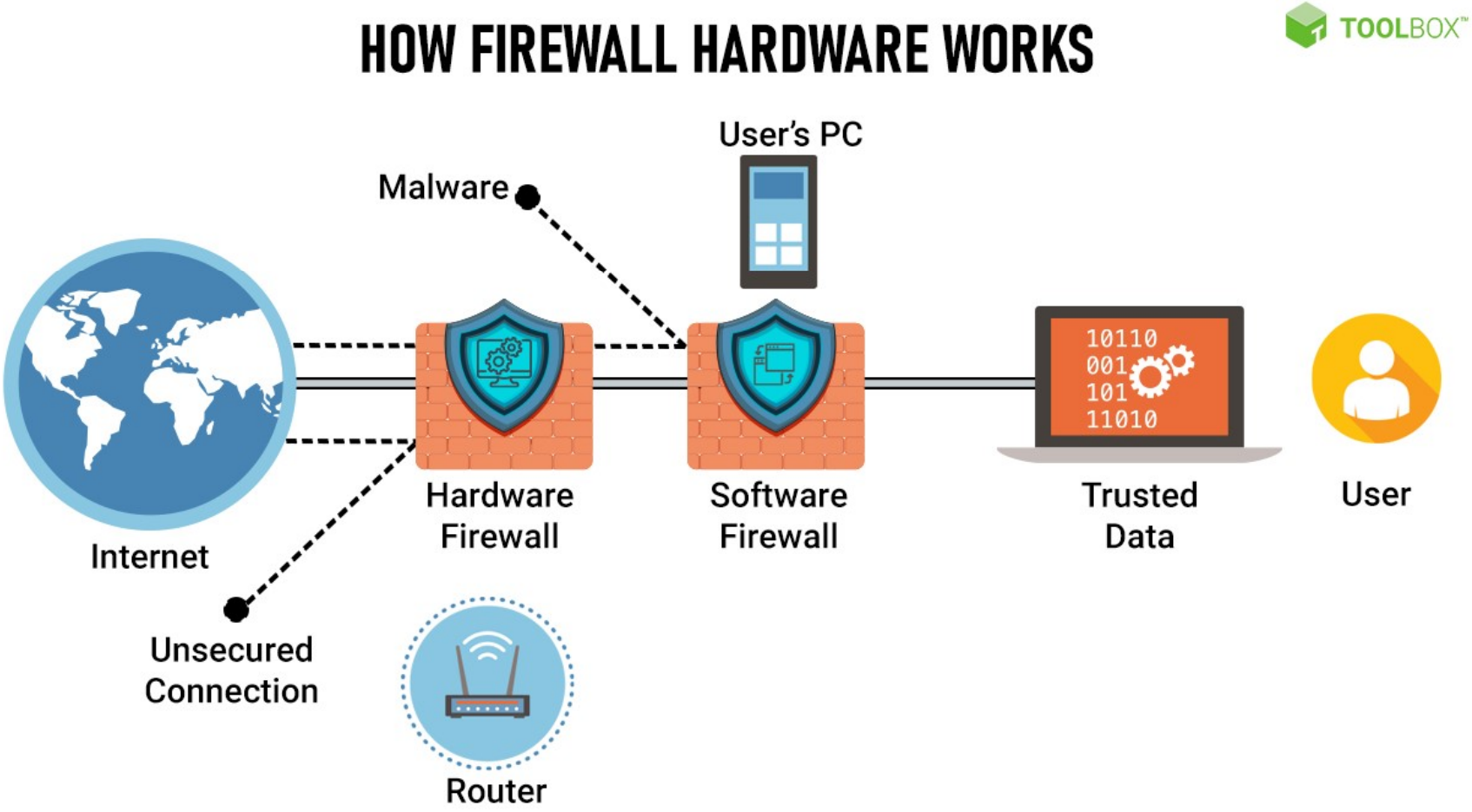
Firewall

- Antivirus comes with Basic Firewall (Software)
- potential drawbacks of a firewall include a slowdown in traffic, especially if packets are being entirely analyzed by a user's local computer.
- accidentally block legitimate sites which can be corrected by making exceptions in the settings and specifying / white-listing the traffic and or ports are allowed past.
- Many computers lack even basic firewall protection which is why it's important to make sure every computer is protected by a Firewall.

Hardware Firewalls Vs Software Firewall

- Hardware Firewalls: A hardware firewall sits between organizations' local network of computers and the Internet.
- The firewall usually inspects all the data that comes in from the Internet, passing along the safe data packets while blocking the potentially dangerous packets.
- In order to properly protect a network without hindering performance, hardware firewalls require expert setup, and so Hardware Firewall may not be a feasible solution for companies without a dedicated IT department.
- For businesses with many computers, however, being able to control network security from one single device simplifies the job.

Hardware Firewalls Vs Software Firewall



Hardware Firewalls Vs Software Firewall

- Software Firewalls: Software firewalls are installed on individual computers on a network.
- Unlike hardware firewalls, software firewalls can easily distinguish between programs on a computer.
- This lets them allow data to one program while blocking another.
- Software firewalls can also filter outgoing data, as well as remote responses to outgoing requests.
- The major downside to software firewalls for a business is their upkeep: they require installation, updating and administration on each individual computer.