Are the current defenses Adequate?

There are many different methodologies & controls to improve cyber security defense, which can improve current security controls. But are they adequate in protecting users & client computers?

To know if the controls are adequate, let us look at how attacks are categorised and the channels they use:

3 Broad Categories of Attack based on the Target:

- **Server side attacks:** Target the Server OS, Applications hosted in a Server
  - Server side attacks require, some sort of service listening on the Target
  - Such as WebServer / Email Server / DB Server
  - Servers expose its services for client's to access, hence Servers are frequent targets
  - Servers also have the highest protection

- **Client side attacks:** Target client OS, Applications installed in a client
  - Client side attacks require, client applications accessing data
  - Such as Web Browser / Media Player / Office Applications / Email Clients
  - The data

- **Attacks Target Users** to perform below
  - Credential Theft
  - Identify Theft
  - Confidential Data Leak
  - Data Manipulation
  - Leads to further Server & Client side attacks

**Based on the Target the Malware delivery channel differs:**

Malwares such as Mirai, Cryptolocker, WannaCry, ShellShock, HeartBleed, Stuxnet require different channels of delivery, & eventually launch an attack and exploit.

1. **Server attacks** are confined to specific services & applications which the Server exposes.

   Such as:
   a. Web specific ports & protocols / Apps
   b. Email specific ports & protocols / Apps
   c. FTP specific ports & protocols / Apps

2. **Client attacks** are those the Users & User Application exposes

   Such as:
   a. Email Access
   b. WebSite Access
   c. Any Web-based Apps
   d. Social Networking Apps (Includes Chat/ Media / File Transfer / Images)
   e. Video Streaming
   f. Media Players
   g. Cloud Storage
h. USB Removable Media

3. Users are also attacked via:
   a. Phishing & Spear-Phishing
   b. Spoofed Websites
   c. Spoofed Emails
   d. Spoofed Contents
   e. Ad / Pop-Up/ Drive-By Downloads
   f. Social Engineering

How well protected, are Servers / Client Computers & Users?

All Hosted Servers & Applications that expose itself are protected by atleast one / all of the below:

1. Perimeter Next Gen Firewall
2. Second-Level Next Gen Firewall
3. Perimeter Next Gen IPS
4. Host IPS
5. Web Application Firewalls along SSL Decryptors
6. DDoS Protectors
7. Endpoint Security on Servers
8. SSL VPN Solutions

All Clients that expose itself are protected by:

1. Endpoint Security running on the Desktop/Laptop/Mobile
2. Anti-SPAM (if Corporate User)
3. Category based WebFiltering (if Corporate User)

Users access all sorts of applications from client computers either in office/at home/ during travel, what sort of technology is available to these users to:

1. Not to open malicious attachment
2. Not to open malicious link
3. Not to share credentials to untrusted/malicious/spoofed websites
4. Train them in identifying anomalies
5. Not to install untrusted apps on Mobile Phones

The list goes on..

It is evident from what we see day-to-day, Clients & Users are easier target since servers to an extent are well protected when compared to Clients & Users. With IoT coming up strong & explosive growth of Mobile Devices -- the attackers now have larger ecosystem to target. Any Technology that can help the Users identify the malicious will go a long way in augmenting the current defenses.