# WHY LAYERED SECURITY IS IMPORTANT

Firewall
Antivirus
Proactive Malware Defense
Remediation
User Education

## WHAT IS LAYERED SECURITY?

Using several different cyber security solutions that work together to reduce the attack surface of a networked system.

## WHAT ARE THE LATEST CHALLENGES?

A majority of IT admins and security practitioners believe there's a significant increase in endpoint risk because of:

**73%** use of commercial cloud applications

**63%** employees working from home and offsite locations

**68%** employee-owned mobile devices

### MOST FREQUENT OFFENDERS

Malware attacks experienced by IT networks in the last year (more than one response allowed):

- Web-borne malware attacks: 80%
- APTs/targeted attacks: 65%
- Rootkits: 65%
- Spear phishing attacks: 55%

### INCREASES IN SEVERITY AND EFFICIENCY

**69%** of respondents said the severity of malware incidents has increased in the last year.

**60%** of the time, attackers are able to compromise an organization within minutes[1].

## WHERE ARE THE HOLES IN YOUR DEFENSES?

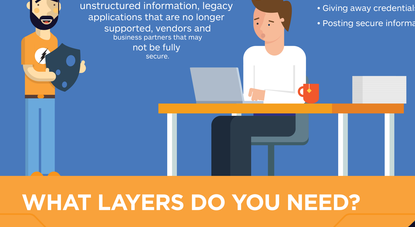
### NOT KEEPING UP

Of the 7 million publicly known information security vulnerabilities, just **10 accounted for almost 97%** of the exploits observed in 2014[2].

**99.9%** of the exploited vulnerabilities were compromised more than ayear **after they were published.**

### WEAK SECURITY

Discovery times too long, known flaws not being patched, security policies not enforced or well-known, missing or poorly implemented encryption, lack of malware protection, weak wireless configurations, physical security flaws, unstructured information, legacy applications that are no longer supported, vendors and business partners that may not be fully secure.



### NEGLIGENT OR UNINFORMED USERS

- Falling for phishing attacks and other social engineering tactics
- Bypassing security measures and installing malware directly on the system
- Giving away credentials in phishing attacks
- Posting secure information over social media

## WHAT LAYERS DO YOU NEED?

### Tech solutions

**Anti-attack software**
Archers: Includes anti-exploit, anti-spam, and anti-phishing technology. Anti-exploit tech can disable attacks before they are able to infiltrate the system.

**Network**
Castle: Fully updated and patched OS software helps keep the network secure.

**Firewall**
Castle wall: Includes IP whitelists, blacklists, and port security. Acts as a border between the outside world and internal network.

**Anti-malware**
Knights: Targets new threats and cleans infections. Can also detect undesired software like PUPs, keeping them from spamming users or draining system resources.

**Traditional AV**
Guards: Prevents infections from viruses, Trojans, worms, and other known threats.

**Internet-facing applications**
Gates: Apps such as Java and Flash leave the network vulnerable to attack if they are not updated.

### Awareness solutions

Are my cyber policies documented?

Are they reasonable?

Are my employees actually following the policies?

Am I using tech that helps enforce these policies?

The IT admin gathers threat intelligence from outside sources and uses it to fend off attacks.

He also helps keep the users secure with strong policies.

The user is the **MOST IMPORTANT SECURITY MEASURE.**

A well-informed user fortifies all other layers of security.

Learn more at **malwarebytes.com/articles**

Malwarebytes


Sources:
1. 2015 State of the Endpoint Report: User- Centric Risk. Sponsored by Lumension, independently conducted by Ponemon Institute LLC (Jan. 2015); Verizon 2015 Data Breach Investigations Report
2. Verizon 2015 Data Breach Investigations Report