Security Environment

Mohamed Albadri

Antivirus

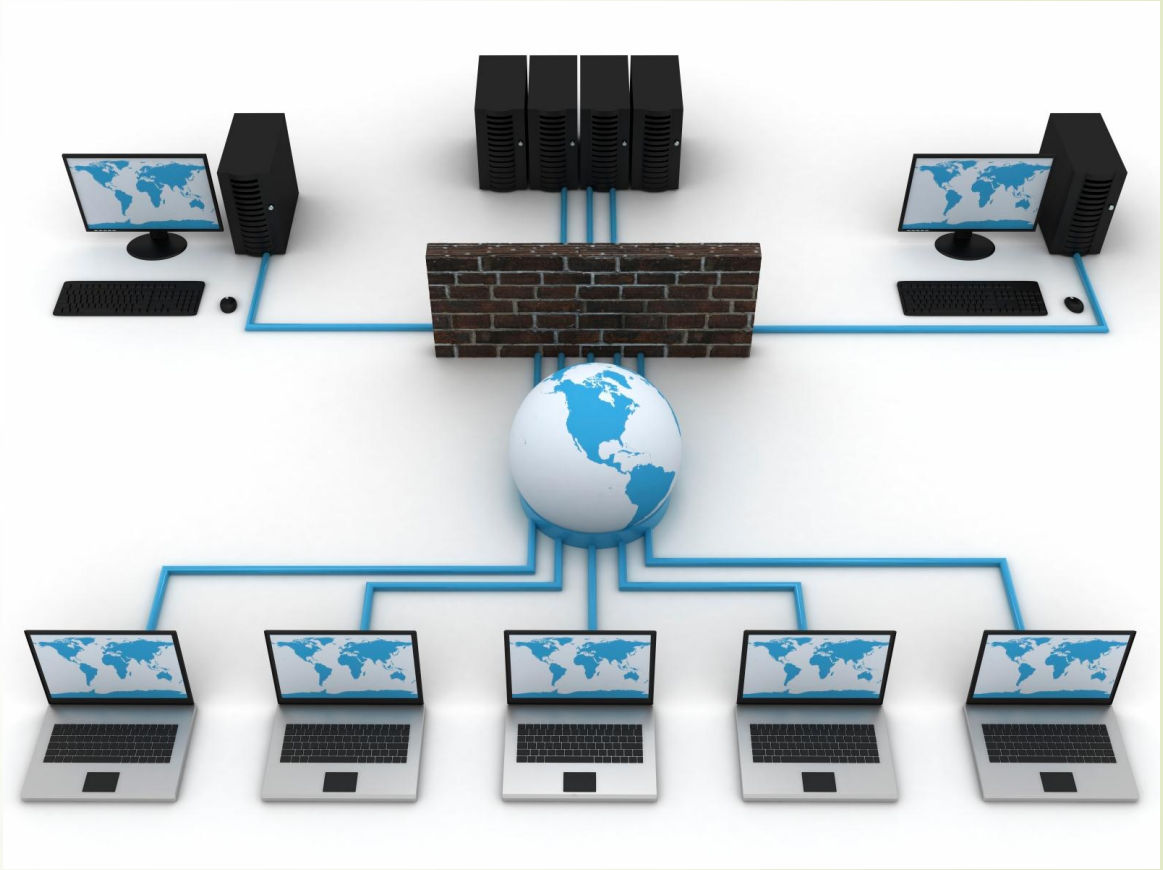
- Malware protection: virus, worm, Trojan, etc.
- Endpoint protection
- Virtual environment
- Cloud based AV

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (February 2016)

Firewall

- Statefull inspection
- NAT
- VPN




CHALLENGERS
LEADERS
Check Point Software Technologies
Palo Alto Networks
Fortinet
Cisco
Juniper Networks
Dell SonicWALL
McAfee
Huawei
WatchGuard
HP
Sophos
Barracuda Networks
F5
AhnLab
Hillstone Networks
Arkoon+Netasq
NICHE PLAYERS
VISIONARIES

Next Generation Firewall NGFW

- Normal Firewall +
- Application control
- Antivirus
- Intrusion Prevention System IPS
- Web filtering

Intrusion Prevention System IPS

- Analyze traffic for a know malicious activities (signature based)
- Inspect traffic for anomaly behavior
- Can be implemented in promiscuous and inline mode
- On detection, it can block traffic, reset connection, and alert the admin.

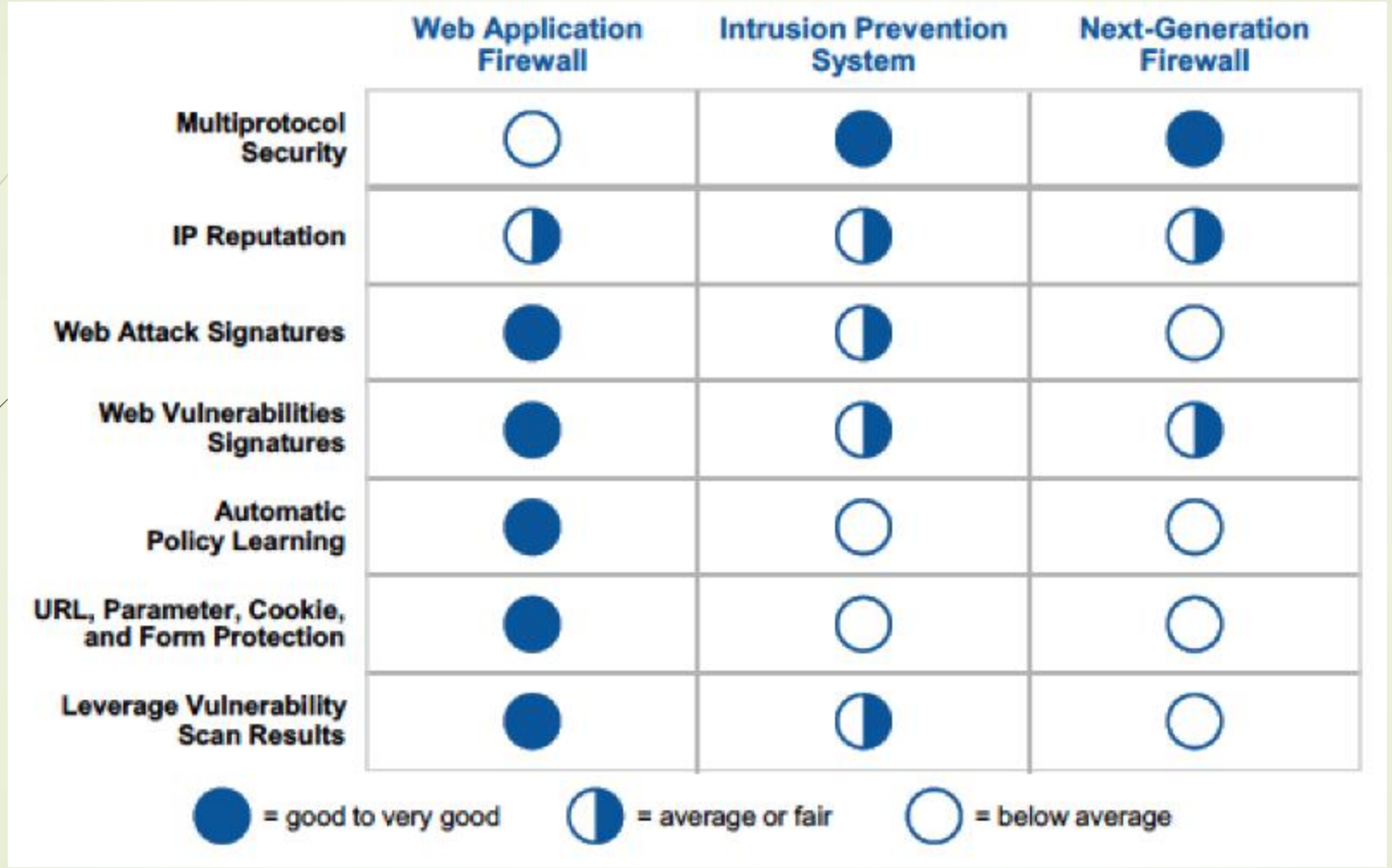
Figure 1. Magic Quadrant for Intrusion Prevention Systems

Source: Gartner (November 2015)

Web Application Firewall WAF

- WAF are designed to protect web applications/servers from web-based attacks
- WAFs protect against web application threats like SQL injection, cross-site scripting, session hijacking, parameter or URL tampering and buffer overflows
- they also detect (and can prevent) new unknown types of attacks. By watching for unusual or unexpected patterns in the traffic they can alert and/or defend against unknown attacks
- They can be used to scan web application for new vulnerabilities
- SSL offloading


CHALLENGERS
LEADERS
F5
Imperva
Citrix
Akamai
Barracuda Networks
NSFOCUS
Fortinet
Radware
Trustwave
Penta Security
DenyAll
Ergon Informatik
Positive Technologies
United Security Providers
AdNovum
DBAPPSecurity
NICHE PLAYERS
VISIONARIES


Web Application Firewall
Intrusion Prevention System
Next-Generation Firewall
Multiprotocol Security
IP Reputation
Web Attack Signatures
Web Vulnerabilities Signatures
Automatic Policy Learning
URL, Parameter, Cookie, and Form Protection
Leverage Vulnerability Scan Results
= good to very good
= average or fair
= below average

Secure Web Gateway

- URL Filtering
- Inspect SSL Encrypted Traffic (SSL Inspection)
- Application Control
- Antivirus
- IPS

Figure 1. Magic Quadrant for Secure Web Gateways

Source: Gartner (May 2015)

Secure Email Gateway

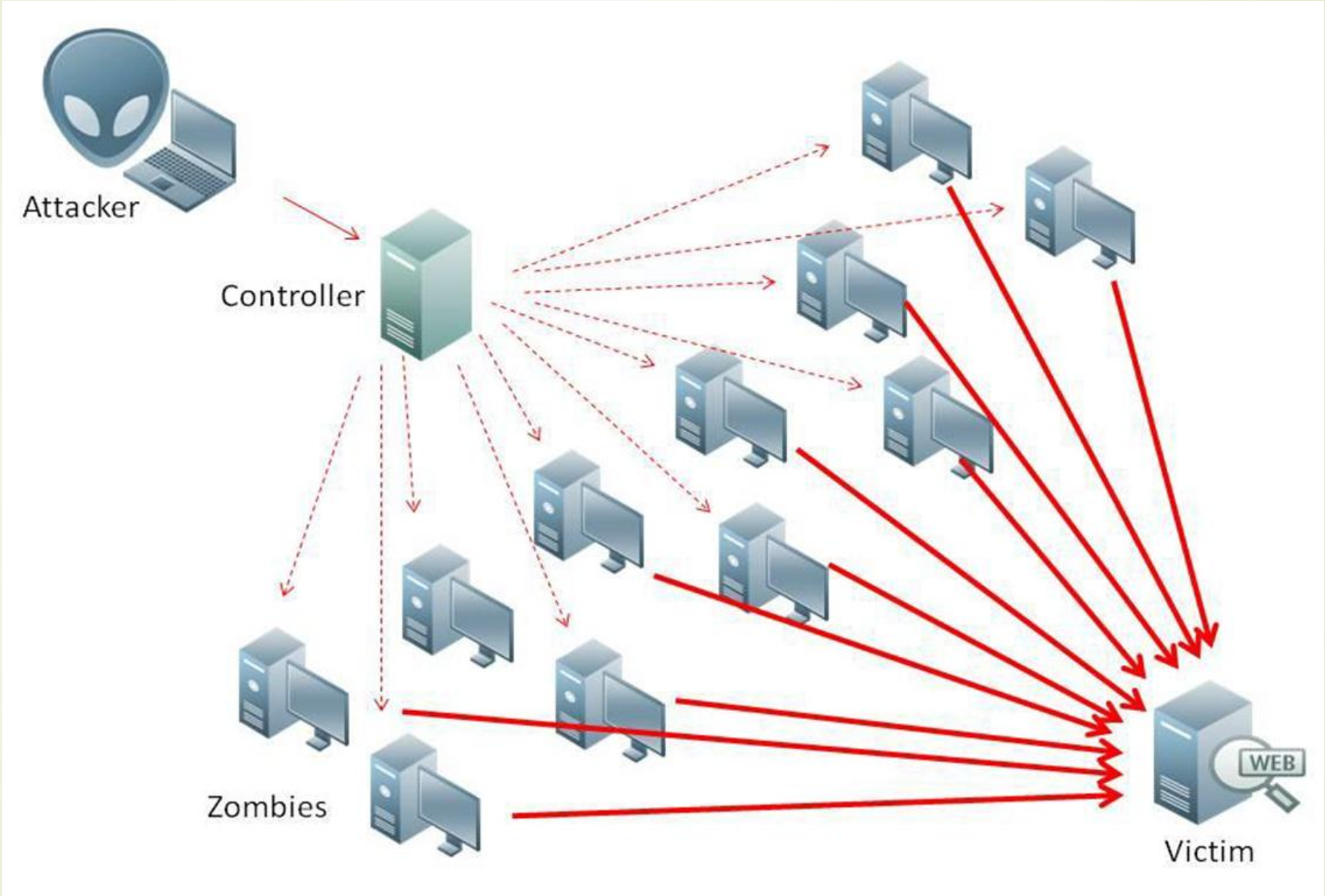
- Protects inbound and outbound email traffic
- Blocks spam and malware
- Prevent phishing and other advanced threats
- Applies Data Leak Prevention DLP policies

Figure 1. Magic Quadrant for Secure Email Gateways

Source: Gartner (June 2015)

DOS/DDOS Prevention

- It is a resource exhaustion attack
- DOS is a single agent single connection attack
- DDOS is a multiple agents (zombies) multiple connection attack


Attacker
Controller
Zombies
WEB
Victim

Network Access Control
NAC

- Control all network access (LAN, wireless, VPN) from one place
- Authenticate, authorize, account wired and wireless users
- Extensive policy enforcement
- Automated device-compliance checks (device posture and remediation)
- network visibility
- BYOD