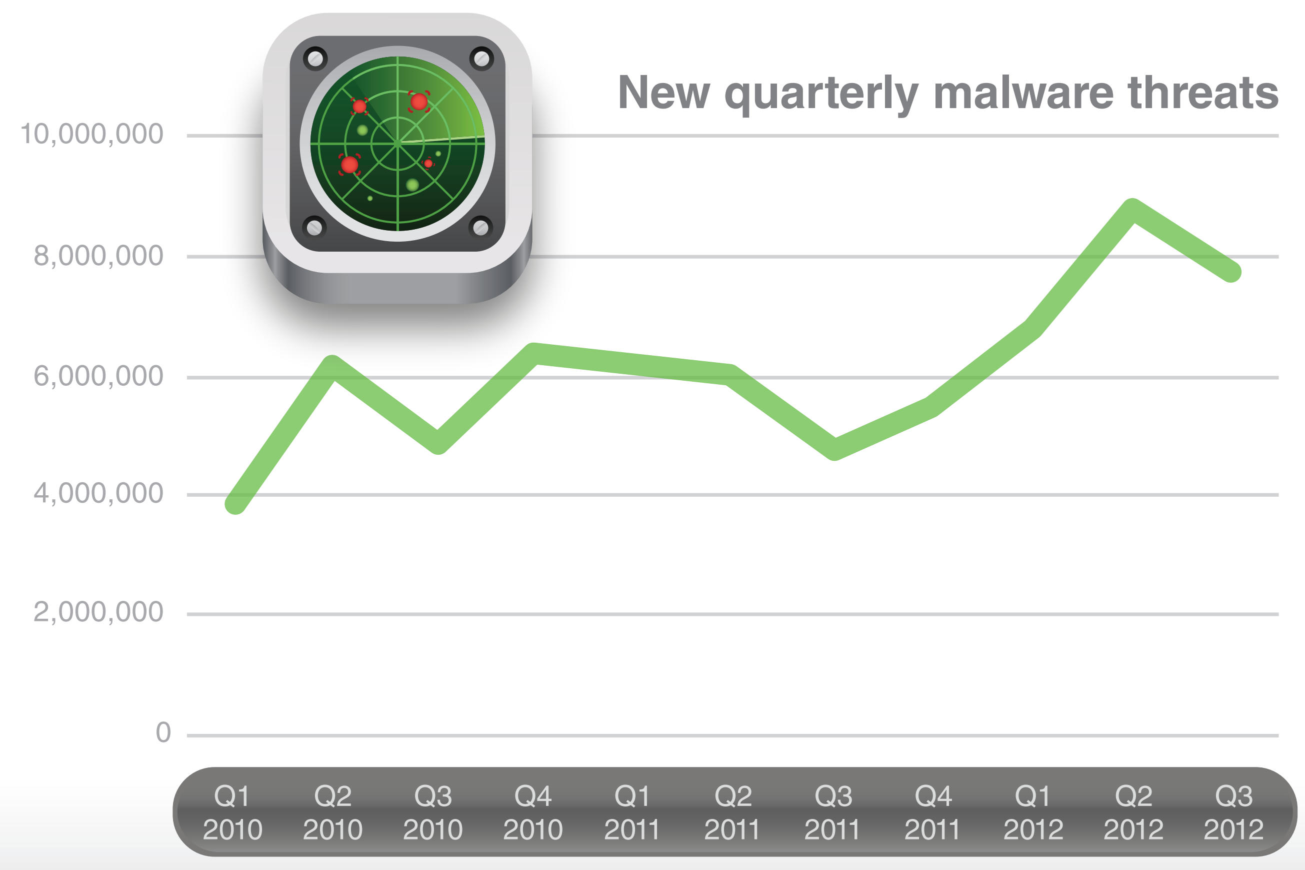
Why your organization needs Infoblox DNS Firewall

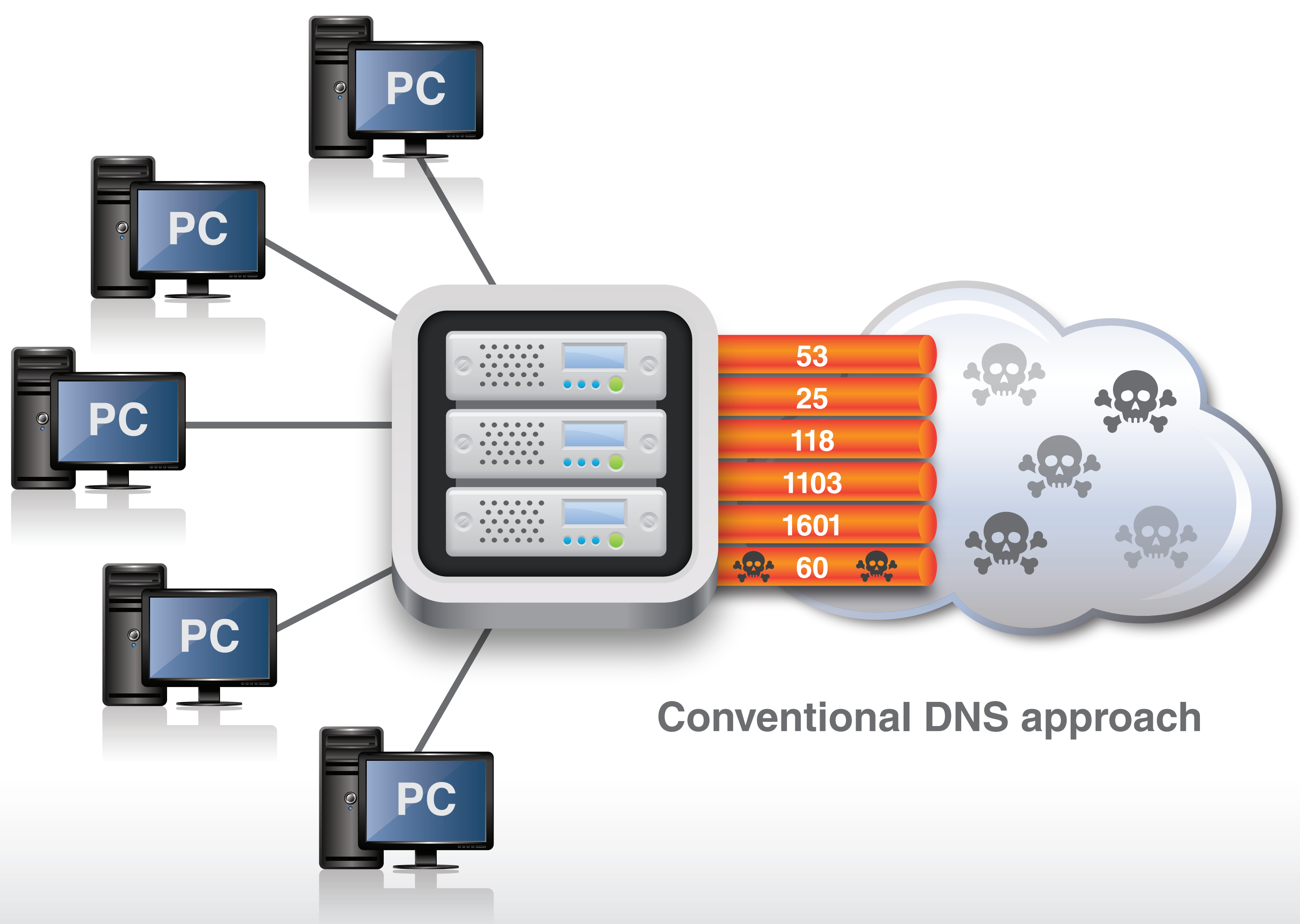
Malware threats are booming

- Around 7.8 million new malware threats per quarter in 2012
- Mobile threats grew almost 10X in 2012*
- 855 successful breaches – 174 million records compromised in 2012**
- 69% of successful breaches utilized malware**
- 54% of breaches took months to discover**
- 92% discovered by external party**

* Source: McAfee Threats Report: Third Quarter 2012
** Source: Verizon Security Study 2012



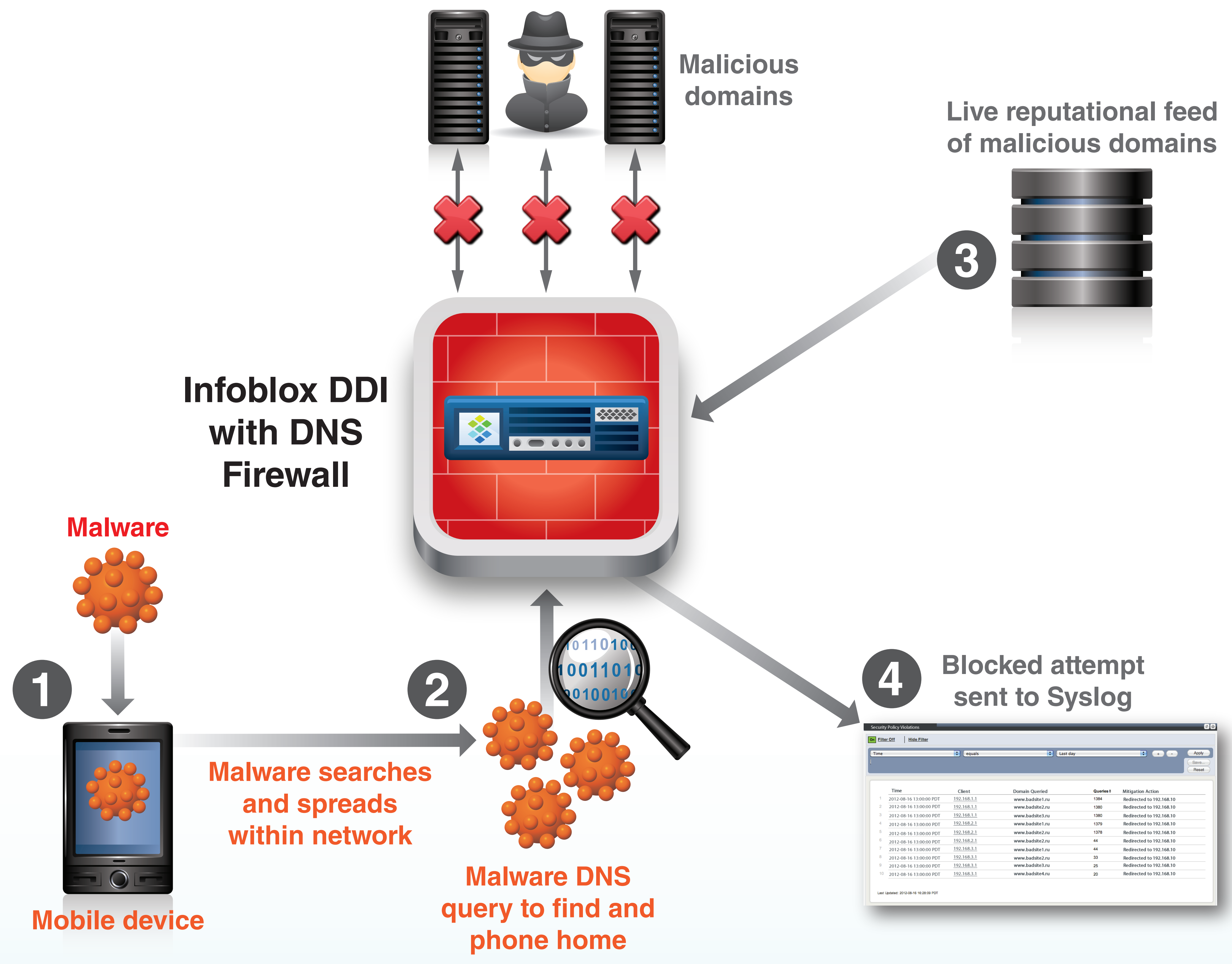
Conventional DNS servers are a hole in your security



Conventional DNS approach

1. Conventional DNS servers can’t distinguish between good and malicious domains
2. Conventional DNS servers can’t block access to malicious domains
3. Conventional DNS reporting provides no visibility to queries to malicious domains

How Infoblox DNS Firewall disrupts malware communications


Malicious domains
Live reputational feed of malicious domains
3
Infoblox DDI with DNS Firewall
Malware
1
2
Malware searches and spreads within network
Mobile device
0110100
1001101
0100100
Malware DNS query to find and phone home
4
Blocked attempt sent to Syslog

1. An infected mobile device is brought into the office. Upon connection, the malware starts to spread to other devices on the network.
2. The malware makes a DNS query for “bad” domain to find “home”. The DNS Firewall has the “bad” domain in its table and blocks the connection.
3. The DNS Server is continually updated by a reputational data feed service to reflect the rapidly changing list of malicious domains.
4. Infoblox Reporting provides list of blocked attempts as well as the
   - IP Address
   - MAC Address
   - DHCP Fingerprint

Infoblox DNS Firewall delivers:

Ability to block malware-based DNS queries to malicious domains

Reporting that helps pinpoint infected clients by IP/MAC address and DHCP Fingerprint

Infoblox
CONTROL YOUR NETWORK

3111 Coronado Drive
Santa Clara, CA 95054

o: +1.408.986.4000
f: +1.408.986.4001

info@infoblox.com
www.infoblox.com