Ransomware: The pervasive business disruptor

An infographic by Frost & Sullivan, commissioned by Dimension Data and Cisco

How does ransomware work?

A *malware that encrypts files on a victim's computer* and servers until the ransom is paid. *Successful ransomware attacks exploit vulnerabilities* in operating systems, cause *massive business disruption*, and generate lucrative revenue for cyber criminals.

Cost of ransomware

1

49%... Global businesses affected by *at least 1 cyber ransom attack in 2016*, of which 39% are ransomware attacks*

2

USD 1 billion... *Revenue cybercriminals* are estimated to generate in the United States alone using ransomware **

3

USD 200 million – USD 300 million... Highest business *impact from a ransomware attack on an international shipping* firm disrupting cargo movement for 2 days and taking 2 weeks to fix ***

Sources: * Cisco 2017 Mid-Year Cyber Security Report | ** FBI | *** Los Angeles Times

Vulnerable target: Is your organisation at risk?

Affected organisations exhibit the following poor cybersecurity practices:
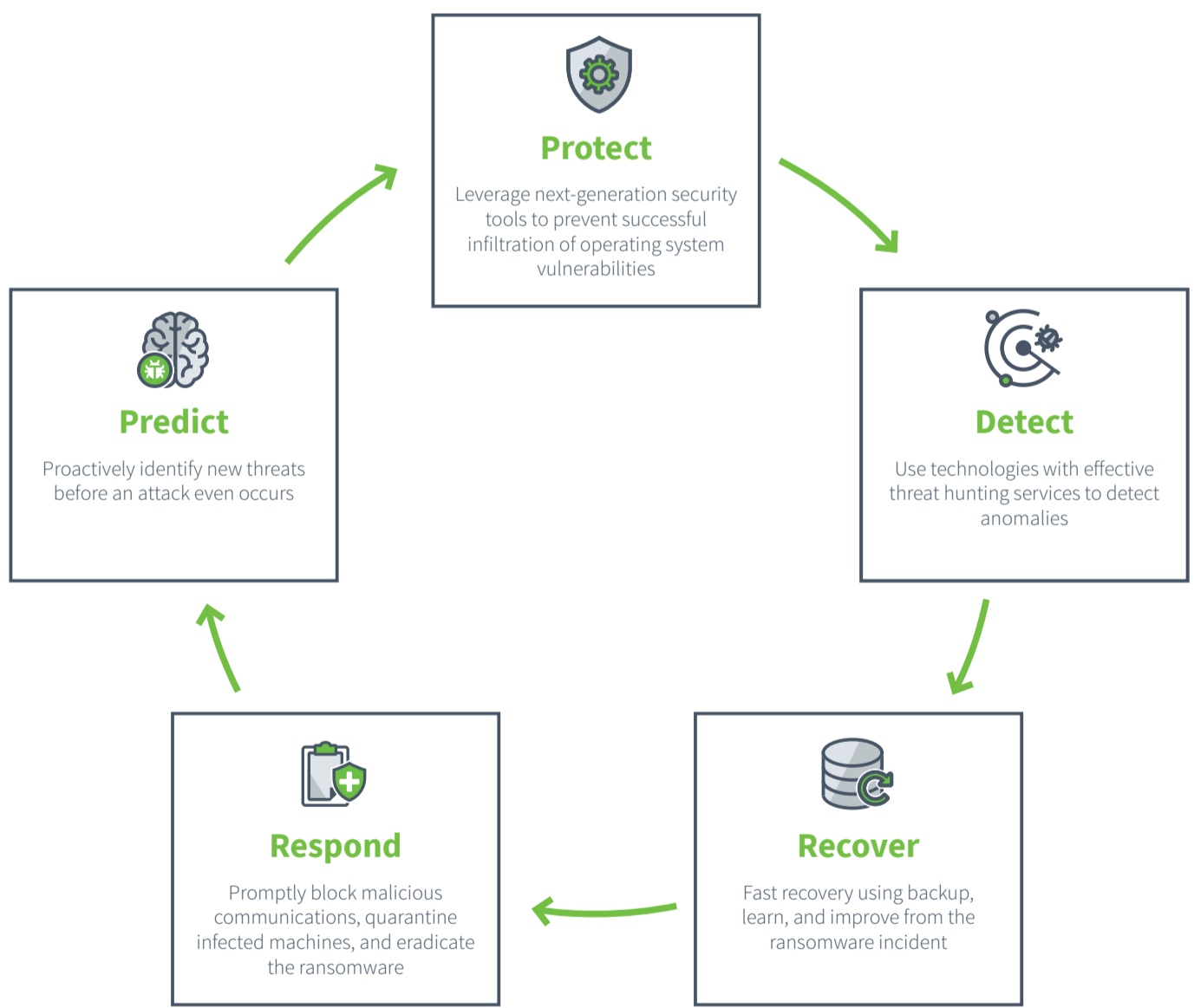
Lack of patch management

Ineffective prevention of malware from infecting and spreading

No backup and recovery system in place

How to fight back using a ransomware defence framework

Protect

Leverage next-generation security tools to prevent successful infiltration of operating system vulnerabilities

Predict

Proactively identify new threats before an attack even occurs

Detect

Use technologies with effective threat hunting services to detect anomalies

Respond

Promptly block malicious communications, quarantine infected machines, and eradicate the ransomware

Recover

Fast recovery using backup, learn, and improve from the ransomware incident

Key questions to consider in your ransomware defence strategy

When was your organisation's last cyber health check? Do you know your assets and vulnerabilities?

Do you have a multi-faceted approach with a combination of security solutions and services to stop the ransomware kill chain?

Have you reviewed your security solutions and its ability to stop ransomware attacks?

Can your networking infrastructure enforce security?

Do you have backup and restore as part of your strategy?

Learn how you can remain business resilient and maximise uptime during a ransomware attack at *www.dimensiondata.com/ransomware*