
carbon
Carbon Cloud
Next-Gen Cyber
Security

# Why do things differently?

Creating intelligent solutions

SECURITY

## Nearly 200 million US voter records leaked

Personal details of American voters were stored on an unsecured and exposed server.

The cumulative cost of data breaches is expected to reach a whopping $8 trillion according to research firm.

Global spending on **cybersecurity solutions** will grow by 33% over the next four years, reaching $134bn annually by 2022, according to Juniper Research.

## "WannaCry" ransomware attack losses could reach $4 billion

Share / Tweet / Reddit / Flipboard / Email

## UK Data Breaches H1 2017

Debenhams, Wonga, Three,
ABTA, Lloyds Banking Group

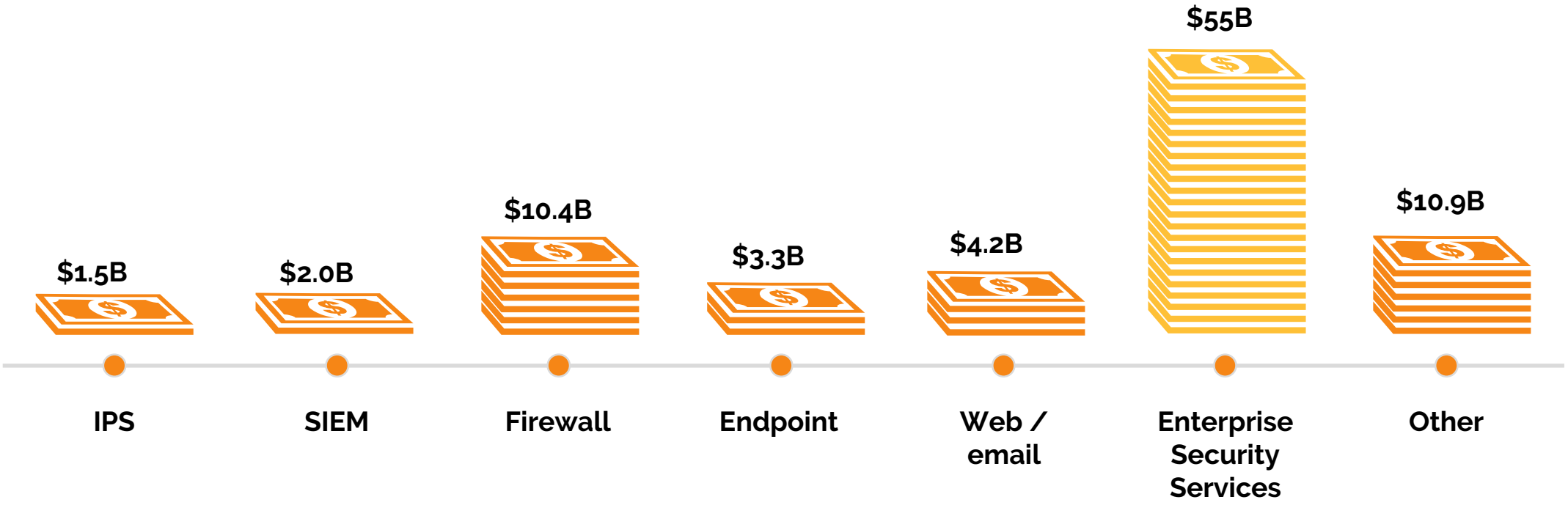
## 'Petya' ransomware attack strikes companies across Europe and US

**Ukraine government, banks and electricity grid hit hardest, but companies in France, Denmark and Pittsburgh, Pennsylvania also attacked**

News Articles from 2017

# Why do things differently?

Creating intelligent solutions




**Security Spending**

$80 billion will be spent on protecting data, but breaches will still be commonplace

Source: IDC 2017 security and infrastructure services forecast

# AI and Machine Learning

Creating intelligent solutions

## Skills Shortage

**66%** Organisations report that they have too few cyber security workers.

## Cost

**33%** Of the Cyber Security workforce earn over £80,000 pa.

The European region faces a projected skills gap of 350,000 workers by 2022

Source: (ISC)² Benchmarking Workforce Capacity and Response to Cyber Risk 2017

# A Holistic Approach

Creating intelligent solutions

- Threat intelligence
- Automated penetration testing
- Exposure analysis


- Policy-based encryption
- Divert attackers
- Isolate systems and services

- Forensic investigation
- Automation of remediation
- Compromise assessment

- Risk prioritisation
- Automated threat management
- AI based threat hunting

# Predict

Creating intelligent solutions

## Predict the Hacker

Hackers are more sophisticated, Enterprises need to improve their Cyber security methodologies and think from the hacker's perspective

## AI

Utilise machine learning and AI to continuously analyse weaknesses and identify where hackers may strike

## Attack Vectors

A complete map of attack vectors will help you to understand the risks and will provide you with recommended remediation options

## Threat Intelligence

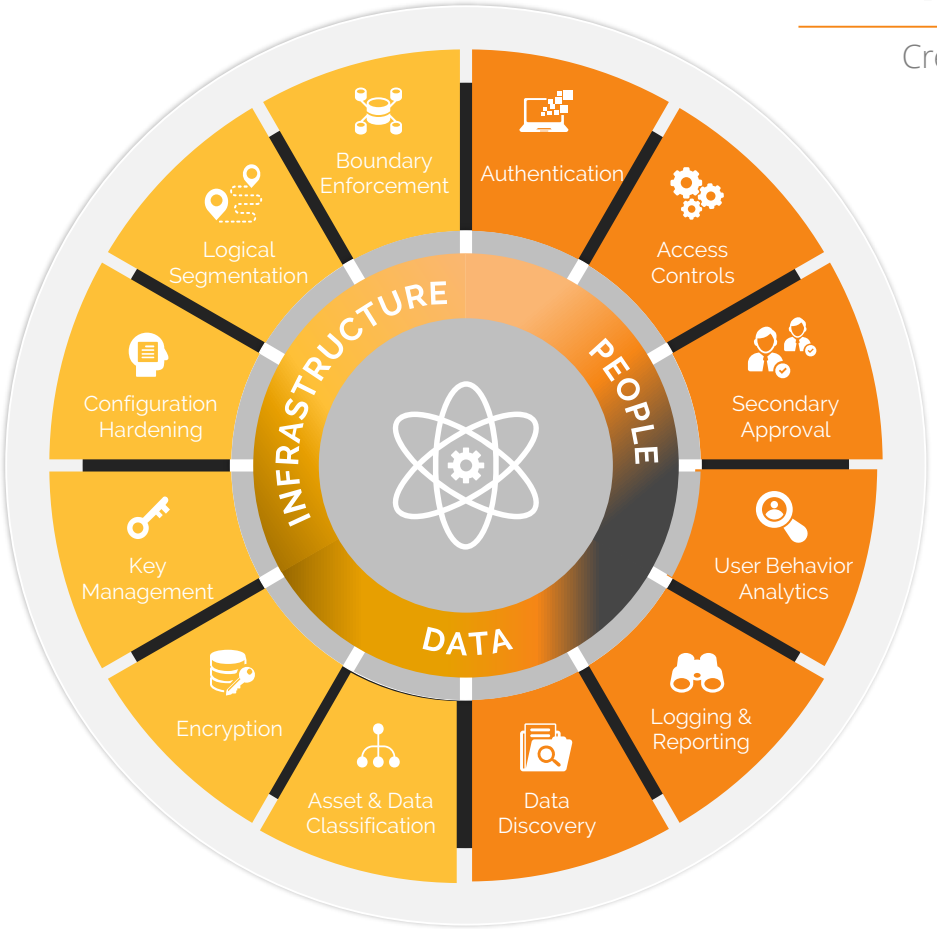
Utilise a global database of potential threats and rapidly test your exposure to new and modified threat profiles

"The biggest threat that most organizations are facing right now is a combination of excessive access for their employees and an increased focus by nation-states on access to sensitive information... From a corporate perspective, you're most focused on ensuring that you can protect the information you have."

– Stephen Schmidt, CISO AWS

# Prevent

Creating intelligent solutions




We can help lock down the cloud infrastructure: virtual servers, storage, network and Admins. Integrating 2 factor authentication, root password vaulting, deep role and object based access controls that are customisable. We also deploy a policy enforcement engine that prevents policy violations by admins and enforces good behavior. It eliminates breaches based on admin error, rogue admin behavior, and compromised admin credentials. We also harden the virtual environment by using templates to compare VM settings with frameworks like PCI, HIPAA, NIST 800-53

"...There is no one technology that's going to solve or protect you forever. You need a **good layered approach** [with] a **risk-based review of what's going on inside** your companies to figure out and identify what your **crown jewels** are and [how and when to **restrict access** to that] information."

– Scott Smith, Assistant Dir Cyber Division, FBI

# Detect

Creating intelligent solutions

## 1st to Detect, 1st to Protect

Use Zero-hour detection solutions to identify attacks before they have an impact

## Use AI

Eliminate human error and alert fatigue. Utilise AI based detection algorithms

## Unusual not always bad

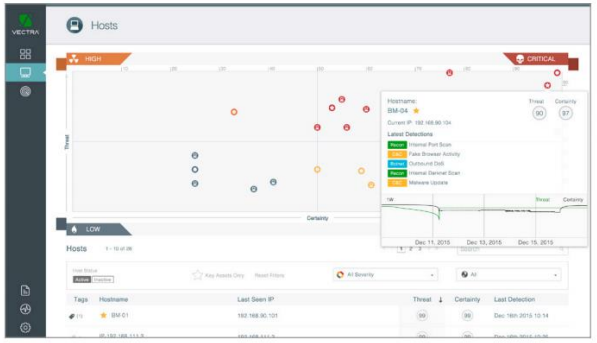
Identify the things that hackers **must** do, prevent the use of encryption as a hiding place

**1 minute 40 seconds – median time until first malicious email in a phishing campaign is opened**

**Median Threat Detection Gap – 99 days**

# Respond

Creating intelligent solutions




Pinpoint hosts at the centre of an attack and automatically track and score threats in context over the full duration of the attack.

## Improve Response Plan

- Use AI to make recommendations
- Automated remediation
- Contain incidents
- Resolve issues that need intervention
- Forensic investigation of attack (use tools)
- Comply with Regulatory / Governance requirements

Gartner has been advising clients since 2013 that “Prevention is futile in 2020. Advanced targeted attacks make prevention-centric strategies obsolete.”

Source:“Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence,” © Gartner

carbon

# Get in Touch


The Old Timber Yard, Groombridge Lane,
Eridge Green, East Sussex, TN3 9LB

hello@carboncloud.co.uk

01892 337337