



# Cyber Assurance

**UNIPART**  
**SECURITY**



90% of large organisations and 74% of small businesses  
experienced a **breach** incident in 2014\*

That's just those who knew.



We can help.  
**Unipart Cyber Assurance.**

\*HM Government 2015 Information Security Breaches Survey

**£1.46m - £3.14m** is the average cost to a large organisation  
**£75k - £311k** is the average cost to a small business  
of its worst security breach of the year.\*

It's time to evaluate your current cyber security.



We can help.



**Unipart Cyber Assurance.**



We're cyber security experts providing services and creative problem solving, powered by the Unipart Way.



## We can help you:

- Identify who is attacking you, what their motives are and how to stop them
  - Build a security-conscious culture within your organisation to reduce incidents
  - Prove to your board that you're investing in the right ways to reduce your cyber risk
  - Earn and maintain independent assurance that'll help you win and keep customers
- 
- 

# Problem

“How can I defend effectively if I don’t know who is attacking and why?”

## Solution

### ZERO DAY DETECT

Prove your systems’ integrity and uncover the truth.

*Uncorrelated Security data in*

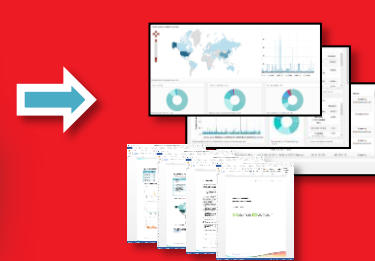
Firewall logs  
Threat intelligence  
Anti-virus events  
Email logs  
Storage records  
Identity data  
Asset records



*Big Data techniques*



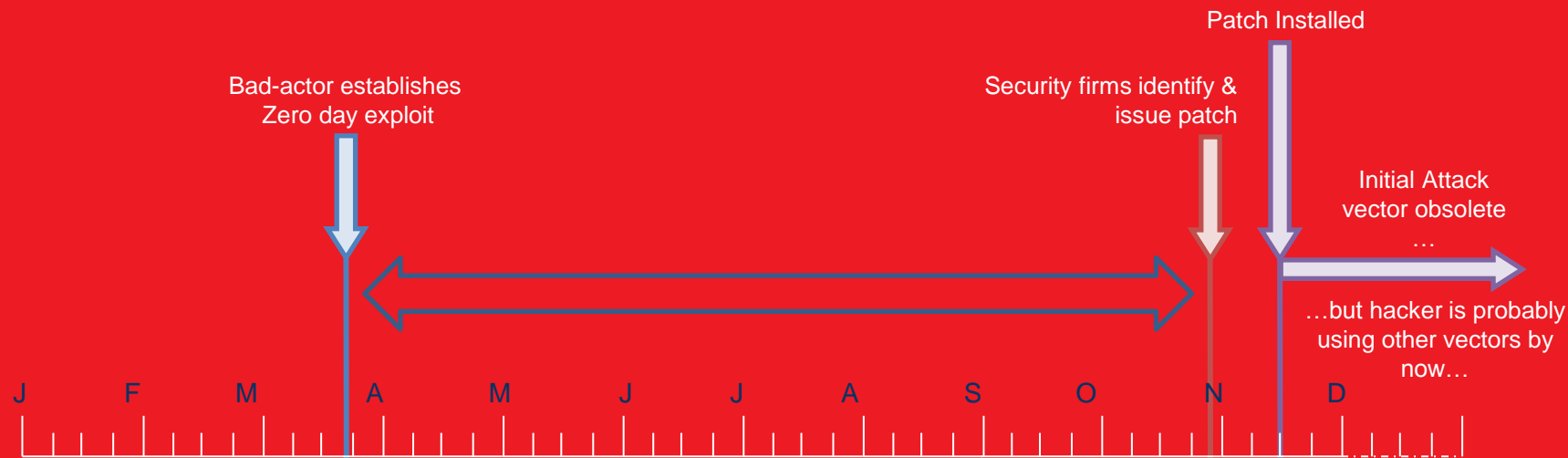
*Valuable Insights out*



*In record time*



# The 'Anatomy of an Attack'



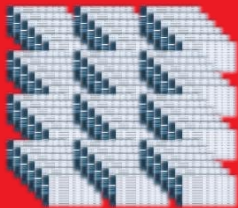
Key questions after the patch release:

1. Did the attacker use the exploit on your network?
2. If so where did he gain entry and from there how did the attack evolve?
3. What information was taken?

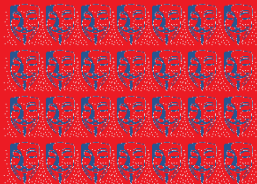
Only way to be sure is to look back over history  
to see if newly uncovered attacks appear in your logs

# The Zero Day Detect Solution

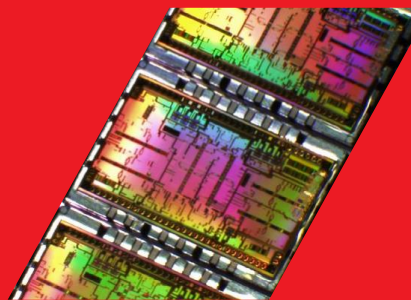
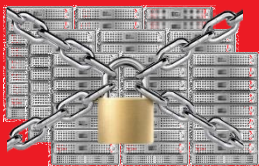
## 1 BIG data



## 2 BIG threats



## 3 Highly sensitive data



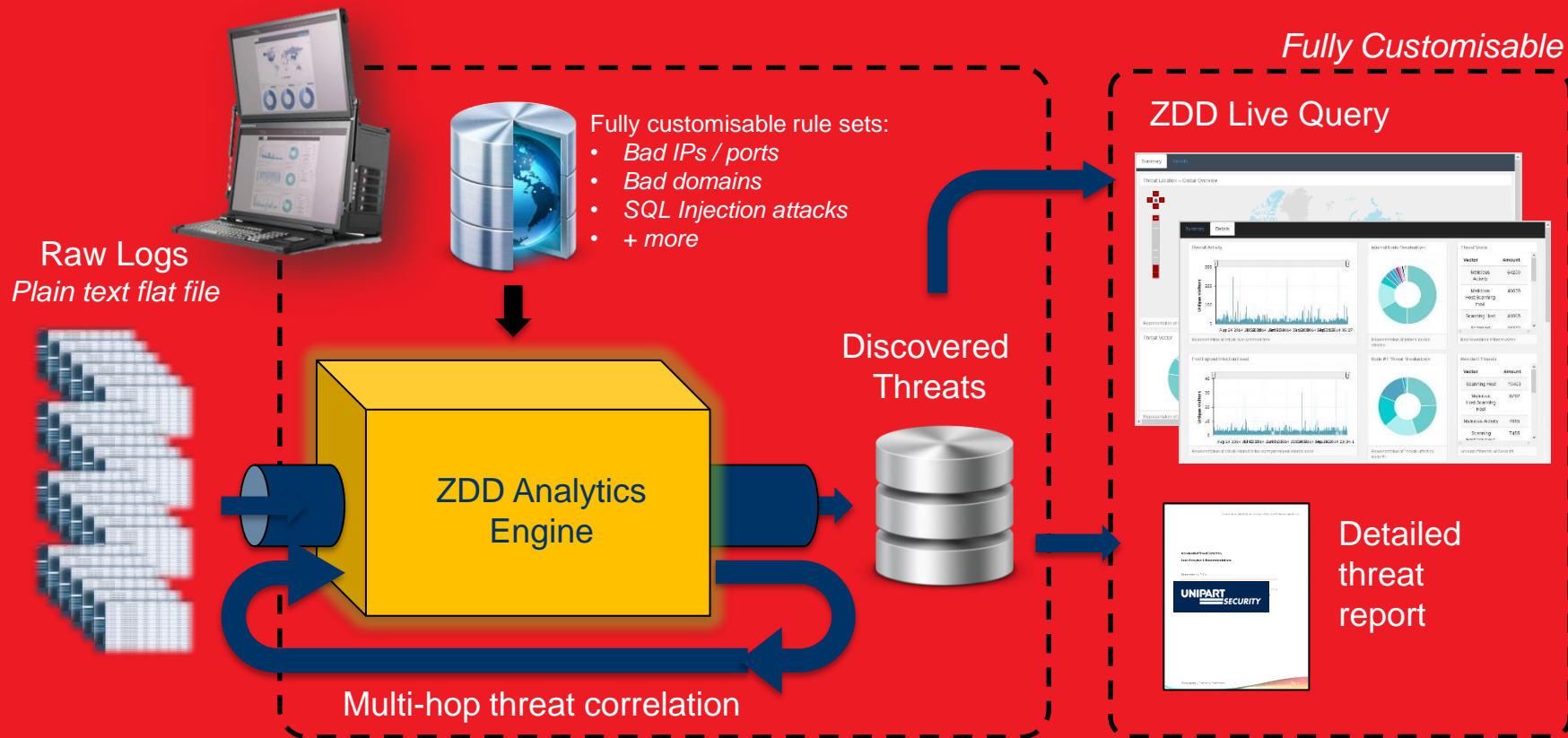
Uses custom silicon:

- Runs up to 10,000x faster than traditional CPU
  - Typically 8TB per Hour!
- Checks against millions of threats in parallel



We bring the compute and the expert to you

# The Zero Day Detect Solution Architecture





# Demonstration



UNIPART SECURITY

Command Manage Status Results Help Logout : Paul

**ACCELERATED THREAT DETECTION**

**ZERO DAY DETECT**

The image shows a screenshot of a security dashboard. The background is a dark grid with glowing yellow and white data points. The text 'UNIPART SECURITY' is in the top left, and 'Command Manage Status Results Help Logout : Paul' is in the top right. The main text 'ACCELERATED THREAT DETECTION' is centered in the middle, and 'ZERO DAY DETECT' is centered in a black bar at the bottom.

**Problem** “A single data loss event could cost me 5% of global turnover from 2016.  
How do I help my employees think differently to protect the business?”

## Solution

### SECUREHUMAN

Build a sustainable cyber security culture within your people.



*We help you understand  
current state*



*We deliver effective  
multi-mode training*



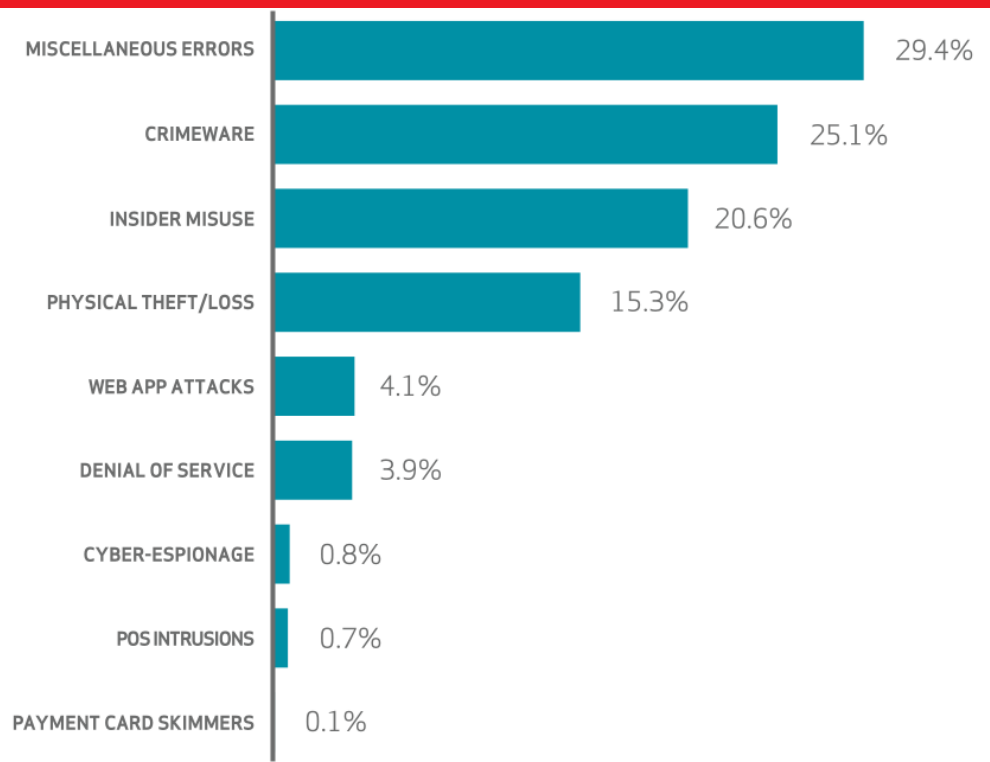
*We provide you with  
tools to sustain change*



*We prove reduction  
in security events*

# 2015 Data Breach Investigations Report

## 'Frequency of incident classification patterns across security incidents'



Analysis of 79,790 security incidents across 61 countries

Q: What's common across over 90% of these incident types?

A: People



# Problem

“Could an external attacker bypass our firewall and access sensitive data?”



## Solution

### PENETRATION TESTING

Protect your technical controls against attack.

- We're an accredited penetration testing provider for your internal or cloud systems
- We use open, peer-reviewed standards
- We use vetted staff who operate from the UK

# Problem

“I need to build trust with clients to win new business”

## Solution

### SECURITY REVIEW

Maintain your accreditations.

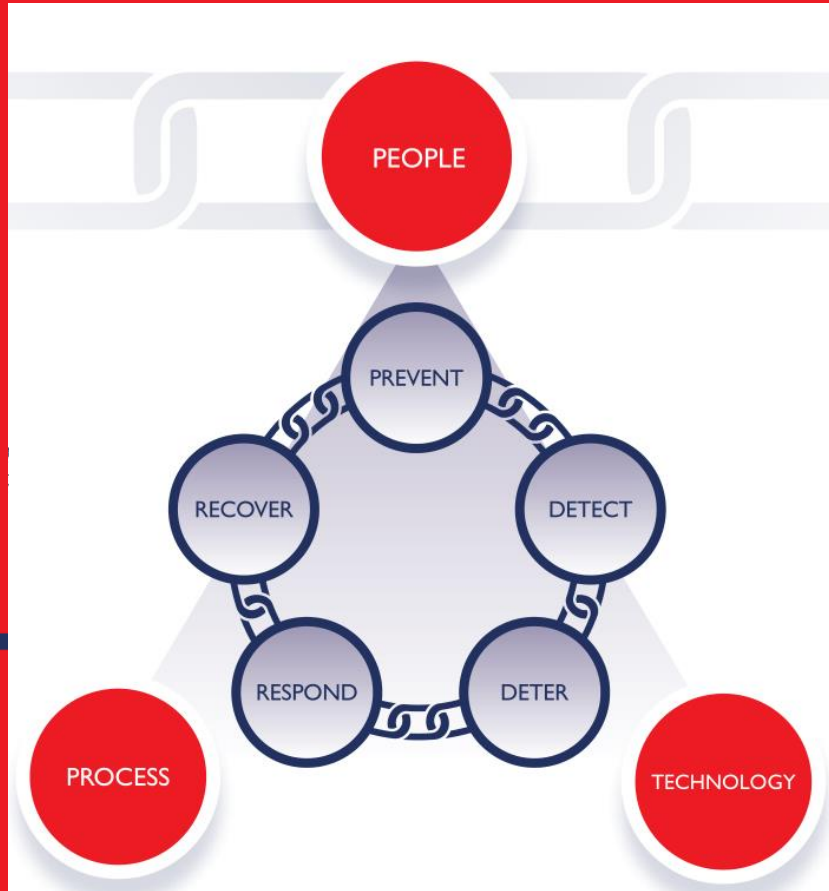
- We are due to become a Cyber Essentials certifying Body
- We can provide ISO27001 Lead Implementers and Auditors



# Our Engagement Model

**1** Define your current and aspirational cyber security maturity

**5** Prove benefits and achieve certification



**3** Help you unlock your greatest resource

**4** Advise on further technical controls



**2** Check that your current technology investments enable the aspiration

# Case Studies



*We liked the fact that they used a very transparent approach to what could be included or excluded in the test and guided us on which areas were appropriate for the style and level of test we needed. Contracting was easy, all electronic proposal discussions were secured and dates were met. The report was thorough and easy to understand – including remedial recommendations*

*Finance Director*



*The service provided was outstanding to none. They found issues our previous penetration testing supplier missed. We would not hesitate to recommend them again*

*IT Operations Manager*