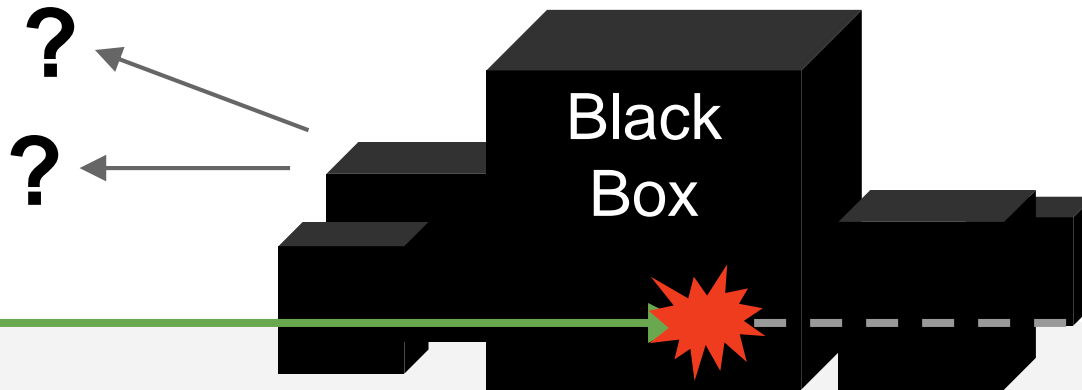


A new, data driven way of monitoring critical environments

Unomaly was founded out of the notion that we need to address the underlying issue of monitoring

Systems are Black Boxes and when they fail, we don't know why

← Things,
Apps,
Services,
Components,
Servers,
Units



We see these stats as a consequence of our inability to get answers to immediate follow up questions

42%

of all incidents are
unknown
Pink Elephant

70%

of all incidents due to
planned changes
Gartner, 2012

20%

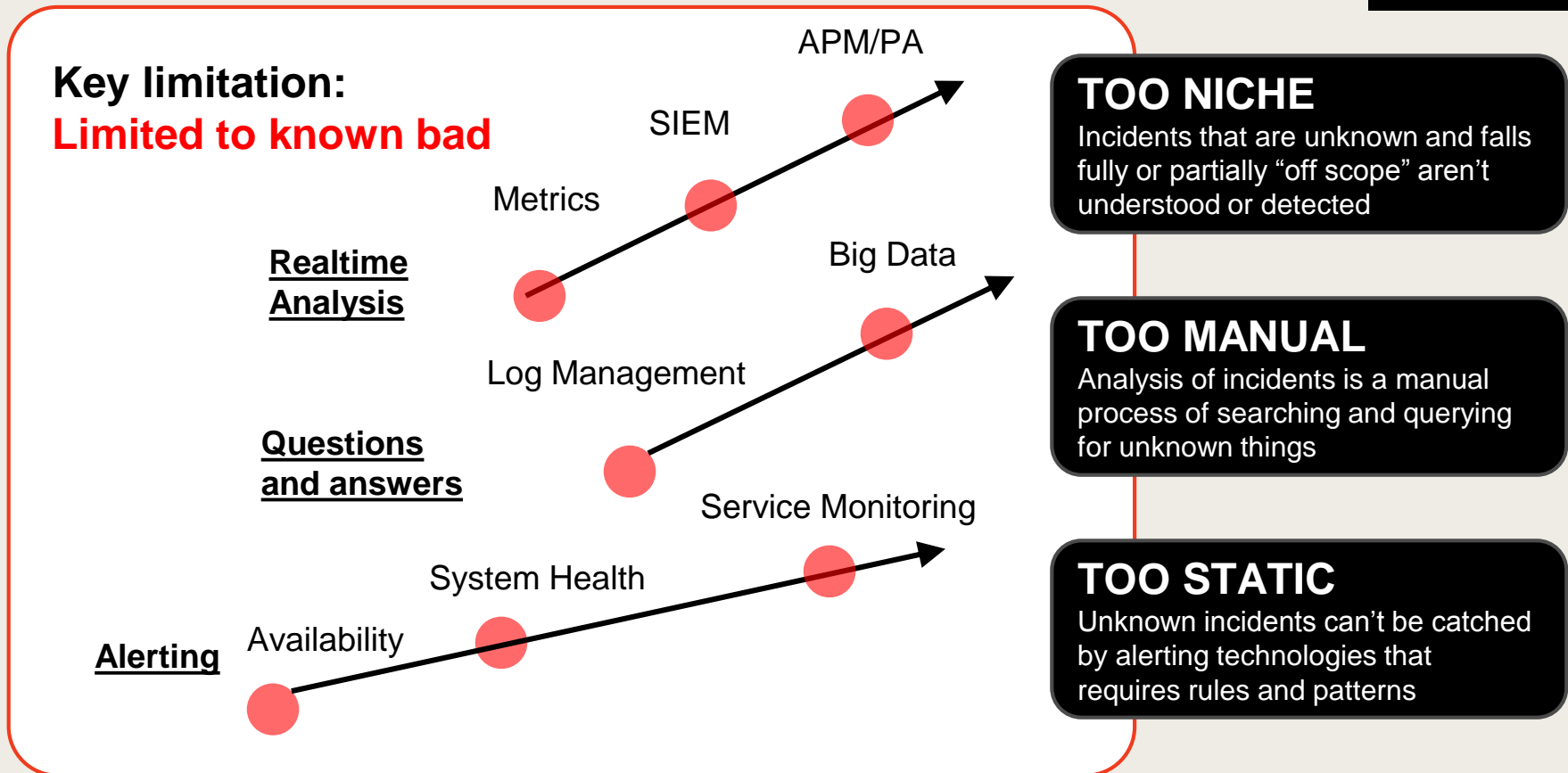
of IT time spent on
troubleshooting
IT Process Institute

69%

of security incidents
discovered by third parties
Verizon Breach Report, 2013

Anomaly is the missing piece that gives answers to questions that other solutions leave behind

Traditional solutions don't provide complete or timely answers on what is really going on and how that relates to history

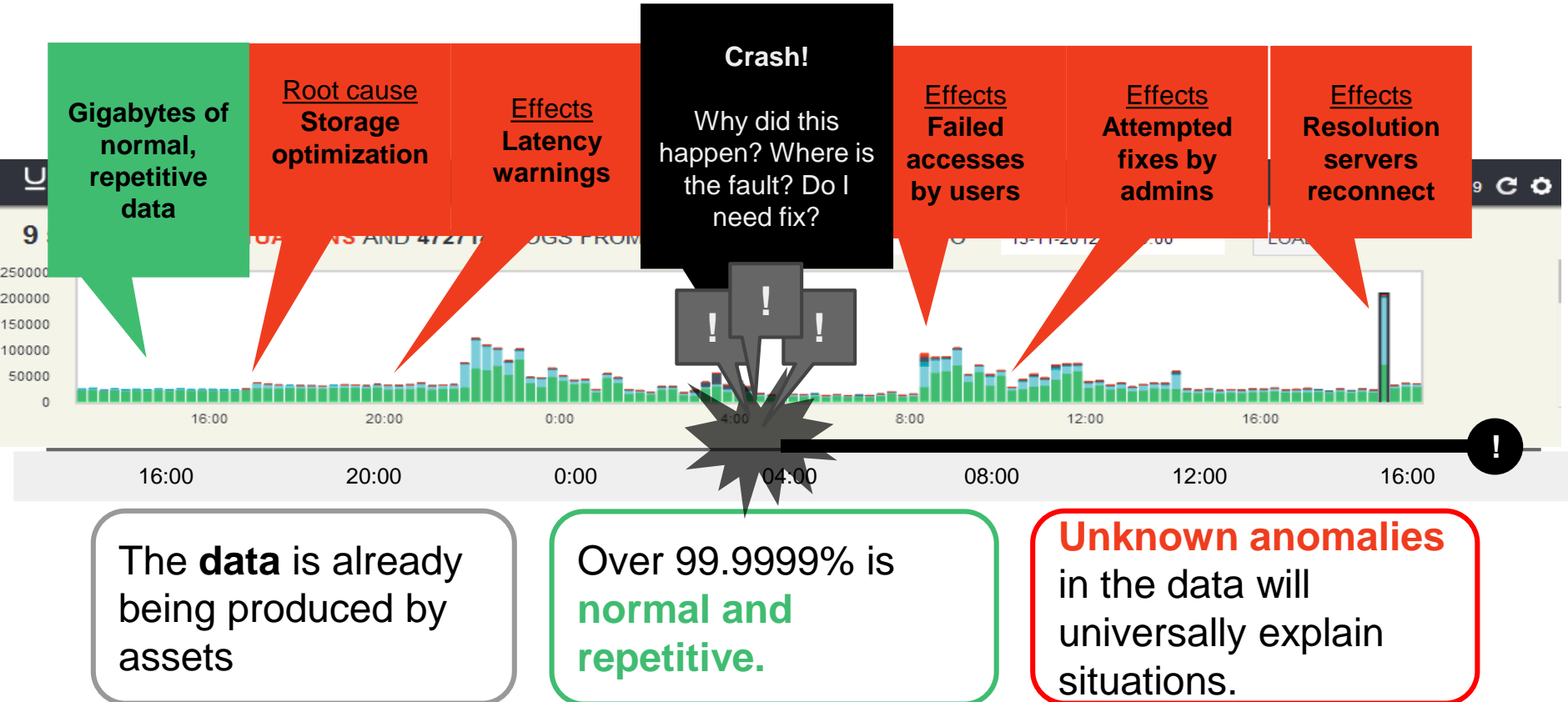


"Less than 1% of all data is analysed" /IDC

Every incident creates new or changing data

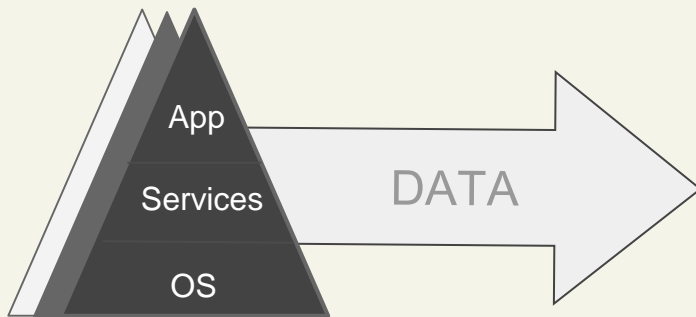
There is no substitute for this data and with this approach there is really no reason not to.

Real customer crash spanning 16 systems and impacting 250 systems



Software that installs and deploys on virtual, hardware or cloud

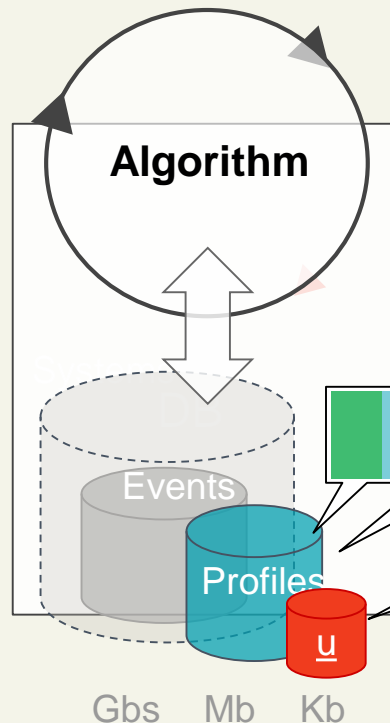
1. Send unstructured data from **any critical system**



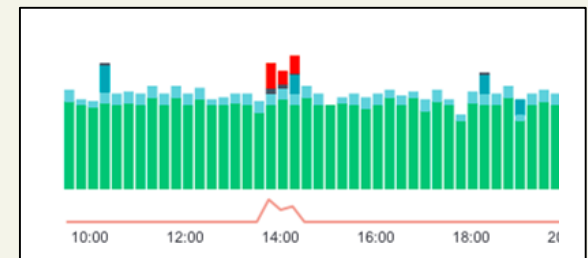
Via

Syslog	SNMP	tcp/udp
Hadoop	Splunk	ELK

2. Continuous profiling of **normal**



3. Automatically identifies **new data**

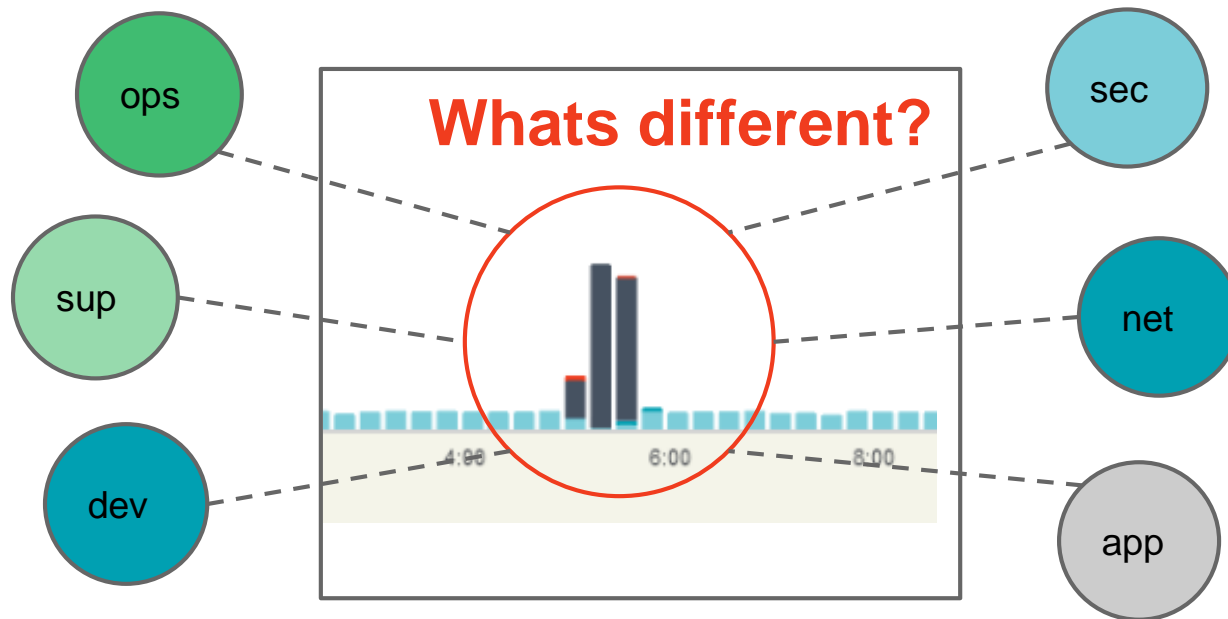


Memory Controller Read Error on Ch

4. Investigate, share, convert, explain, report

For an organisation this means that the hurdle of acting is removed

One focal point and ground truth for all stakeholders



**Reduced risk,
guesswork and
troubleshooting**

**Faster mean
time to detect,
repair and
recover**

**Improved
communication
and
collaboration**

**Enhanced
organisational
learning**

This is no magic, but a pragmatic way of resolving the underlying issue.

Benefits of the approach

1

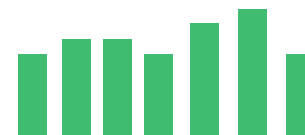
Independent

Any unstructured, high volume data in any variant means it can profile any software asset.

2

Automated

Continuously analyses and profiles assets out of the data they normally produce



3

Universal

Universally uncovers the unique, new and changing data that incidents create



4

Simple

Click to investigate
Alert and push
Convert data
Share and collaborate
Report

