Intalock

THE DATA SPECIALISTS

The Modern Response - A Defenders Perspective

Nathaniel Wieriks

Security Practice Manager
Nathaniel.wieriks@intalock.com.au
0411969958

Intalock
THE DATA SPECIALISTS

How would you PREVENT an APT attack?

You could:

- BLOCK all active content entering your environment
- BLOCK all changes to the windows start up keys

But would you?

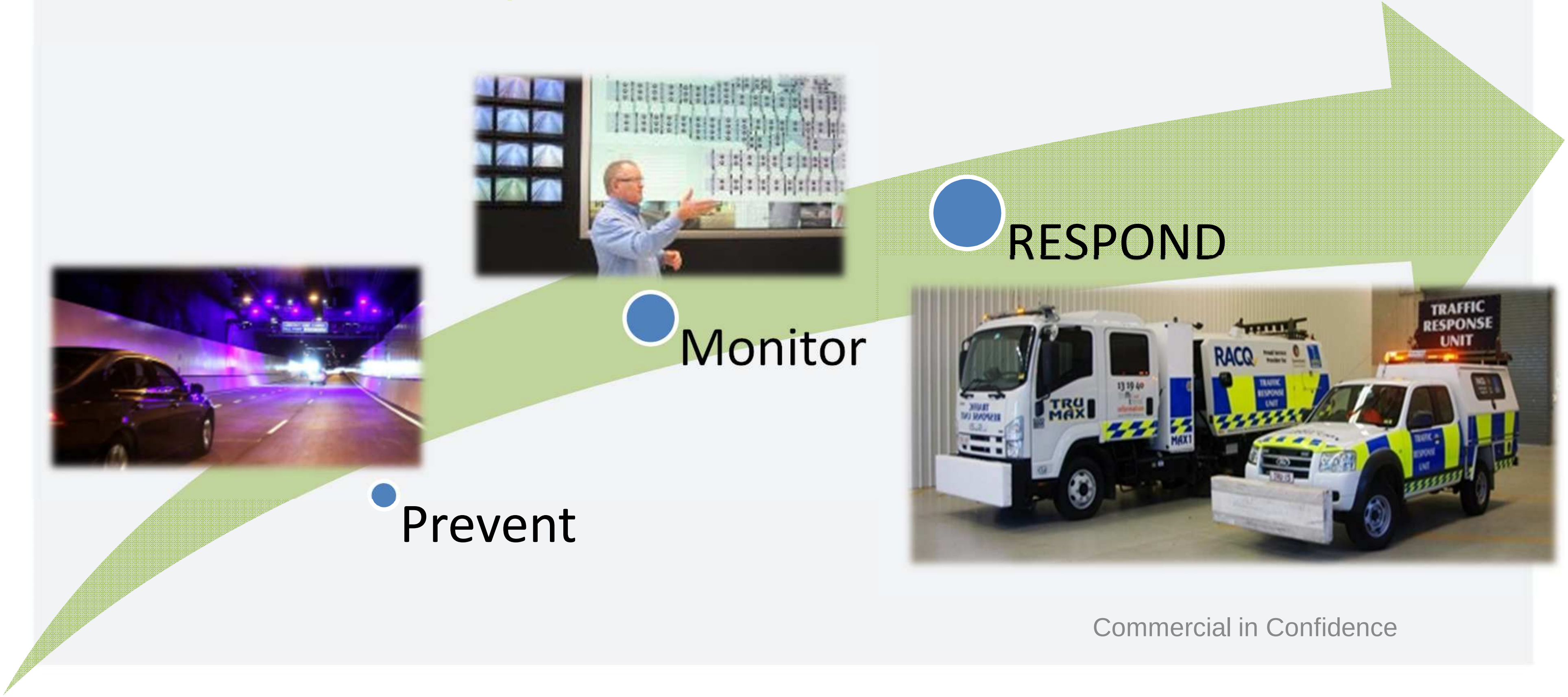
How would you DETECT an APT attack?

Maybe you should:

- MONITOR all active content entering your environment
- MONITOR all changes to the windows start up keys

Would you rather know?

What would you DO about an APT attack?



Prevent

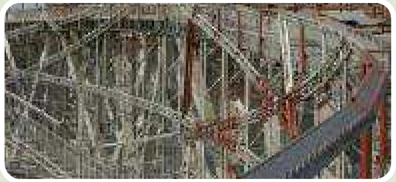
Monitor

RESPOND

Why do we have security?

Reduce the RISK of negative effects on company assets by ensuring:

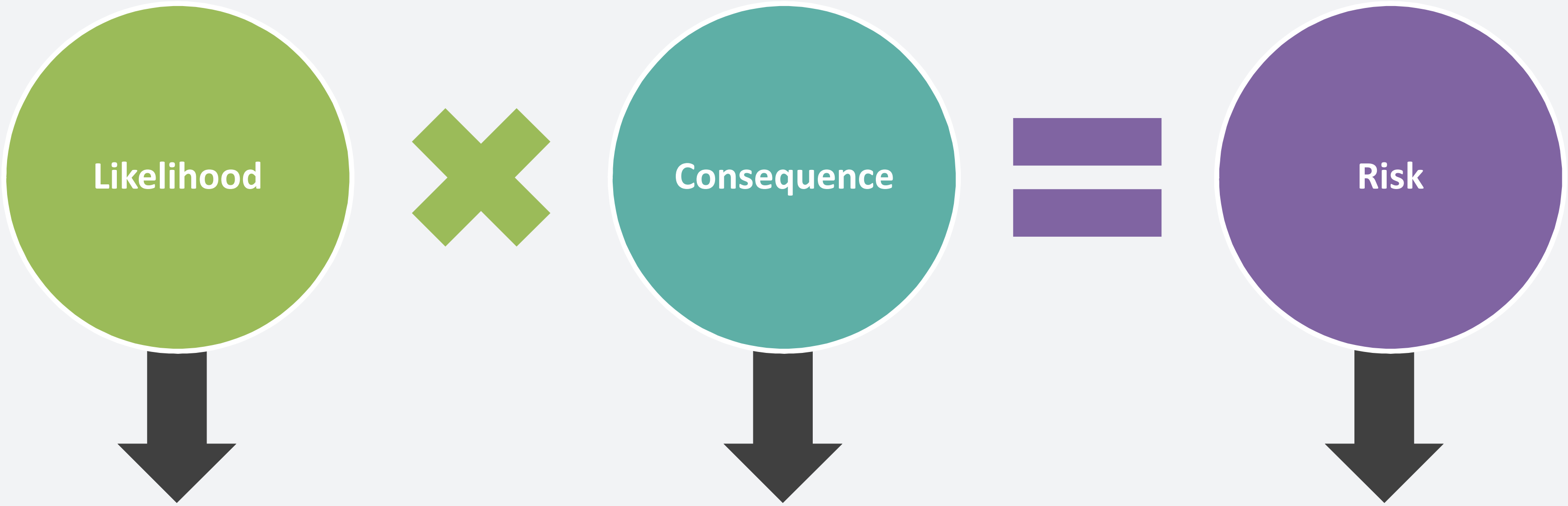
Confidentiality



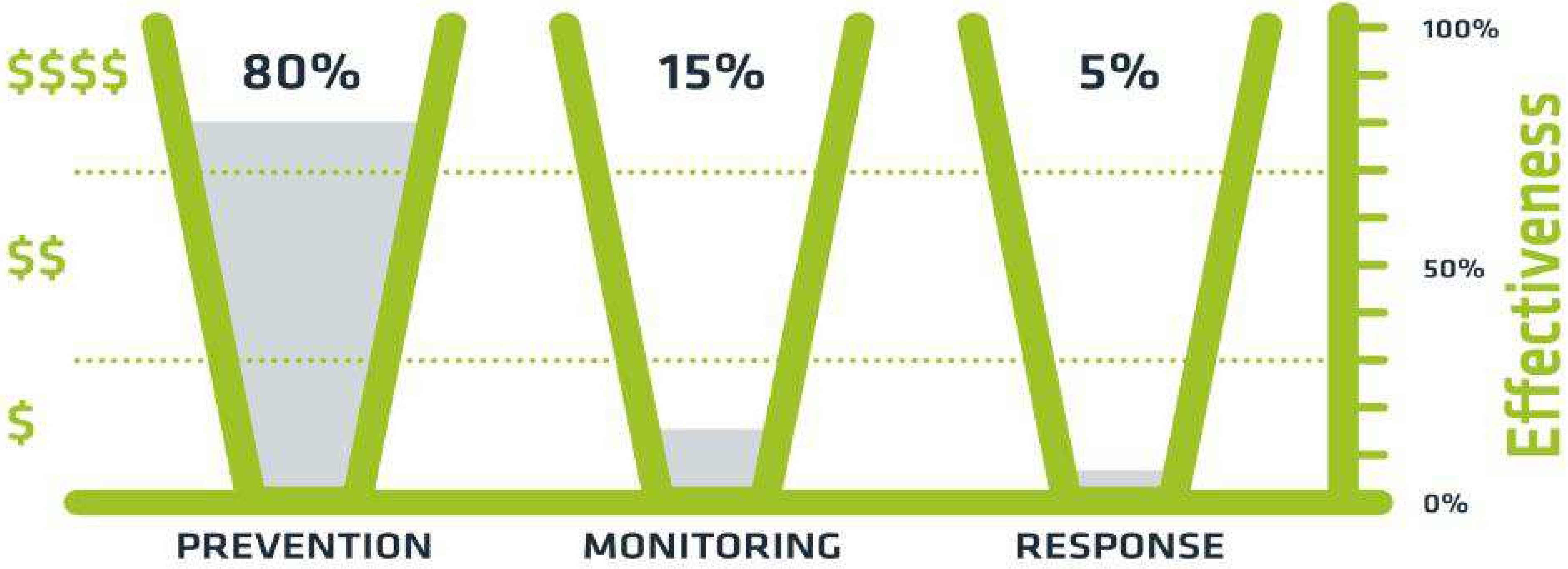
Integrity

Availability

How do you measure risk?

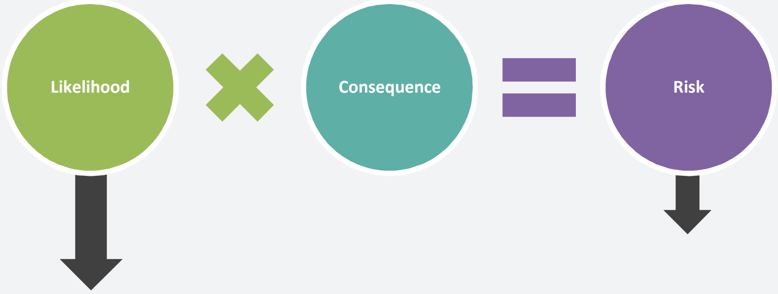


Traditional Ideal Security Budget Spend



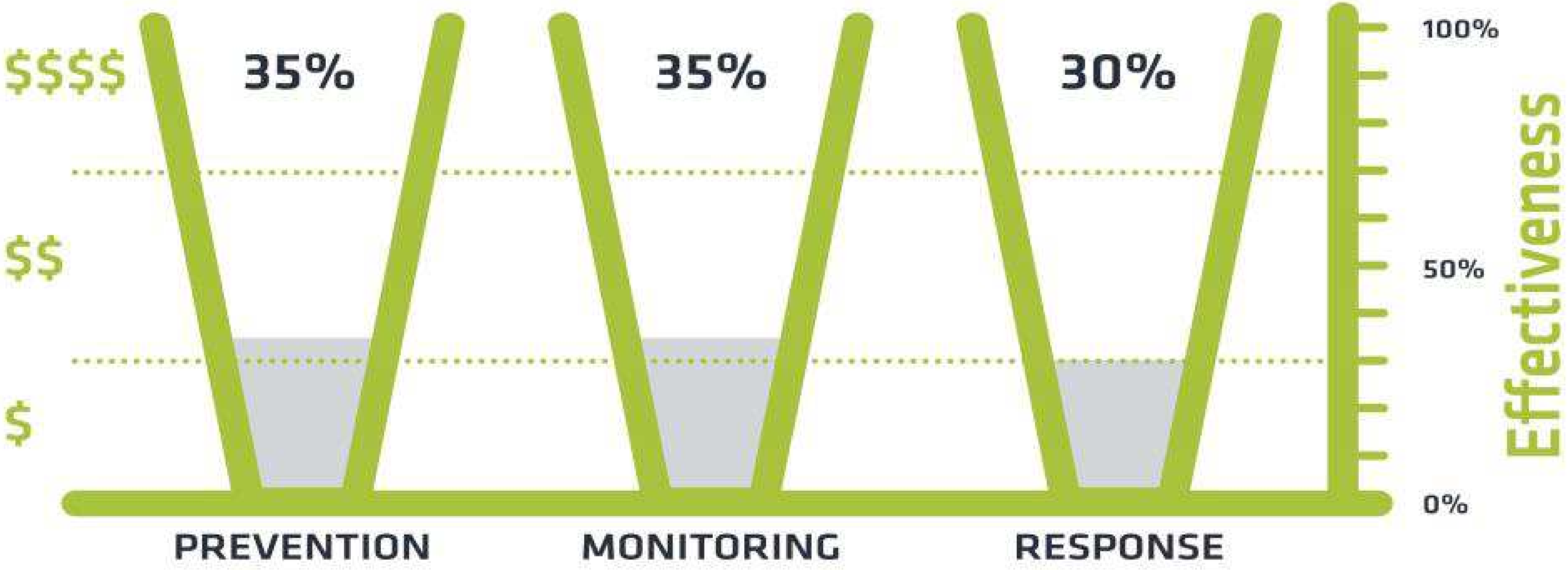
Total Budget spend 1.5 Million

How do traditional security methods reduce risk?



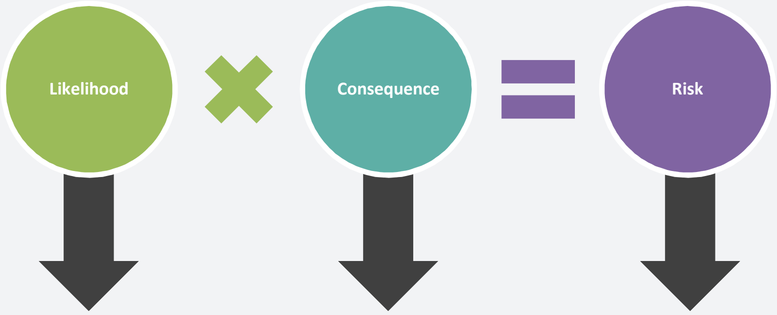
Prevention/Blocking technologies reduce **Likelihood**….ONLY

Balanced Ideal Security Budget Spend



Total Budget spend 900K

How do modern security methods reduce risk?



Monitoring and Response methods
reduce **Consequence**...EFFECTIVELY

Intalock

THE DATA SPECIALISTS