City of Baltimore
$18M Ransome

Equifax
143M credit records exposed

Wanna Cry
Ransom of computers world wide

US Voter Registry 2017
198M Voter Records

Target
40M credit cards, 110M personal records
Each had a patch available, that was not applied.
48% Of all companies have experienced a cybersecurity breach

57% Breached due to an unpatched vulnerability

34% Knew they were vulnerable before they were breached
THE PROBLEM

Corporations, (and State and Local Governments), have poor cyber hygiene, and can't keep up with the basics

- OS Patching
- 3rd Party Software Patching
- Software Deployment
- Configuration Management
Majority of corporate security investment on vulnerability management “Detection”

PROTECTION vs. DETECTION

Detection

Protection
Patching Software Deploy Config Mgt

Be a smaller target ™
Automation of cyber hygiene fundamentals
CORPORATE THREAT SURFACE

Breakdown of the most common security issues identified by:

- Unpatched: 60%
- Misconfigured: 20%
- Bad Behavior: 20%

80% of the corporate attack surface can be eliminated through patching and config management.
OS Patching

Solution 1

Solution 2

Solution 3

OS Patching

3rd Party Software Patching

Deploy / Enforce Required Software

Configuration Settings (pswd, USB, etc)
Automate the fundamentals of Cyber Hygiene

- OS Patching
- 3rd Party Software Patching
- Configuration Settings (pswd, USB, etc)
- Deploy / Enforce Required Software
CLOUD BASED
View and report on the patch vulnerability and compliance status of your full infrastructure

CROSS PLATFORM (Win, Mac, Linux)
Set OS and 3rd party patching policies that are automatically enforced

FULLY AUTOMATED
Establish and enforce a broad set of configuration policies that simplifies regulatory compliance

LOW COST / DAY ONE ROI
Begin patching systems within minutes of installation
WHO IS BUYING?
Thank you