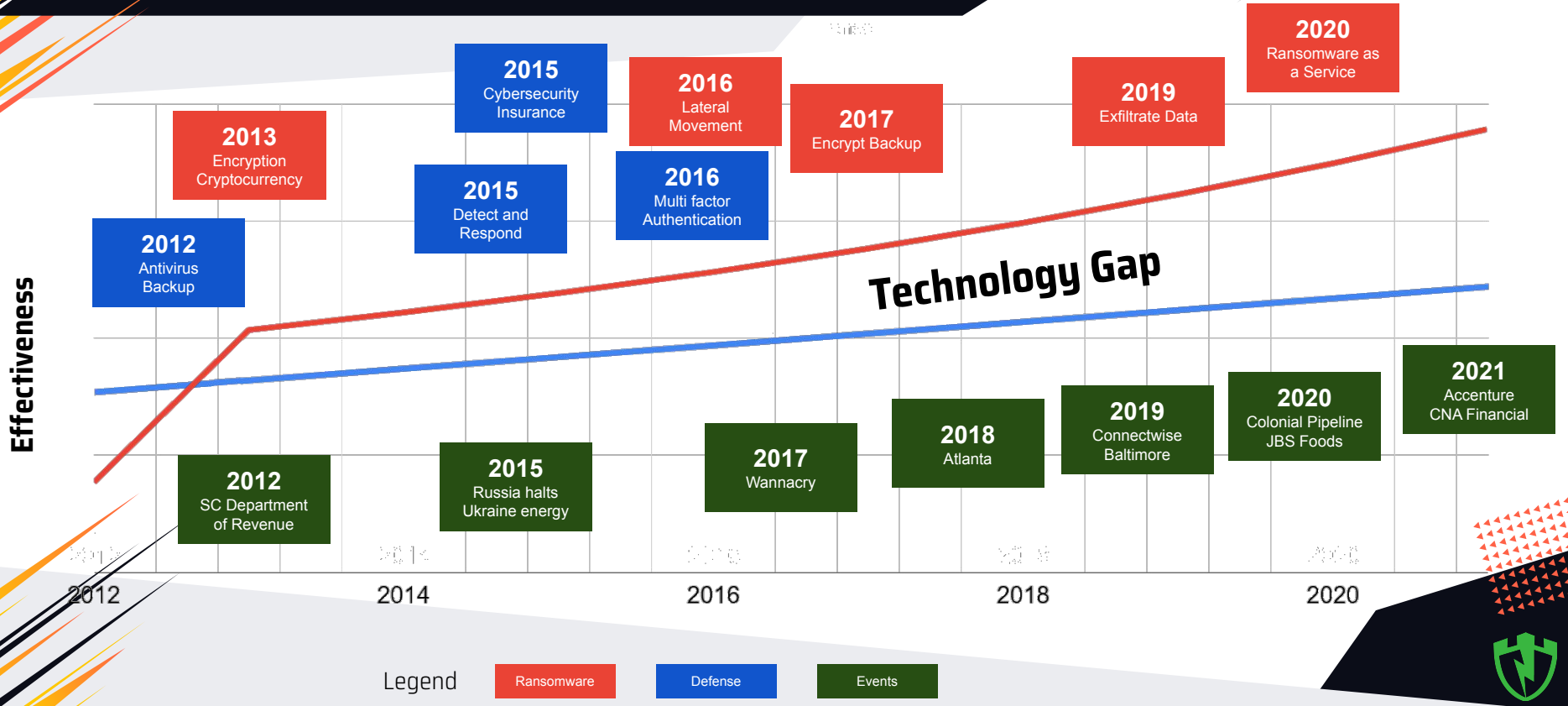
WE ARE NOT THEM
ROB CHENG / CEO / PC MATIC

HELLO!

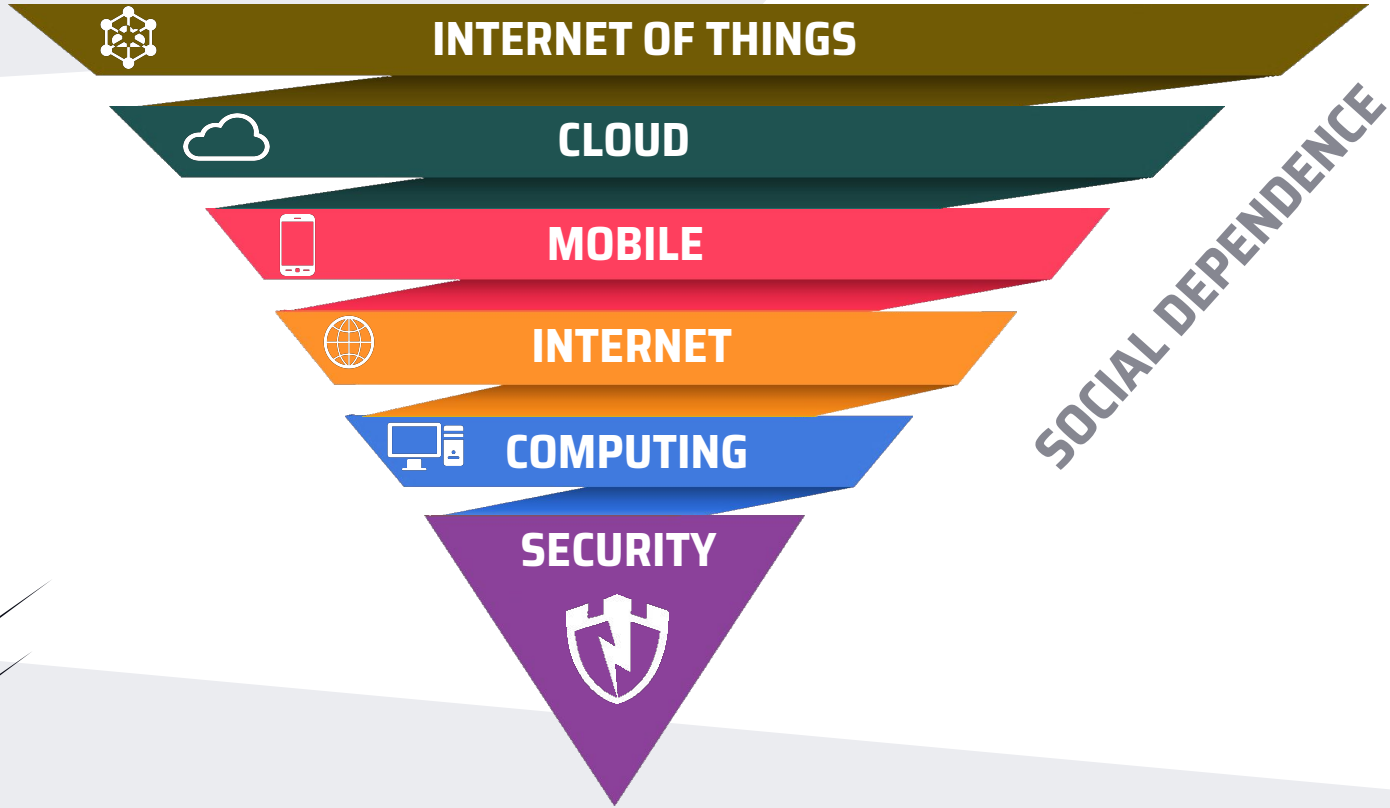
I am Rob Cheng

- 1999 - CEO / Founder PC Matic
- Myrtle Beach SC
- 2011 - American made antivirus based on whitelist

THE CYBERSECURITY TECHNOLOGY GAP



SECURITY IS THE FOUNDATION OF DIGITAL FUTURE



CYBERSECURITY ALL STARS

NIST ZERO TRUST CENTER OF EXCELLENCE

AUGUST 2021, PC MATIC IS SELECTED AMONG 24 OTHER CYBERSECURITY COMPANIES.

NIST CENTER OF EXCELLENCE BY LOCATION

“THEY are the people that care more about money and wealth than good cybersecurity.

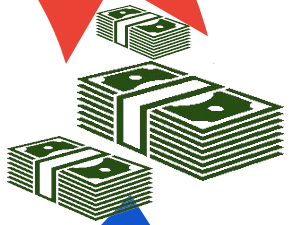
THE CYBER BUBBLE

Investors - The Future

The more money the ransomware industry makes, the more money the cybersecurity makes, the more investors borrow to fund these companies. The converse must be true for the ransomware threat to be thwarted.

Cybersecurity Industry

Ransomware Industry



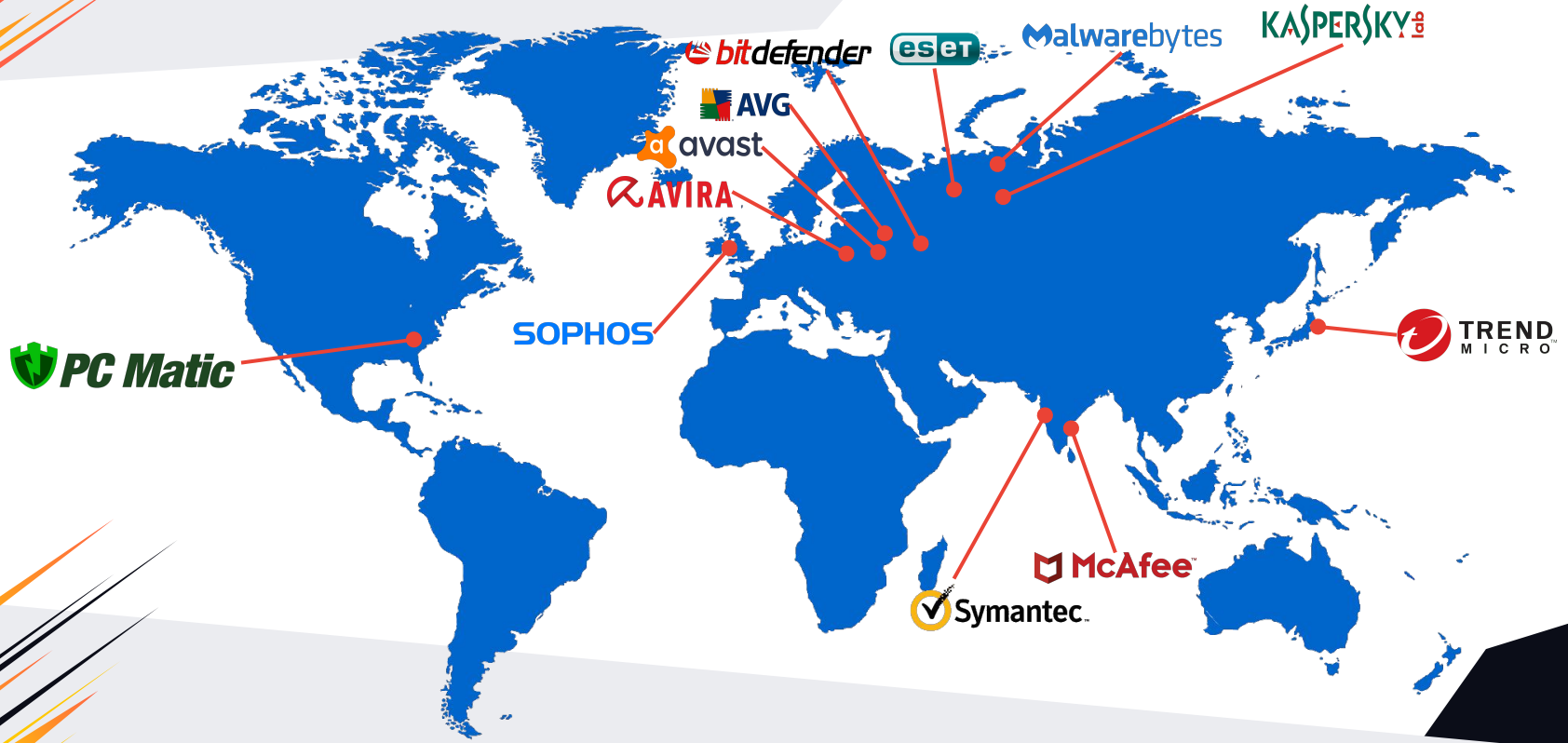
WE ARE NOT THEM

Information Technology

A CYBER BUBBLE ANALOGY

- Lemonade costs $.05 per cup and their costs are $1.00 per cup.
- For every cup sold, investors give the stand owners between $1.50 - $2.00 per cup.
- Investors are betting that you will continue to buy lemonade for the rest of your life.
- By funding large losses, investors are betting that no other lemonade stand can compete.
- This tactic stifles competition and innovation.
- This is the bubble.
- We are not them.

ANTIVIRUS COUNTRY OF ORIGIN



MADE IN AMERICA

- Creates American jobs
- Supply chain attacks
- More secure
- Live and work by the same rules with the same law enforcement
- Cybersecurity is independence from other nations.

NIST CYBERSECURITY FRAMEWORK

FOUNDATIONAL

Identify (ID)

AM: Asset Management
BE: Business Environment
GV: Governance
RA: Risk Assessment
RM: Risk Management

PC Matic — ID:AM, PR:AC

FORESCOUT — ID:AM

"The activities in the Identify Function are ***foundational*** for effective use of the Framework"
– NIST Cyber Security Framework
version 1.1 - April 16, 2018

Protect (PR)

AC: Access Control
AT: Awareness Training
DS: Data Security
IP: Information Protection Processes and Procedures
PT: Protective Technology

PC Matic — ID:AM, PR:AC

TRAINING*
- KnowBe4 — PR:AT
- COFENSE — PR:AT

AUTHENTICATION*
- DUO — PR:AC
- okta — PR:AC
- AUTHY — PR:AC

Detect (DE)

AE: Anomolies and Events
CM: Security Continuous Monitoring
DP: Detection Processes

ANTIVIRUS*
- Trellix — DE:CM, DE:DP
- SOPHOS — DE:CM, DE:DP
- TREND MICRO — DE:CM, DE:DP
- Symantec — DE:CM, DE:DP

EDR/XDR
- CROWDSTRIKE — DE:CM, DE:DP, RS:AN, RS:MI
- Carbon Black. — DE:CM, DE:DP, RS:AN, RS:MI
- SentinelOne — DE:CM, DE:DP, RS:AN, RS:MI
- paloalto — DE:CM, DE:DP, RS:AN, RS:MI

PATCHING*
- tenable — DE:AE
- TANIUM — DE:AE

Respond (RS)

RP: Response Planning
CO: Communications
AN: Analysis
MI: Mitigation
IM: Improvements

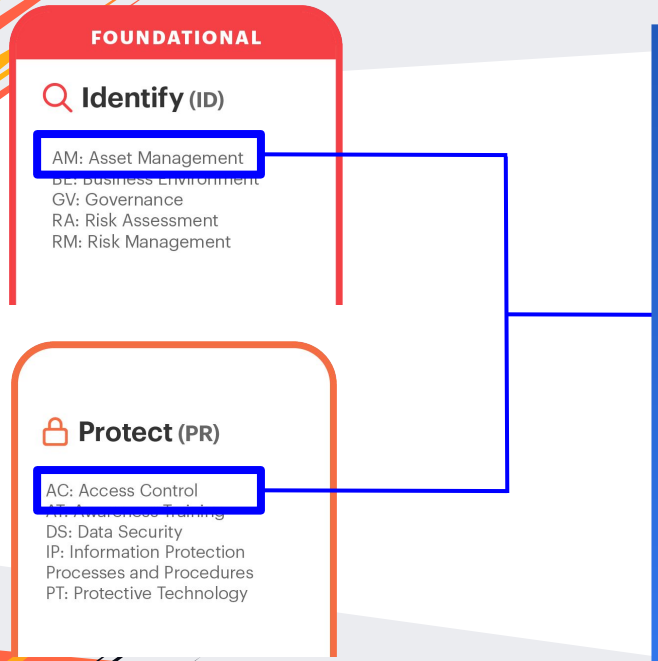
Recover (RC)

RP: Recovery Planning
IM: Improvements
CO: Communications

BACKUP*
- VEEAM — RC:RP
- datto — RC:RP
- Zerto — RC:RP

INSURANCE*
- AIG — RC:RP
- HISCOX — RC:RP
- CHUBB — RC:RP

SOFTWARE ASSET MANAGEMENT



- Asset Management is hardware and software.
- Know what's to be protected
- Software asset management is known as application whitelisting, application allowlisting, application control, and default deny.
- Access Control restricts based on what is known good.
- Everything is authorized
- This is foundational according to NIST.

SOLVING APPLICATION WHITELISTING GOVERNANCE

TWO COMPLEMENTARY WHITELISTS

- > 22B processes and scripts
- Updated hourly (24 x 7)
- Commercial and downloaded software

- Low prevalence and custom software
- Real time block notification
- Instantaneous remediation
- Whitelist hash, signature, or directory

ZERO DAY VULNERABILITIES

- Unknown security holes in good software
- 80% of internet went down in Italy due to a VMware vulnerability (Feb 2023)
- “This is How They Tell Me the World Ends” by Nicole Perlroth
- The United States, North Korea, China and Iran stockpile vulnerabilities in popular software

ZERO DAY VULNERABILITIES

Prevention

Identify (ID)

AM: Asset Management
BE: Business Environment
GV: Governance
RA: Risk Assessment
RM: Risk Management

Protect (PR)

AC: Access Control
AT: Awareness Training
DS: Data Security
IP: Information Protection Processes and Procedures
PT: Protective Technology

PC Matic	ID:AM, PR:AC
FORESCOUT	ID:AM
TRAINING*: KnowBe4	PR:AT
TRAINING*: COFENSE	PR:AT
AUTHENTICATION*: DUO	PR:AC
AUTHENTICATION*: okta	PR:AC
AUTHENTICATION*: AUTHY	PR:AC

"The activities in the Identify Function are ***foundational*** for effective use of the Framework"
– NIST Cyber Security Framework
version 1.1 - April 16, 2018

Reaction

Detect (DE)

AE: Anomolies and Events
CM: Security Continuous Monitoring
DP: Detection Processes

Respond (RS)

RP: Response Planning
CO: Communications
AN: Analysis
MI: Mitigation
IM: Improvements

ANTIVIRUS*	Trellix	DE:CM, DE:DP
ANTIVIRUS*	SOPHOS	DE:CM, DE:DP
ANTIVIRUS*	TREND MICRO	DE:CM, DE:DP
ANTIVIRUS*	Symantec	DE:CM, DE:DP
EDR/XDR	CROWDSTRIKE	DE:CM, DE:DP, RS:AN, RS:MI
EDR/XDR	Carbon Black.	DE:CM, DE:DP, RS:AN, RS:MI
EDR/XDR	SentinelOne	DE:CM, DE:DP, RS:AN, RS:MI
EDR/XDR	paloalto	DE:CM, DE:DP, RS:AN, RS:MI
PATCHING*	tenable	DE:AE
PATCHING*	TANIUM	DE:AE

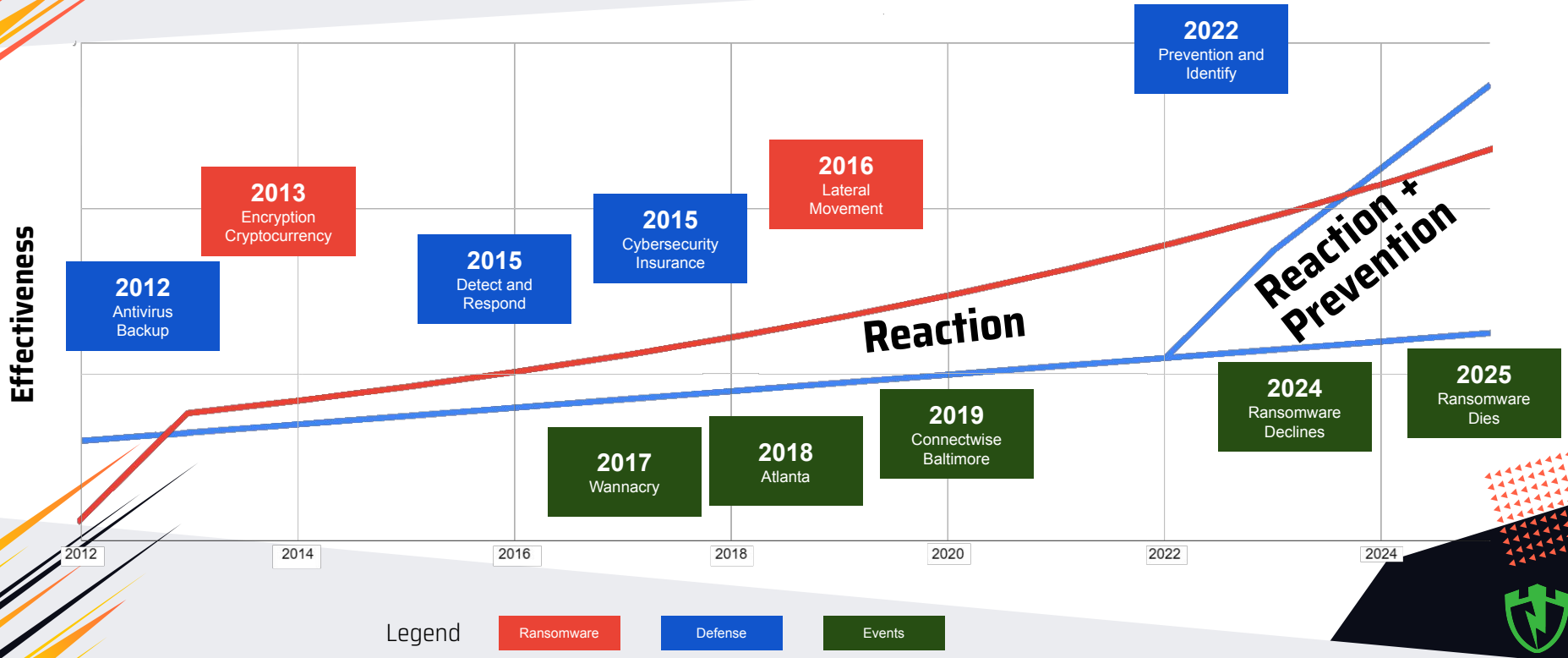
Recovery

Recover (RC)

RP: Recovery Planning
IM: Improvements
CO: Communications

BACKUP*	VEEAM	RC:RP
BACKUP*	datto	RC:RP
BACKUP*	Zerto	RC:RP
INSURANCE*	AIG	RC:RP
INSURANCE*	HISCOX	RC:RP
INSURANCE*	CHUBB	RC:RP

THE CYBERSECURITY TECHNOLOGY GAP



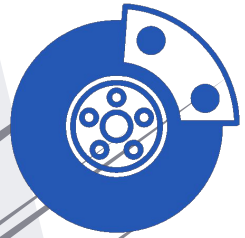
AIRBAGS HAVE IMPROVED AUTOMOBILE SAFETY

Airbags

- Minimizing Damage
- Worst case possible
- Add more airbags

Reaction

Brakes



- Prevention Foundational
- Prevention precedes reaction.
- Cars had brakes first.

Prevention

AMERICA'S CYBER MISSION

- Win Zero Day
- The best defense wins
- The first nation impervious to ransomware and nation state attacks.
- America's global power is restored.

THANKS!

Any questions?

Let's work together

- @chengrob
- rob@pcmatic.com

TRANSPARENCY SOLVES RANSOMWARE

COLONIAL PIPELINE

Transparency

- Highest profile ransomware attack
- Worldwide news
- Congressional Inquiry
- What antivirus failed?
- Koch Industries
- Opacity allows bad products to thrive.
- The market cannot function.