Point-of-Sale (POS) Malware: Tactics and Strategies for Protecting Customer Payment Information

Bit9 and Carbon Black

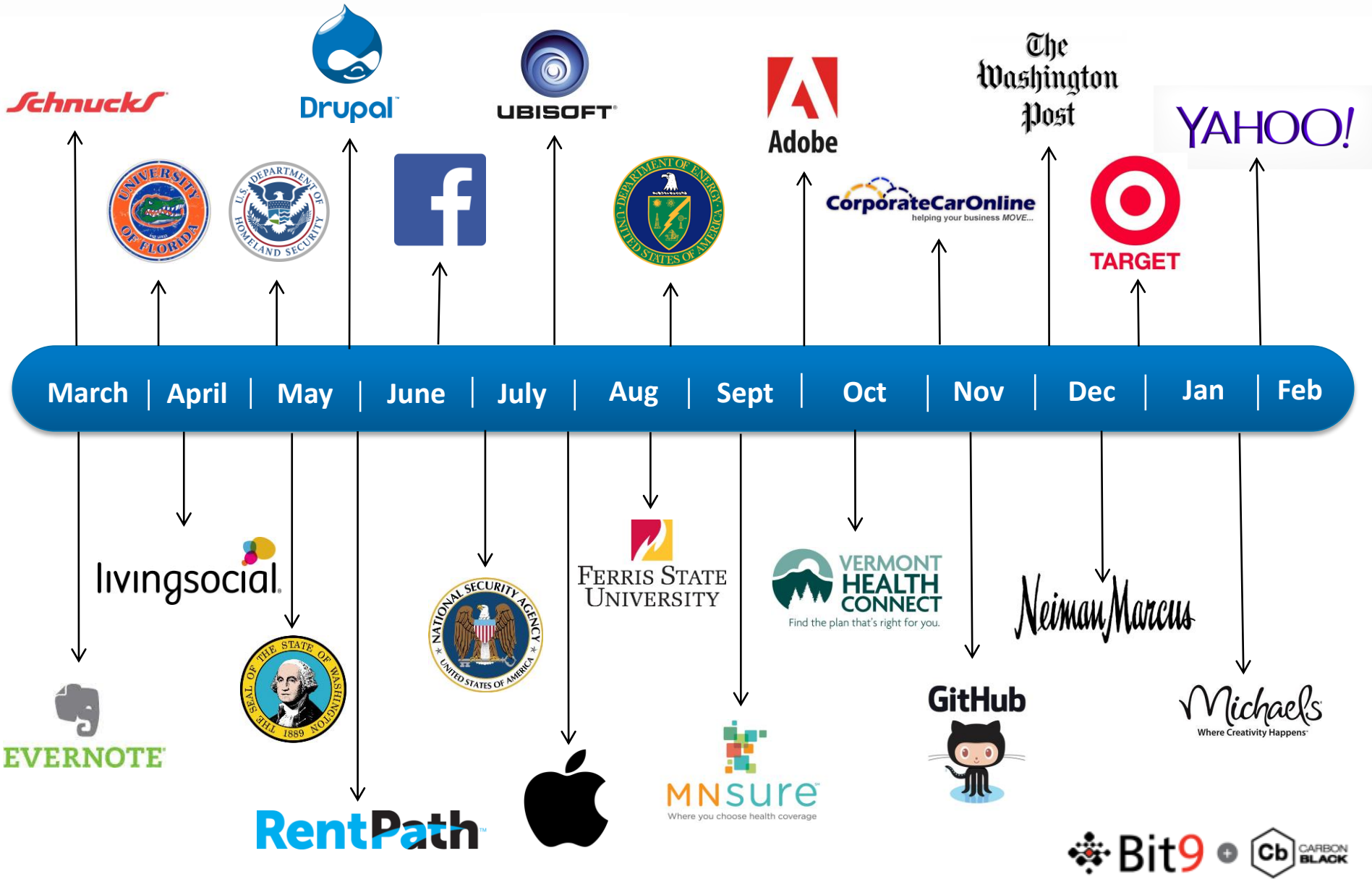
Jeffrey J. Guy | 20 Feb 14
jjguy@bit9.com
@jjguy

Introduction

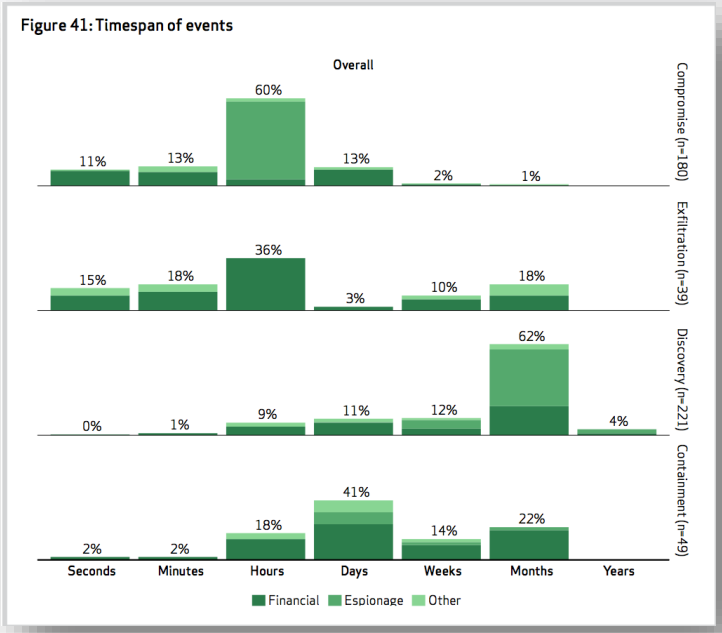
- **Jeffrey J. Guy**
  - Background
    - 6 years USAF, USAF Red Team
    - 7 years ManTech, CNO R&D services
    - 2 years at Cb, now Bit9
  - Director, Product Management at Bit9
    - Formerly Director of Operations at Carbon Black
- **Feb. 13, 2014**
  - Bit9 and Carbon Black merged to deliver single solution prevention, detection and response

Bit9 + Cb CARBON BLACK

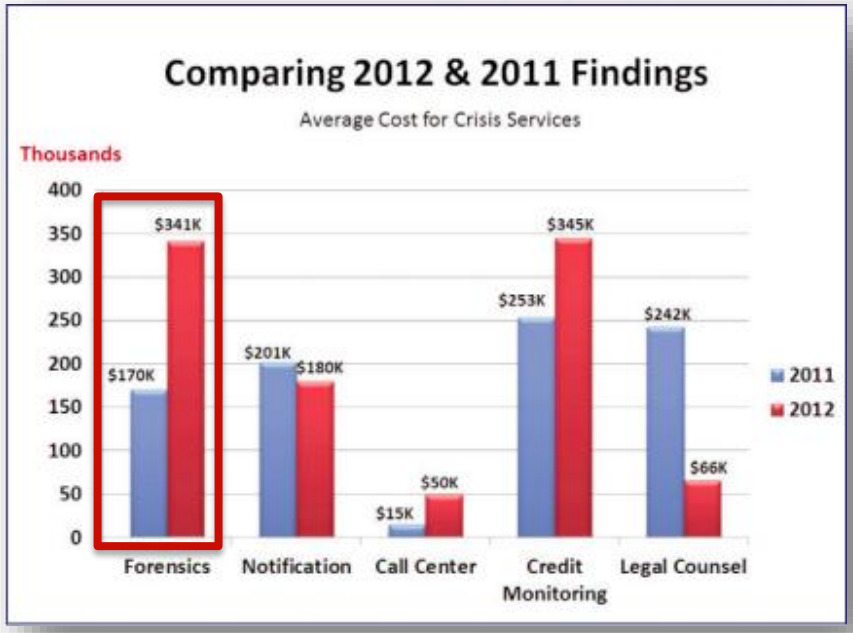
Assume You Will Get Breached (Last 12 Months)



The State of Information Security



Verizon 2013 Data Breach Report



NetDiligence, Cyber Insurance Claims Report

Compromise happens in seconds

Data exfiltration starts minutes later

It continues undetected for months

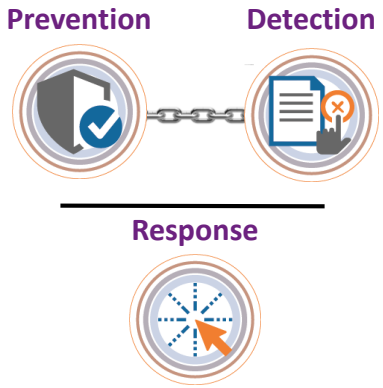
Remediation takes weeks

At $341k per incident in forensics costs

THIS IS UNSUSTAINABLE

Bit9 + Cb CARBON BLACK

Endpoint security is evolving



Traditional Security

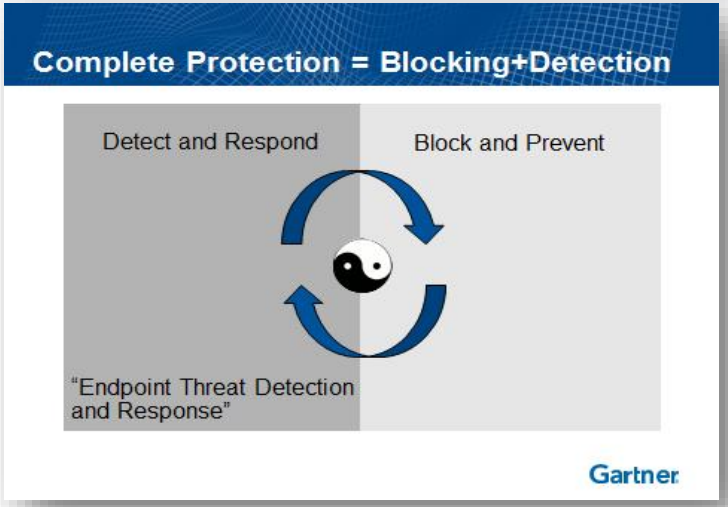
- **Prevention**: Provided by endpoint antivirus. Easily bypassed.
- **Detection**: Provided by endpoint antivirus. Efficacy limited to the opinion of your AV vendor's signature database.
- **Response**: Usually by external consultants.

Emerging Model

Prevention, detection and response as a single, integrated and continuous process.

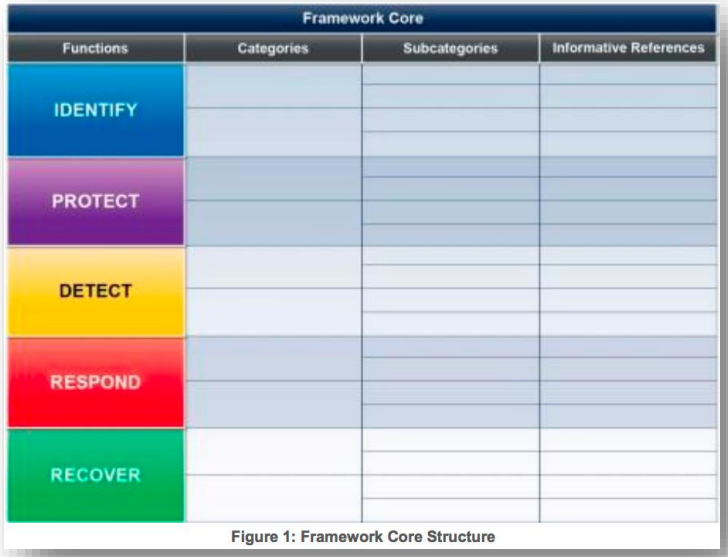
Bit9 + Cb CARBON BLACK

Protection = Prevention, Detection and Response



Gartner Endpoint Threat Detection and Response Tools and Practices, Sept. 2013

"Security…will shift to rapid detection and response capabilities linked to protection systems to block further spread of the attack."



NIST Cybersecurity Framework for Critical Infrastructure, Feb 2014

"Functions organize basic cybersecurity activities at their highest level. These Functions are: Identify, Protect, Detect, Respond, and Recover."

Bit9 + Cb CARBON BLACK

Prevention

Traditional Prevention

- Small local signature database of known-bad, wide-spread, well-known threats
- Single global database, centrally managed
- Efficacy limited to the opinion of your vendor's global database, at the moment of compromise

Emerging Prevention

- Local database of known-good applications
- Tailored policies to *your* environment, not the world's
- Lessons from network perimeter history: default-deny

Bit9 + Cb CARBON BLACK

Detection

Traditional Detection

- Small local signature database of threat data
- Single global database, centrally managed
- Efficacy limited to the opinion of your vendor's global database, ~~at the moment of compromise~~
- Only action is block, thus requires high confidence

Emerging Detection

- Large global database of threat data
  - IOCs, VirusTotal, iSIGHT, US Cert, Bit9 Software Reputation Service and ATIs
- Efficacy is the consensus opinion of the industry's collective intelligence
- Can block or flag for review, increasing overall utility
- True detection in depth

Bit9 + Cb CARBON BLACK

Response

Traditional Response

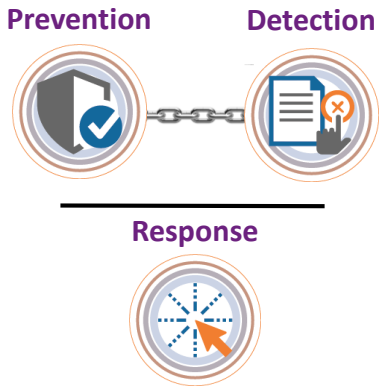
- Ad hoc, as-needed activity by expensive, external consultants
- Relies heavily on disk and memory artifacts for historical record
- Guidelines on IR prep (e.g., NIST 800-61, etc.) limit preparations to administrative measures

Emerging Response

- Even your entry-level staff can do IR in seconds
- Complete historical record of when/where/what/how
- Better, faster and cheaper than traditional IR

Bit9 + Cb CARBON BLACK

What Does This Mean for Your Security?



Traditional Security Bottom Line

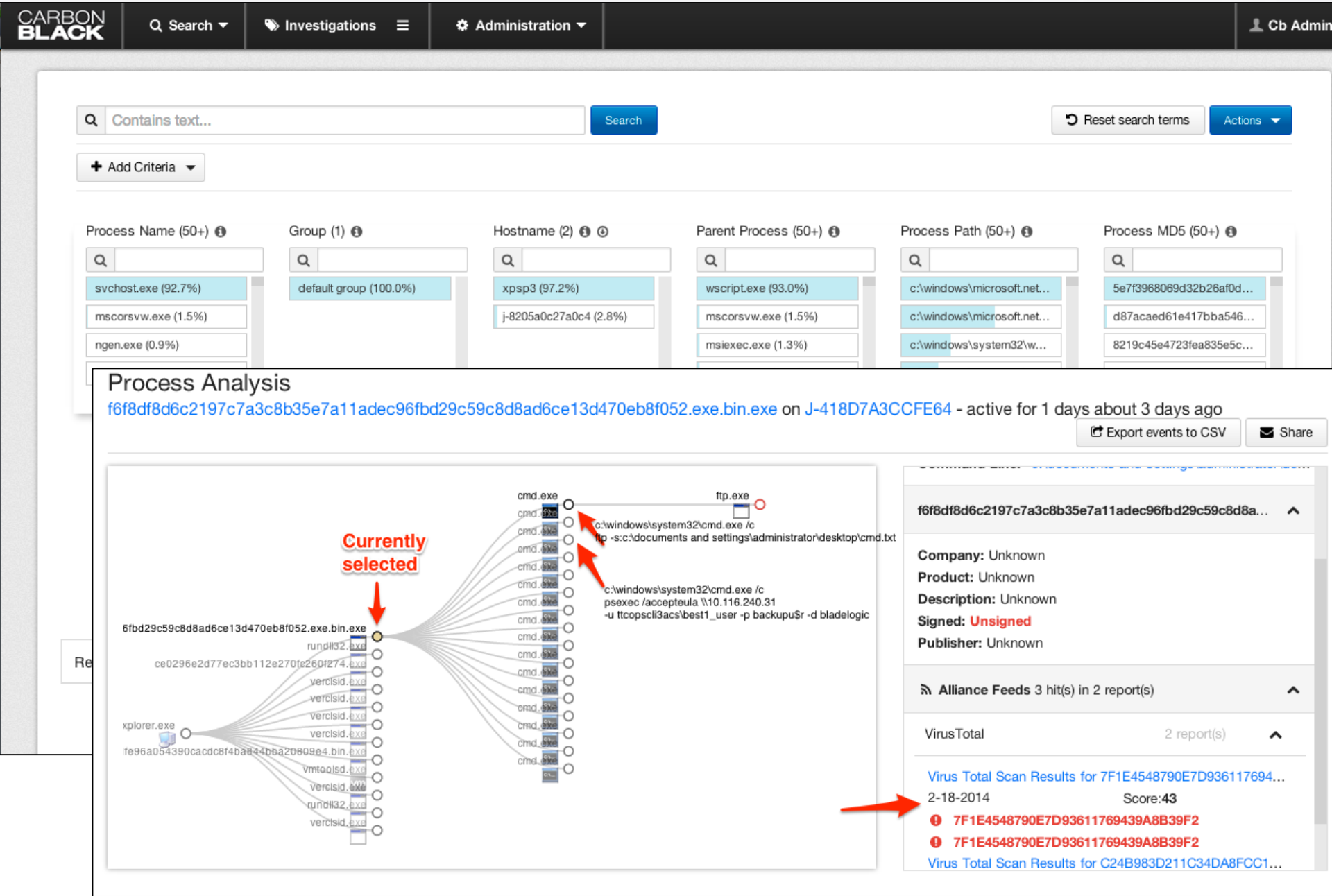
- **Prevention**: dependent on AV signature of your one chosen vendor *at the moment of compromise*
- **Detection**: dependent on AV signature of your one chosen vendor
- **Response**: expensive and time-consuming forensics, limited to present and future

Emerging Security Bottom Line

- **Prevention**: likely never runs, default-deny
- **Detection**: consensus opinion of the industry's collective intelligence
- **Response**: complete breadth and depth in seconds, including complete history

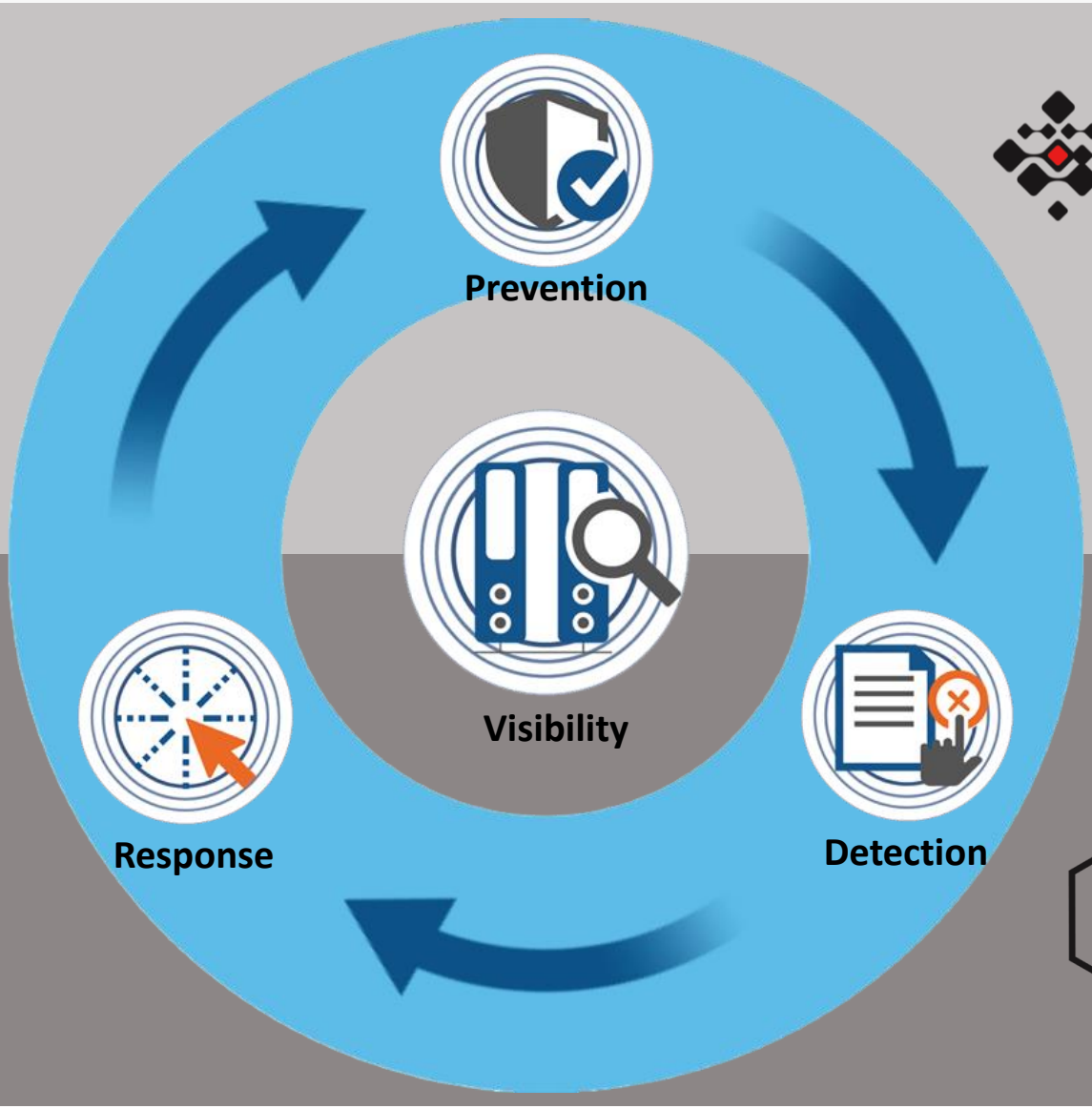
Bit9 + Cb CARBON BLACK

BlackPOS in Carbon Black – DEMO!



Security Lifecycle

Prevent



Detect & Respond

Bit9

CARBON BLACK

Come Say “Hi” at RSA!

Bit9 + Carbon Black Now One Company | Advanced Threat Protection Booth #827

Jeffrey J. Guy
jjguy@bit9.com
@jjguy

Bit9 + Carbon Black