Deception through History...
How to keep pace?

- <5 Hours to Break In
- 15 Hours to Exfiltrate Data
- 79 Days to Find
- 4.5 Hrs to Break Out
- 60% Move Laterally
- 12 Hours to Exfiltrate

Root Cause Analysis
Confident Response
Predictive Defenses
Attacks are Frequent and Costly

64% Of respondents confirmed their company experienced at least one successful attack on their endpoint(s)\(^1\)

$3.86M Average total cost of a data breach—and breaches that take over 30 days to contain can cost companies an extra $1 million\(^2\)

221 Days on average to identify the root cause of a criminal attack and another 81 days to contain it\(^3\)

---

\(^1\) Ponemon Institute 2018 State of Endpoint Security Risk, sponsored by Barkly
\(^2\) Ponemon Institute 2018 Cost of Data Breach Study, sponsored by IBM
\(^3\) Ponemon Institute 2018 Cost of Data Breach Study, sponsored by IBM
Attackers Are Out-Innovating Us

Attackers have access to the same technology that you do.

“Set and forget” is no longer an option.

We need a new approach.
CYBER DECEPTION IS ONE PIECE OF THE PUZZLE
You Need a Solution that Evolves with Attackers

Traditional Antivirus
Focuses on Prevention Only

Carbon Black
Provides Full Security Lifecycle

INTEL
NEXT-GEN AV

BEHAVIORAL ANALYTICS

ENDPOINT DETECTION & RESPONSE (EDR)

Prevent More Attacks

Analyzing Endpoint Behavior

>500B EVENTS PER DAY

MILLIONS OF ENDPOINTS

TIME

STOP NEVER SEEN BEFORE ATTACKS

STAY AHEAD OF EMERGING ATTACKS
What We Deliver

**SUPERIOR PROTECTION**
Prevent known and new threats as they evolve

**ACTIONABLE INSIGHTS**
Real-time investigation and remediation

**SIMPLIFIED OPERATIONS**
Operate faster and more effectively

*Reduce cost and complexity* by consolidating multiple security solutions
Carbon Black Is a Camera On Your Endpoints

- Metadata on every executed binary
- Network connections
- File modifications
- Cross-process events
- File executions
- Registry modifications
- No blind spots
- Continuous recording
- Proprietary data shaping
Quick & Easy Investigations

Access the complete activity record of any endpoint—even if it is offline

Intuitive attack chain visualizations—see what happened at every stage of the attack

Quickly uncover advanced threats and minimize attacker dwell time
Real-time Investigation & Remediation

- Secure shell access an endpoint
- Isolate infected systems
- Execute or kill processes
- Collect and store detailed data for later investigation
- Remove and ban malicious files
- Delete files
- Run custom scripts for full remediation

Result: Respond to and close security gaps in real time without IT involvement
Consolidated Endpoint Protection Platform

CB Predictive Security Cloud

COLLECTIVE INTEL

Next-Gen AV & EDR
Managed Alert Monitoring & Triage
Real-time Endpoint Query & Remediation
Advanced Threat Hunting
Virtual Datacenter Security

One Lightweight Agent

Everything you need to secure your endpoints
Time to Change the Game!

Make the attackers start playing by your rules.

Can’t Tell Real from Fake...  Increase the Attacker Costs...  Find an easier Target!
Final thought...

How Often Are Attackers Expecting Deception?

- 42% Anticipating
- Frequently 26%
- Unsure or Neutral 19%
- Rarely 33%
- Not At All 6%
- Always 16%

(450 sample size)
To Learn More Visit

www.carbonblack.com