CROWDSTRIKE

THE PROBLEM

ANDREW MUNCHBACH – MANAGER, SECURITY ENGINEERING

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

- Define the problem.
- Understand the problem.
- Work the problem.
- Adapt.
- Q&A

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

DEFINE THE PROBLEM.

What are we working with…

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

THE DEMOCRATIZATION OF CYBER THREATS.

The widespread availability of tools, techniques, and procedures that were, at one time, only available to and used by the most advanced threat actors.

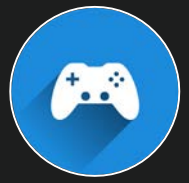
2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

- ETERNALBLUE
- ETERNALROMANCE
- BRUTALKANGAROO
- ETERNALROCKS
- DOUBLEPULSAR
- AND ON AND ON…

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

DEMOCRATIZATION OF IT

Cloud



IoT

BYOD

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

UNDERSTAND THE PROBLEM.

Okay, now what…

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

UNDERSTAND

Blue Team Problem

- If you're *defending* something, you're on the Blue Team
- With a prevention-only strategy, you have to be right 100% of the time.
- Attackers only have to be right once.

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

WORK THE PROBLEM

It’s okay if you cry a little in the process…

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

GET INFORMATION. GET IN THE WAY. GET OUT OF DODGE.

Detect

Disrupt

Remediate

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

ADAPT

The TSA paradigm…

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

TSA PARADIGM

- Belt
- Shoes
- Liquids over 3 ounces
- Jackets
- Laptops
- *Underware

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

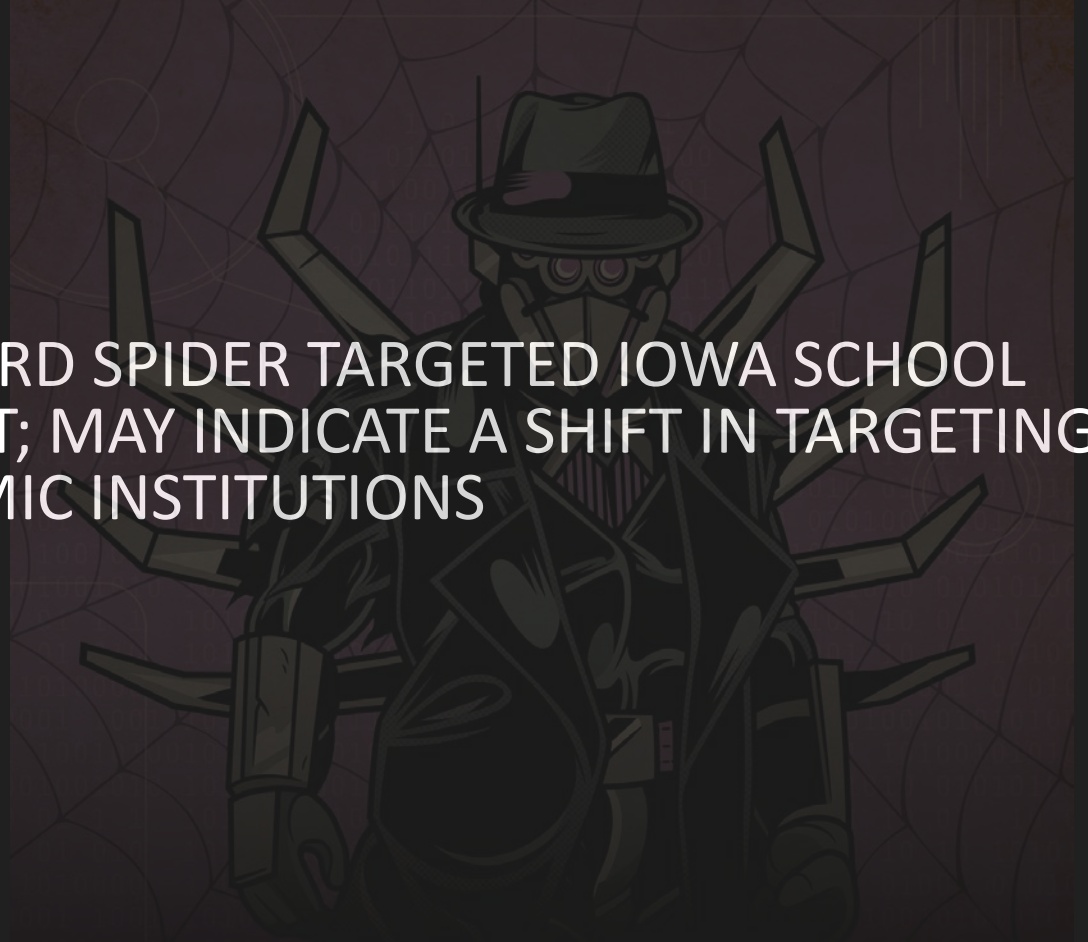
THE LAST ATTACK WILL LIKELY NOT BE THE SAME AS THE NEXT ATTACK…

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

…YOU NEED A TECHNOLOGY THAT CAN ADAPT ON YOUR BEHALF AND AT YOUR BEHEST.

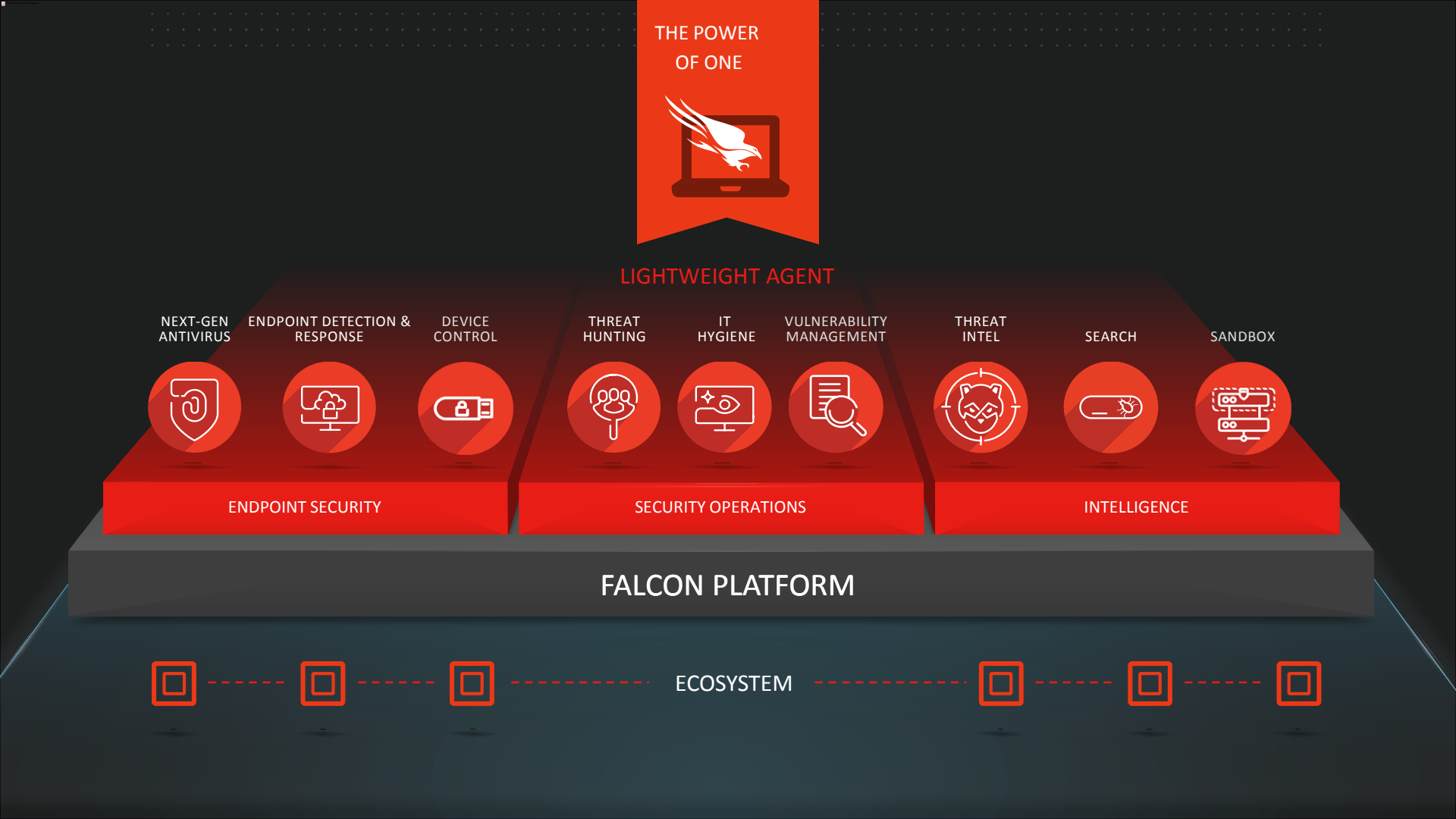
2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE



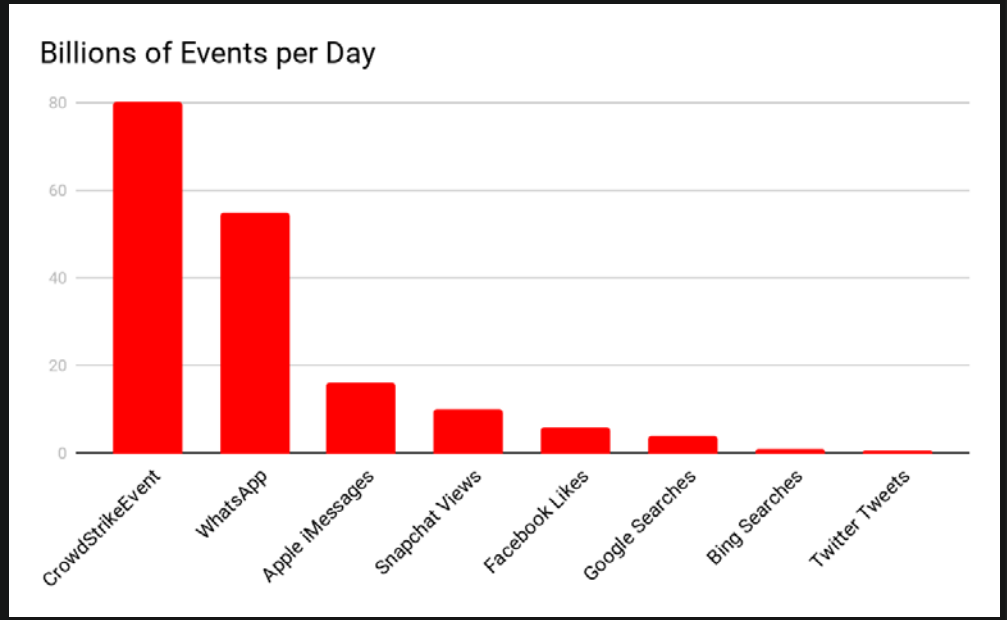
OVERLORD SPIDER TARGETED IOWA SCHOOL DISTRICT; MAY INDICATE A SHIFT IN TARGETING TO ACADEMIC INSTITUTIONS

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

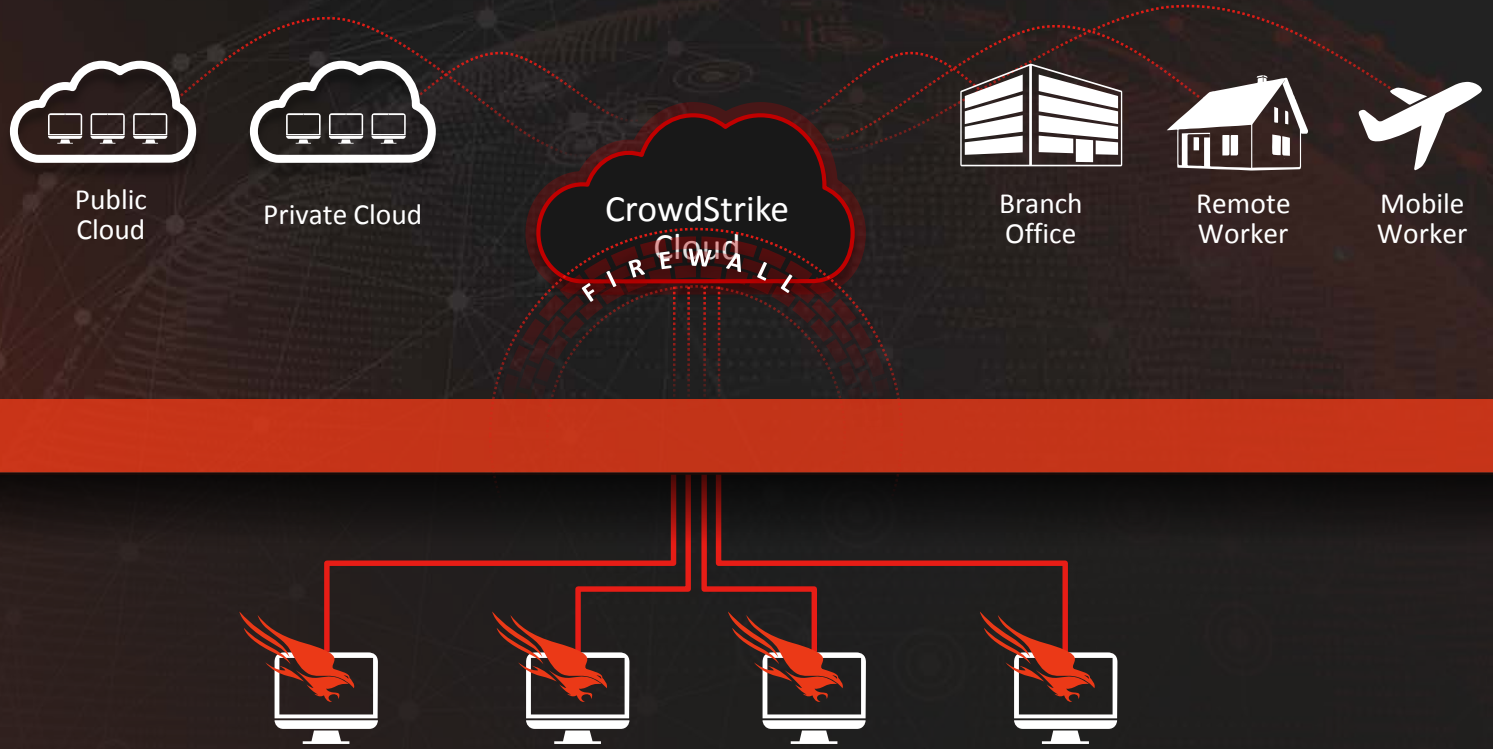

THE POWER
OF ONE
LIGHTWEIGHT AGENT
NEXT-GEN ANTIVIRUS
ENDPOINT DETECTION & RESPONSE
DEVICE CONTROL
THREAT HUNTING
IT HYGIENE
VULNERABILITY MANAGEMENT
THREAT INTEL
SEARCH
SANDBOX
ENDPOINT SECURITY
SECURITY OPERATIONS
INTELLIGENCE
FALCON PLATFORM
ECOSYSTEM

FALCON PLATFORM STATISTICS

Peak Events Per Second >2.42M	Average Events Per Second >900K
Data Processed Per Day >70 TB	Events Per Day >80B
Stored for ThreatGraph Mult. PBs	Stored for EDR Investigate Mult. PBs



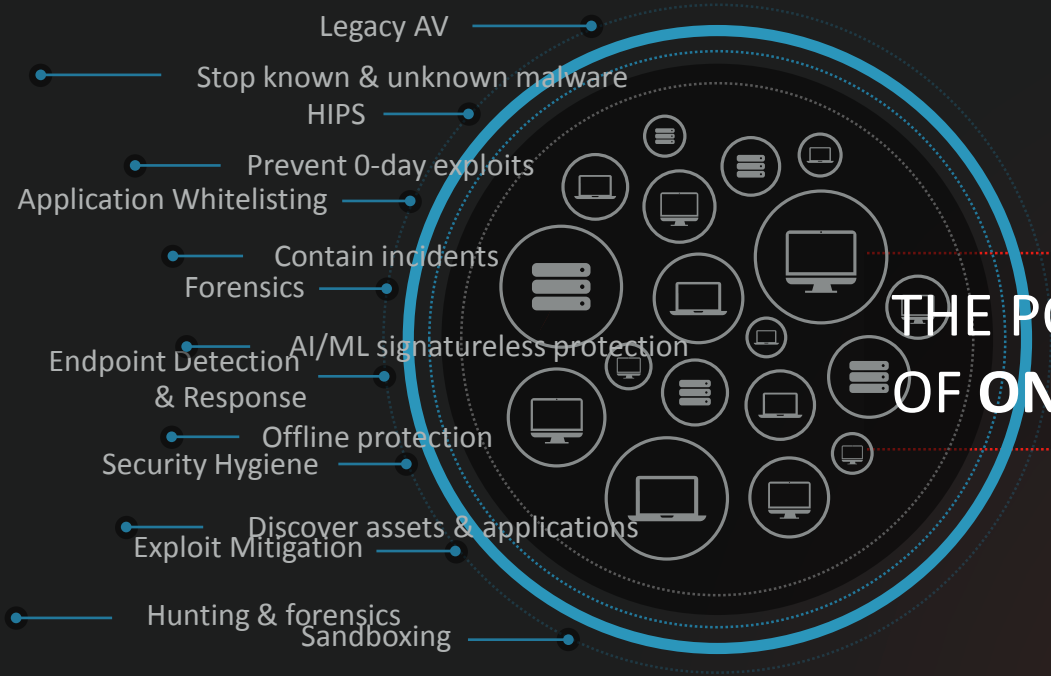
PROTECTING EVERY ENDPOINT EVERYWHERE



SOLUTION: CROWDSTRIKE FALCON

LEGACY SOLUTIONS

SINGLE LIGHTWEIGHT AGENT



THE POWER OF **ONE**

CROWDSTRIKE

MANAGED HUNTING – **FALCON OVERWATCH**

BENEFITS

BUSINESS VALUE

Stop the "Mega" Breach

Force Multiplier

Community Immunity

Reduce Alert Fatigue: Focus on What Matters

FINDING THE ADVERSARY
So You Don't Have To

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

CROWDSTRIKE

QUESTIONS?

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.