Sophos Intercept X

SOPHOS
Security made simple.

5 Example: NotPetya

$400M

2 Protection Tech

- Traditional ✓
- CryptoGuard ✓
- Machine Learning ✓
- Anti-Exploit ✓

4 Competitor Weakness

1
Primary Point of Failure

1 Attacker Tactics

- 400K malware samples per day — Known Threats
- \+
- $2,500 per victim — Ransomware
- \+
- 25% known / 75% unknown — Unknown Executables
- \+
- 1/4 malware weaponized office files — Exploits & File-less
- =

3 Our Advantage

Sophos
Power of the Plus

7 Why Deep?

Deep Learning Advantages

- Smarter
- More Scalable
- Lighter

6 Proof Point

5K/400/0
Flexible Systems

8 Sophos Difference

Machine Learning Experts

DARPA 2010 — EXPERIENCE	"One of the best ...ever." Maik Morgenstern CTO, AV-TEST — 3RD PARTY PROVEN
20ms — PERFORMANCE	+100 million — SOPHOS LABS

1 Types of threat

KNOWN THREATS Traditional approaches struggle to keep up with unknown threats 400K: The number NEW malware samples SophosLabs analyzes every day.

RANSOMWARE The gap in defenses has allowed new threats to arise, most notably ransomware. $2500: The average ransomware victim pays out $2500 per attack (Ponemon). 7% of the time they pay over $10K (Ponemon). Recently we've seen ransomware victim Reckitt Benckiser and Maersk shipping claim losses of $100 million and $300 million from ransomware.

UNKNOWN .EXE Attackers are constantly creating new malware variants, this unknown malware is more difficult for traditional techniques to detect. 75%/25%: Of the 400K samples analyzed by SophosLabs, approximately 75% of the samples are unique to that specific organization, meaning they are unknown.

EXPLOITS Adversaries have an arsenal of exploits and techniques at their disposal which they can use to execute file-less attacks, distribute malware, or make their attack more successful. ¼ weaponized: In fact, 26% (Verizon Data Breach Investigations Report 2017) of malware attacks used Weaponized Office files, where attackers used macros in Office files like Word docs as part of their attack.

2 Protection tech

TRADITIONAL To stop these threats historically we've used a combination of signatures and heuristics. This is what traditional endpoint security, including Sophos Endpoint, is based on. It works very well for known threats.

CRYPTOGUARD Our Intercept X product has a feature called CryptoGuard. When we see any malicious encryption happening we stop it in its tracks. Then we roll-back any changes made by the ransomware.

MACHINE LEARNING We employ deep learning, an advanced form of machine learning to detect unknown malware. Using the industry's #1 malware detection engine we're able to detect never-seen-before malware before it ever runs on the endpoint.

ANTI-EXPLOIT We also employ anti-exploit technology to frustrate attackers by preventing their favorite tools and techniques. Rather than examining millions of malware samples, we focus on approximately 25 exploits attackers rely on to spread malware, steal credentials, and escape detection.

3 Our Advantage: Power of the Plus

It's the **power of the plus** that really sets Sophos apart. We're the most comprehensive endpoint protection – thanks to our unique combination of techniques– built to stop the widest range of endpoint threats today and tomorrow.

4 Competitor Weakness: Single Point of Failure

Compare this to other vendors.Ask them what components do they have? How strong are each of their components? How does that add up? Others often rely only on one primary technique. What if it fails?

5 Threat Example

2017 saw big ransomware news including the WannaCry and NotPetya outbreaks. $400M: NotPetya cost companies like Fedex and Merck over $400M.

Traditional Sophos Endpoint stopped WannaCry once a signature was available. This technique requires a "first victim".

CryptoGuard Intercept X and Server customers were protected from WannaCry thanks to our CryptoGaurd technology. This requires the ransomware to execute.

Machine Learning Our machine learning technology was able to identify WannaCry as ransomware, stopping it before it executed.

Anti-Exploit Our anti-exploit technology in Intercept X was able to block DoublePulsar, the exploit used to install the malware, stopping before it ever got on the machine.

As you can see multiple layers of defense stop WannaCry. That's the power of the plus!

6 Customer Example

Flexible Systems "We deployed Intercept X to more than 5,000 endpoints. Since deploying, it has stopped 400 new ransomware attacks and we've had zero ransomware infections."

7 Deep Learning Drill Down

Deep learning has advantages over other types of machine learning.

Smarter Deep learning is able to automatically uncover the best combination and manipulation of inputs that would otherwise be impossible for humans to determine.

More Scalable Deep learning elegantly scales to hundreds of millions of training samples, meaning our model can "memorize" the entire observable threat landscape.

Lighter Another advantage is the small size of the model. Ours is only 12MB.

8 Sophos Machine Learning Experts

Experience Our model was created with DARPA driven technology for the 2010 Cyber Genome Program to uncover the "DNA" of malware and other cyber threats.

3rd Party Results Proven on VirusTotal & NSS Labs. Maik Morgenstern, CTO of AV-TEST, said our results were "one of the best performance scores we have ever seen in our tests".

Performance In 20 milliseconds we are able to extract millions of features from a file, run them through our host-based model, and determine if it is benign or malicious.

SophosLabs Our team of data scientists are part of the SophosLabs group, giving them access to hundreds of millions of samples to create the best possible models.