Leveraging AI and machine learning to fight today‘s digital threats

Vince Steckler, CEO Avast

July 12, 2017

AI and ML are hot buzzwords in security

- “AI based advanced threat prevention”
- “Hyper-dimensional security analytics”
- “Complex proactive behavioral modeling”
- “Next-gen”, “X-gen”

The data amounts in security are huge

- 3.5 billion malware attacks
- >500 million visits to malicious websites
- 20 to 30 million phishing attacks
- 20 to 30 million new executable files

Man vs. machine in security

Humans still win in certain areas

But machines are better in many other aspects

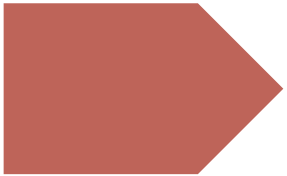
Key properties of AI and ML

Autonomous
New environments require reactions at super-human speeds

Explainable
Security decisions have real-world consequences

Self-improving
AI must stay up to date with new threats/trends/evasion techniques

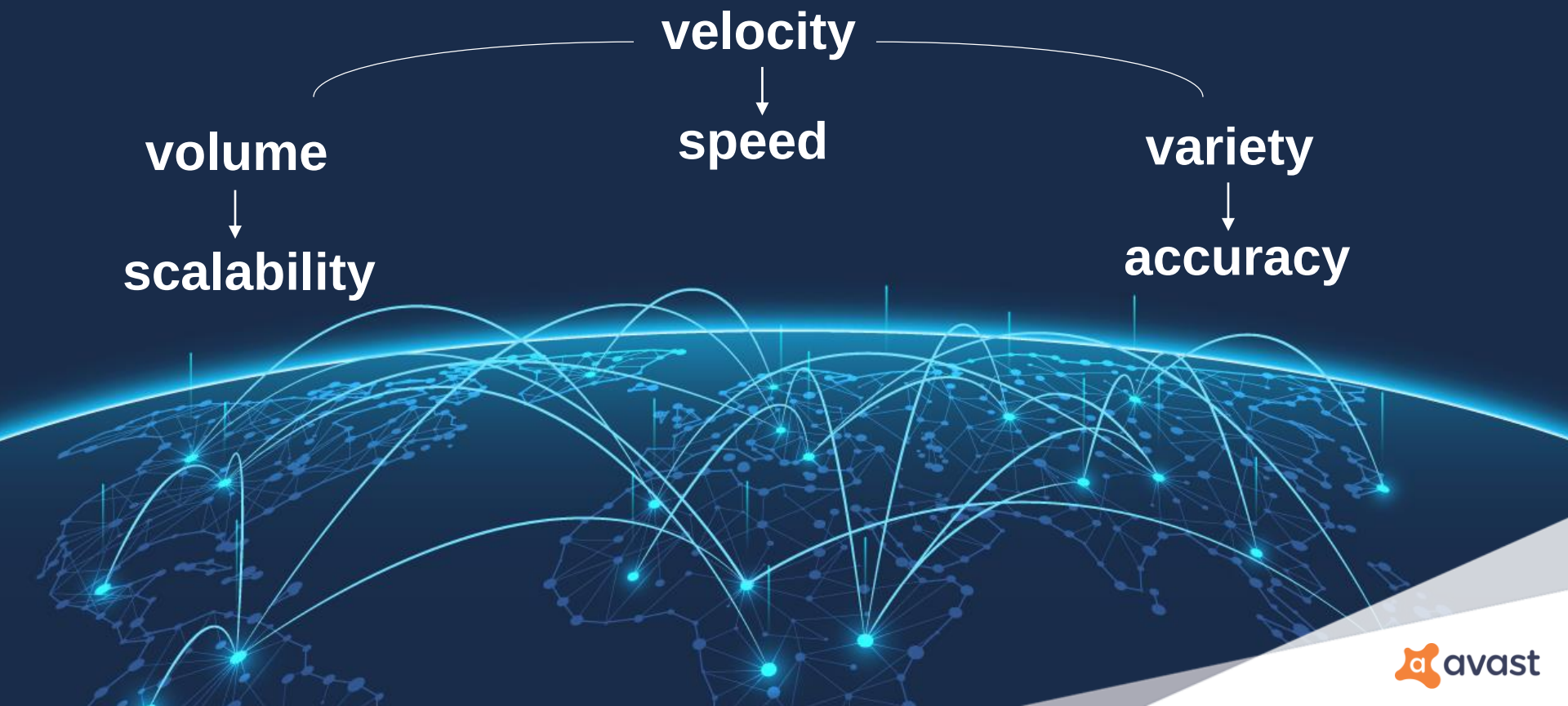
Self-defending
Defensive AI will be under attack all the time



Safe
AI systems have higher requirements in terms of code quality and robustness

avast

ML when applied to security is very powerful

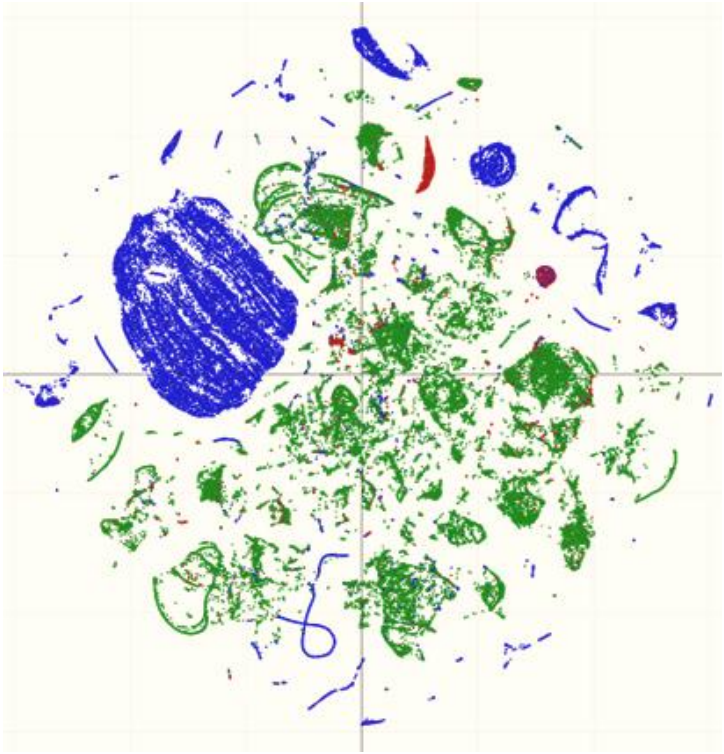


avast

Global connected devices

38,500,000,000

Teaching machines to fight malware – cluster example



CLEAN
MALWARE
PUP

Avast CyberCapture samples (N=100,000)
Using t-SNE to reduce dimension

avast


Thank you