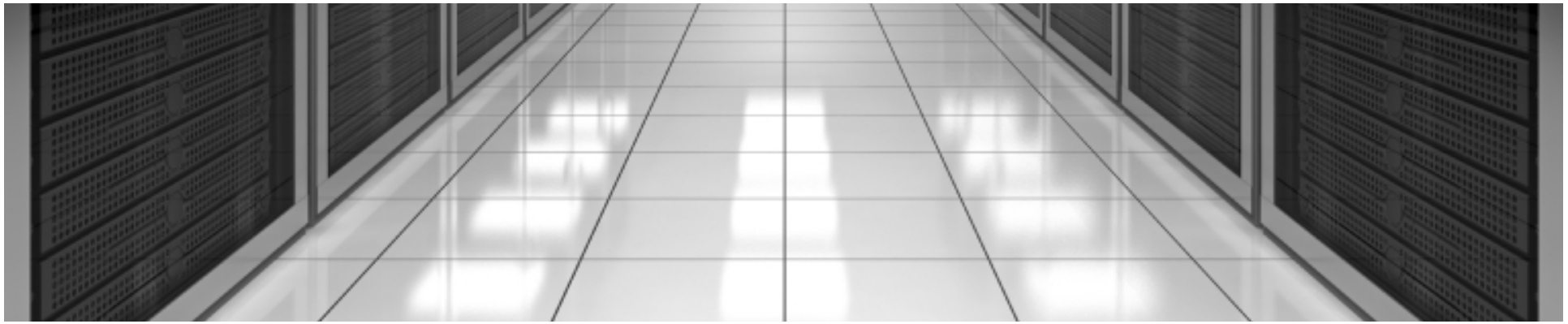
PERIMETER
E-SECURITY

AV VENDORS AREN'T
AS STUPID AS THEY LOOK

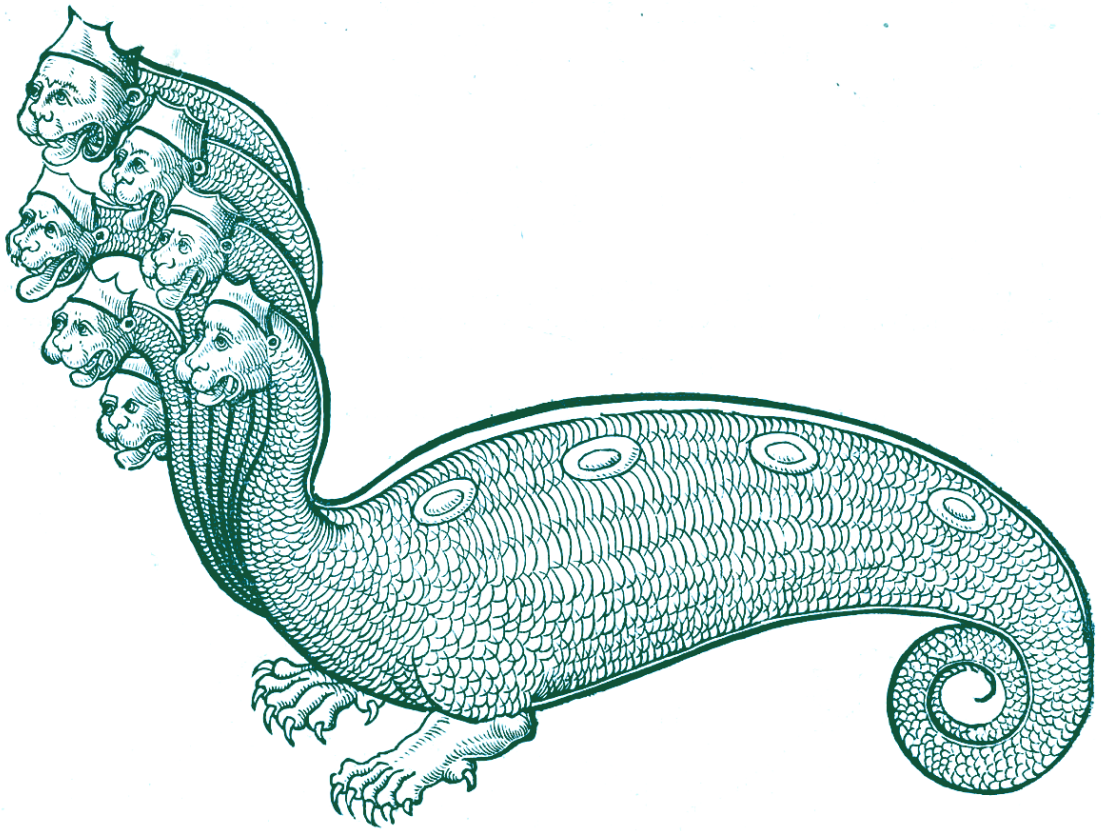


John Viega (john@viega.org)
EVP of Product and Engineering

PERIMETER
E-SECURITY

Anti-virus is a misnomer

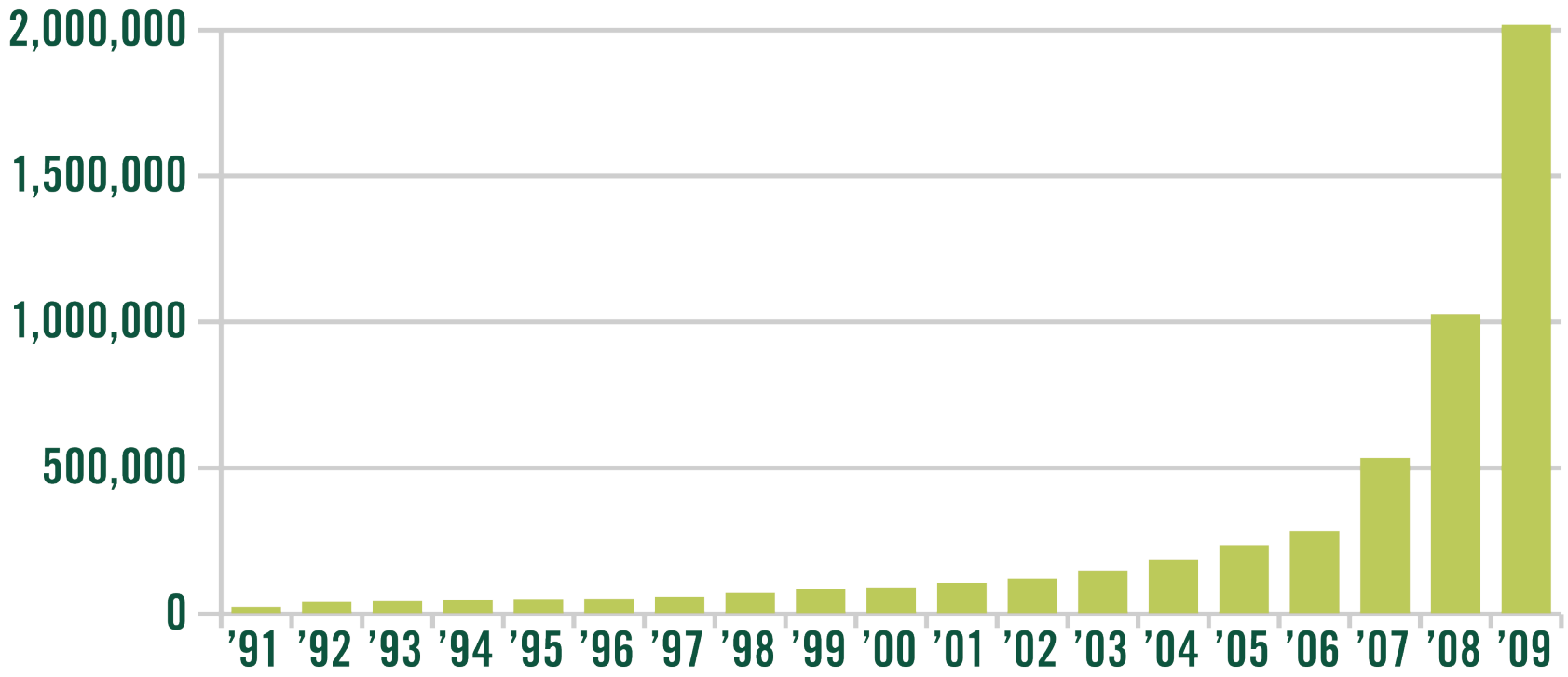
- Viruses
- Worms
- Botnet software
- Trojans
- Rootkits
- Spyware
- Adware
- Attack tools



- AV technologies try to eliminate it all
- Let’s generically say malware.

PERIMETER
E-SECURITY

Problem Scope

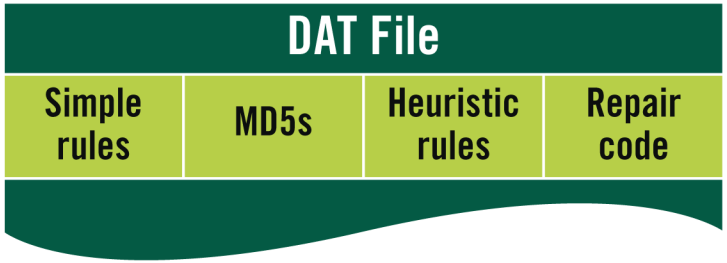


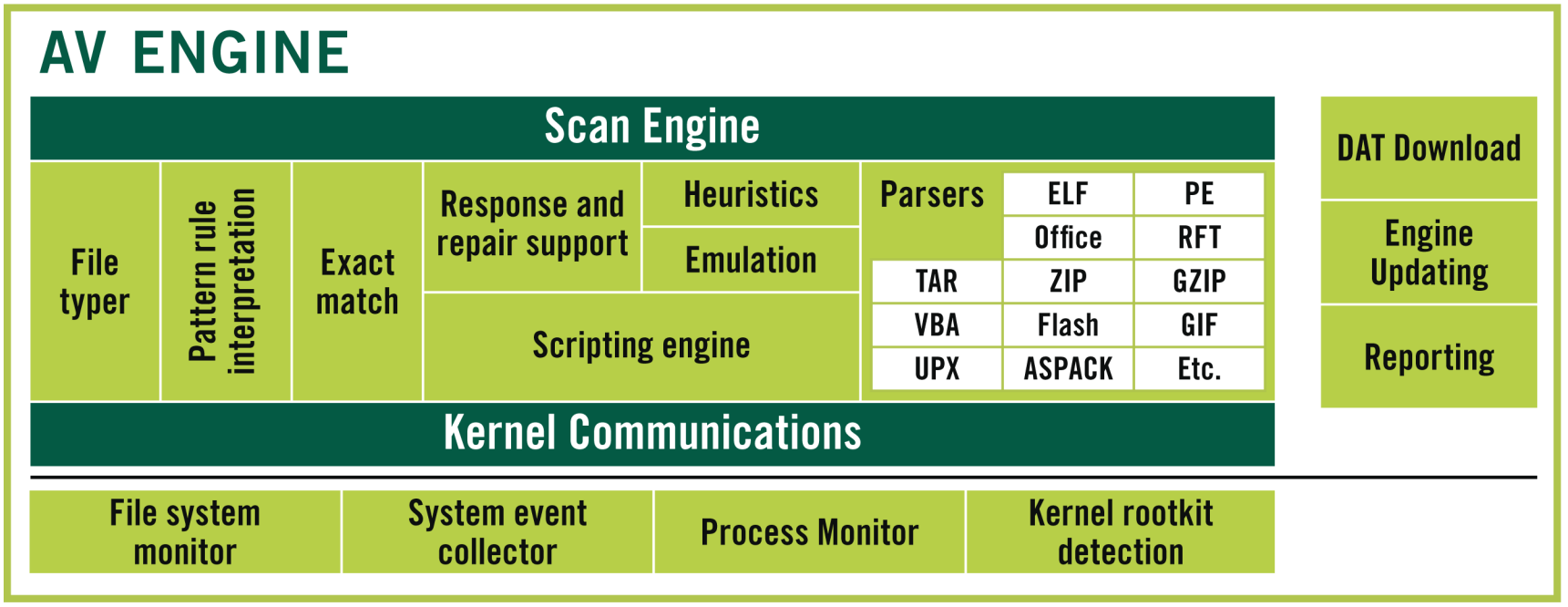
PERIMETER
E-SECURITY

Under the hood

PERIMETER E-SECURITY

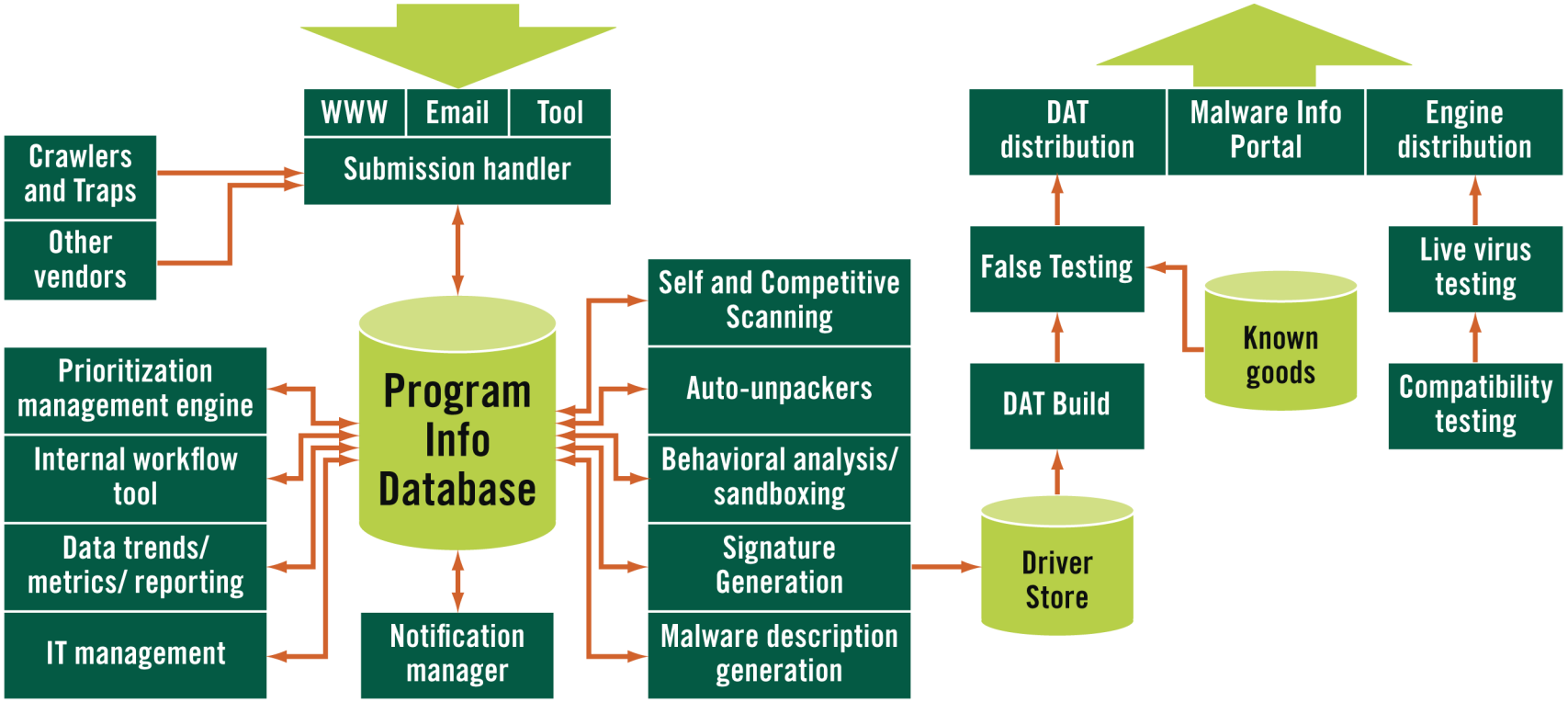
Under the hood





PERIMETER
E-SECURITY

Typical automation



PERIMETER E-SECURITY

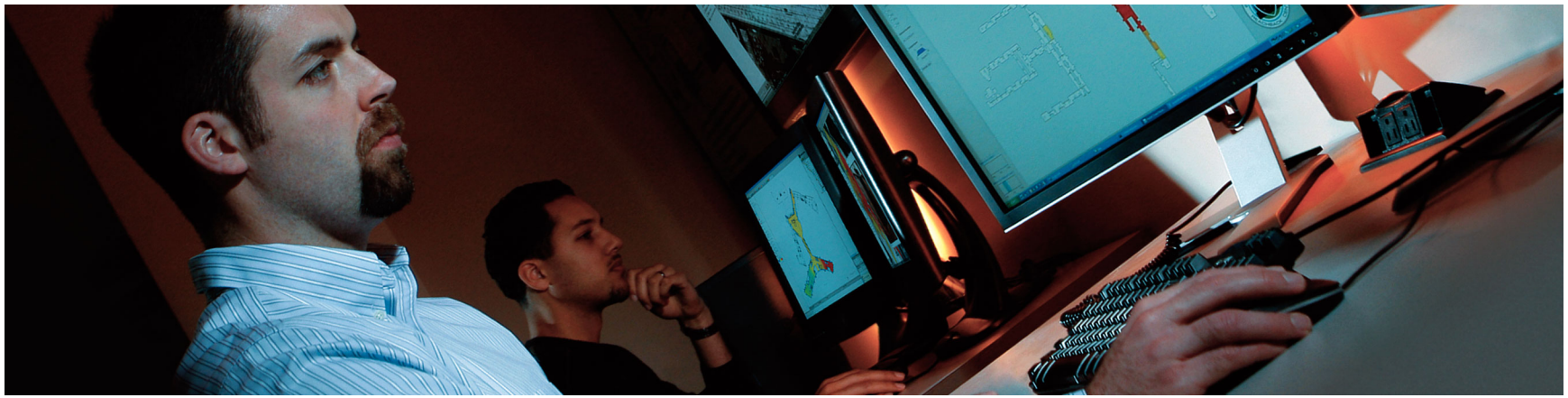
A researcher's todo list

- Help prioritize samples
- Figure out who should be dealing w/ samples
- Run some samples, see what they do
- Get someone to reverse engineer this sample
- Write a description of functionality
- Write a generic detector for that botnet
- Write repair code to wipe that botnet
- Produce a special DAT for BigCo
- Let BigCo know what happened to them
- Write some automation to make life easier

PERIMETER
E-SECURITY

Common problems

- False positives
- Seeing enough malware
- Performance
- Operational scale
- Cleaning up infections
- The testing problem
- Bad guys disabling your product
- Server-side polymorphism
- Getting coverage quickly

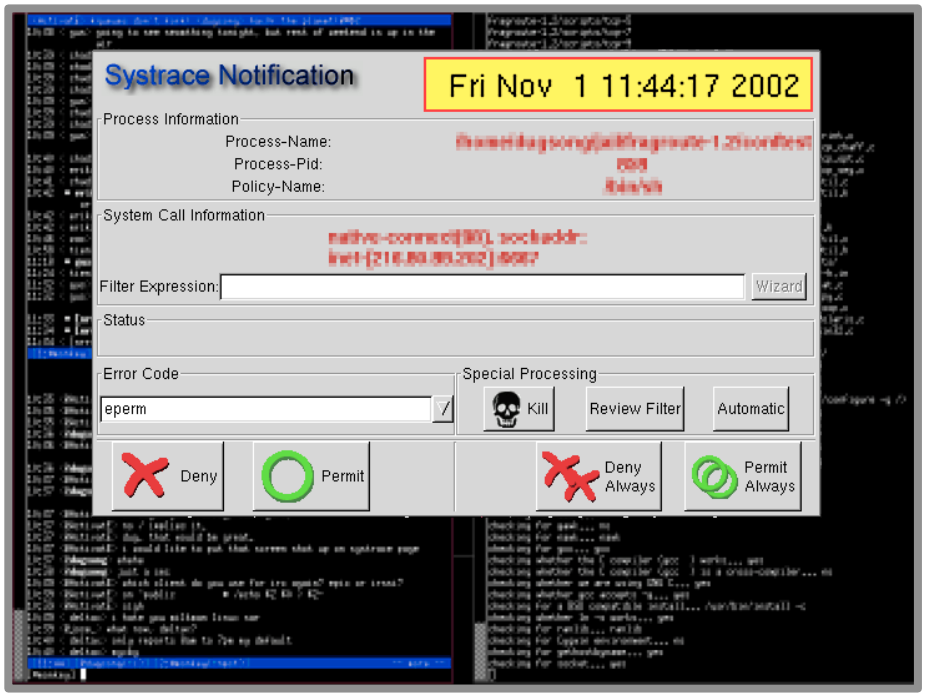


PERIMETER
E-SECURITY

Comparatives are broken

- Testing fake malware
- Testing old malware
- Not using products in the wild
- Vendors skewing the sample set

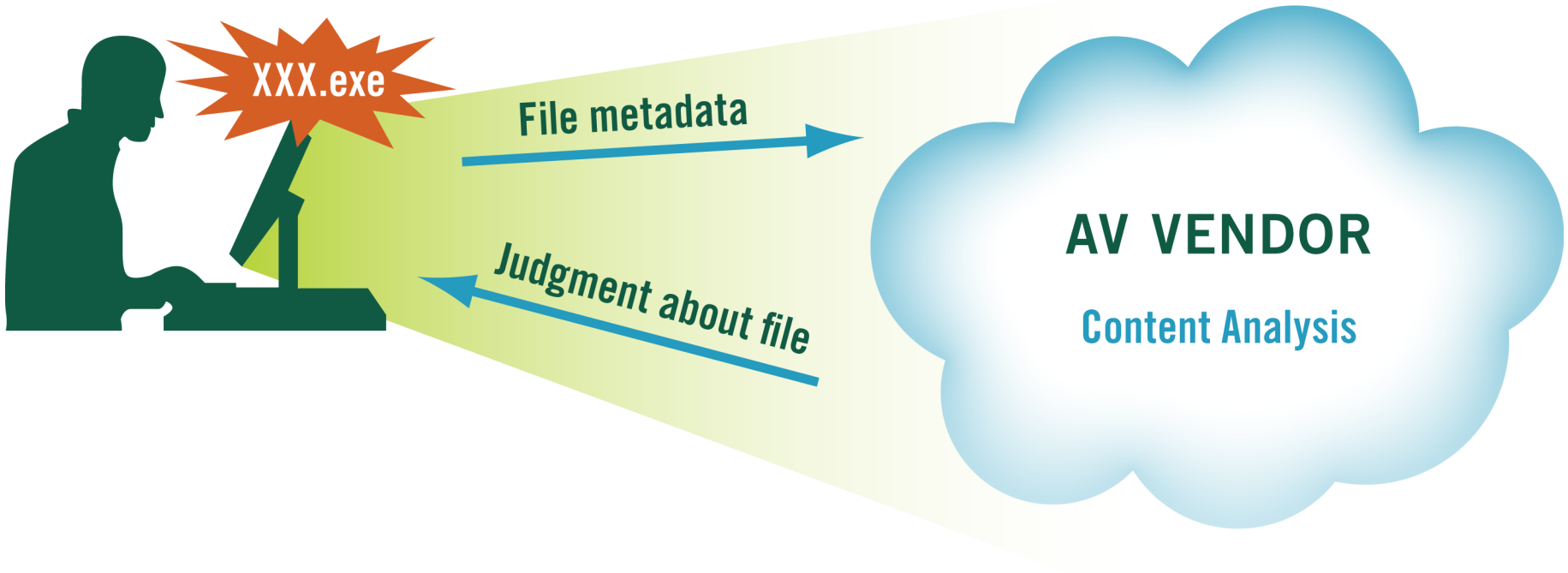
- IEEE is tackling this problem



TOMORROW'S TECHNOLOGY TODAY

PERIMETER
E-SECURITY

Generic Cloud AV



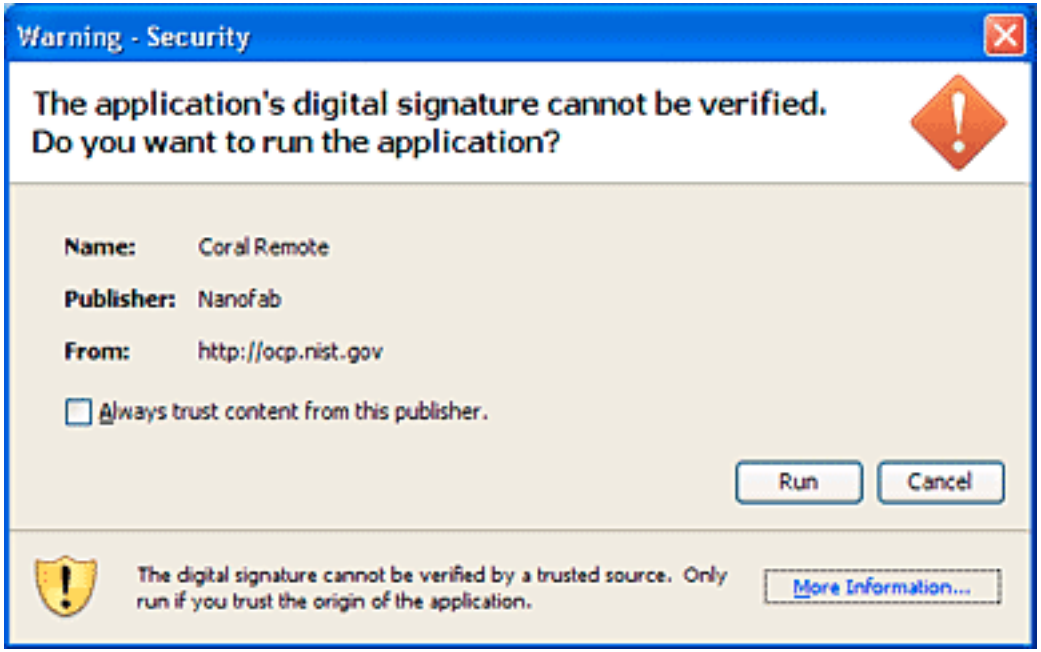
PERIMETER
E-SECURITY

Program classification

PERIMETER E-SECURITY

The packer problem

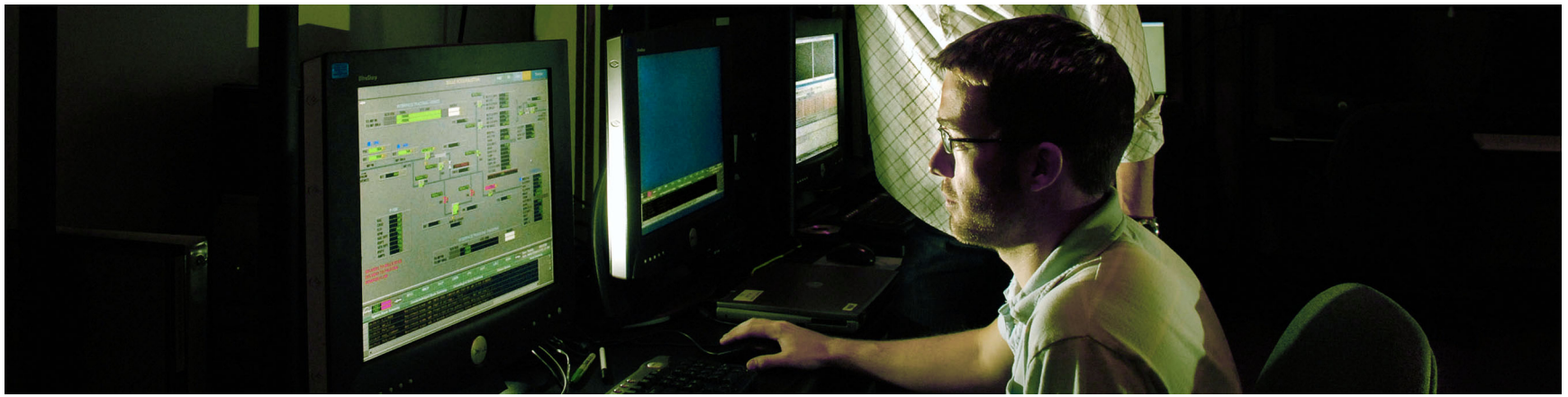
- Industry can white-list packers
- Digital signatures when exceptions are needed
  - Vendors will whitelist/blacklist PKI creds, not just programs
- Dispute process for bad signatures



PERIMETER
E-SECURITY

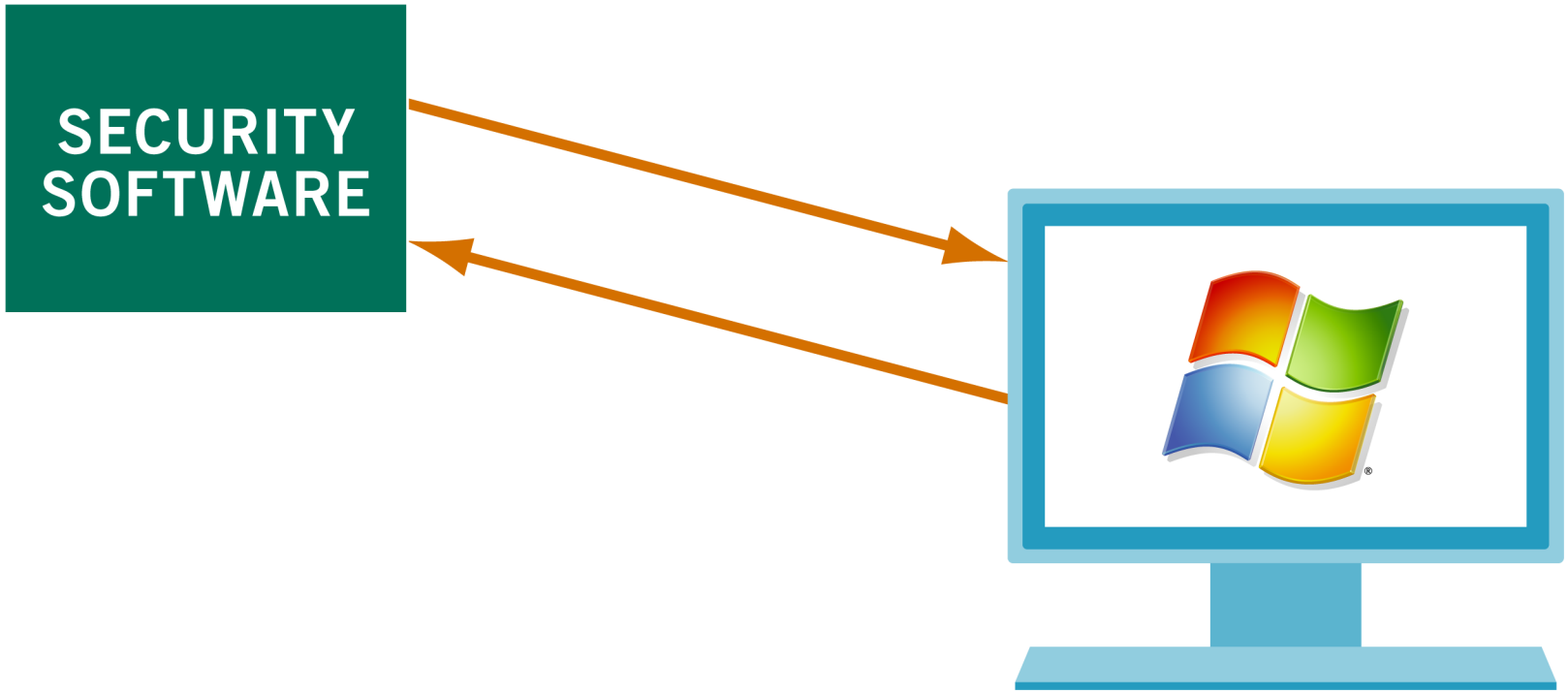
Problems revisited

- False positives
- Seeing enough malware
- Performance
- Operational scale
- Cleaning up infections
- The testing problem
- Bad guys disabling your product
- Server-side polymorphism
- Getting coverage quickly



PERIMETER
E-SECURITY

Virtualization



PERIMETER
E-SECURITY

Change will be slow

- Enterprise forklifts are difficult
- Changes in operational process are tough
- Consumers buy based on brand, not quality
- Change often needs to come in new revenue streams
  - Cloud-based audit
  - Automatic machine clean-up

PERIMETER
E-SECURITY

Thank you!

John Viega
jviega@perimeterusa.com
Twitter: viega