

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: SP01-W12

Who Watches the Watchers: IP Protection for Privileged Users

Richard Ford

Chief Scientist
Forcepoint

#RSAC

INTRODUCTION

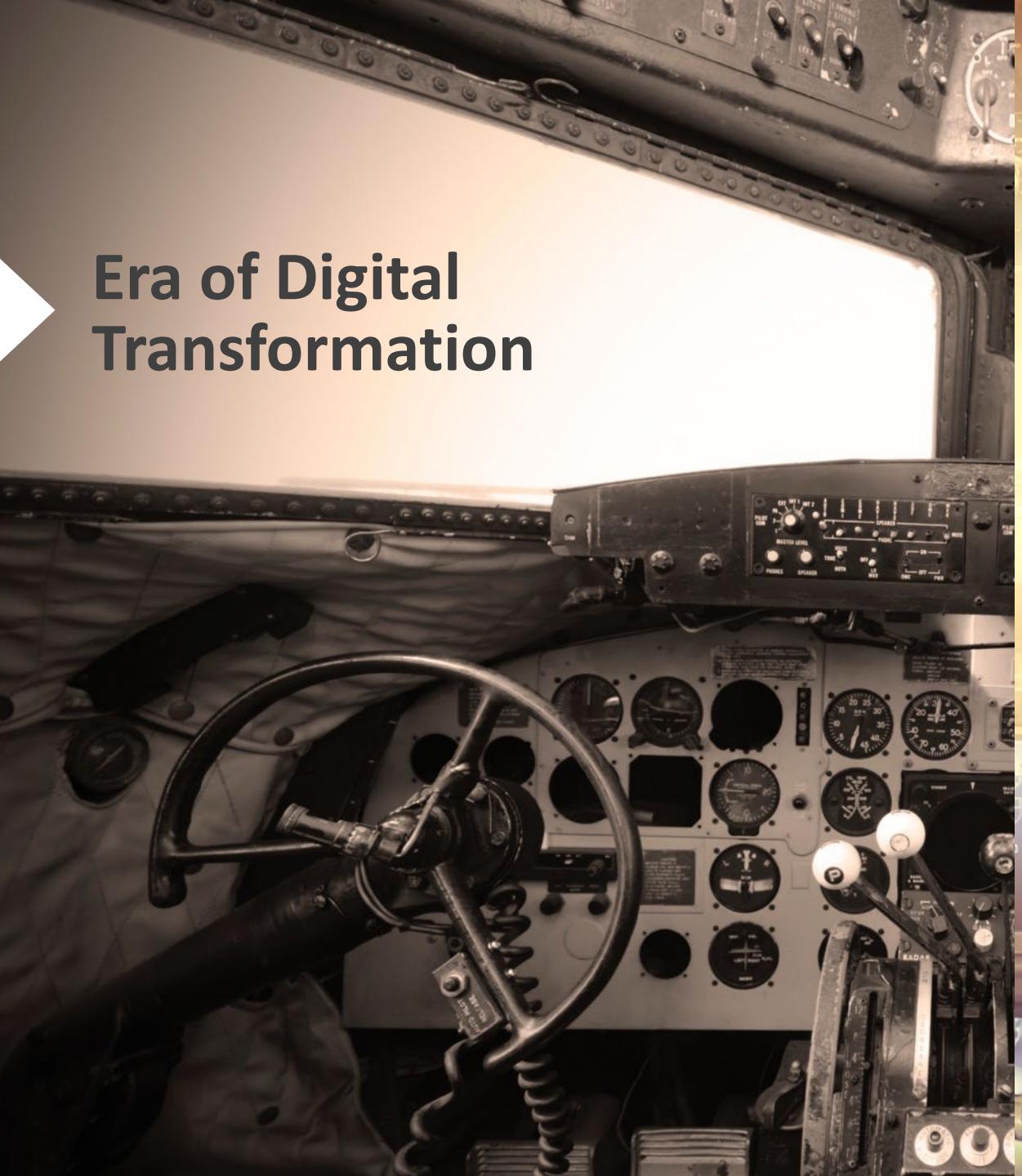
Dr. Richard Ford

Chief Scientist, Forcepoint

Dr. Ford leads the research and technology vision to help Forcepoint achieve its mission of delivering human-centric security and intelligence.



Era of Digital Transformation





Insider Threat is
a Real Problem

A photograph showing the lower half of a person's body, likely a woman, walking away from the viewer. She is wearing dark trousers and tan leather high-heeled pumps. The background is a bright, modern interior space with large windows.

Theft of IP



When the Thief is
the Creator...



A wooden gavel with a light-colored handle and a dark wood head lies horizontally across a dark, polished wooden bench. In the background, a judge's bench is visible, featuring a red and gold ornate chair. The scene is set in a formal courtroom with warm lighting.

An Interesting Real-World Use Case

An Interesting Real-World Use Case

- This case is still pending.
- Mr. Zheng disputes the allegations.
- GE has stated that they are in “close cooperation with the FBI.”*

*Source: WSJ

According to the Criminal Complaint...

SUMMARY OF THE INVESTIGATION

GE's Identification of the Crimes Under Investigation

19. In 2014, GE corporate security learned that Zheng had copied 19,020 electronic files from one of his GE-issued computers onto a USB external storage device, believed to be a thumb drive. GE has been unable to determine the contents of the 19,020 files, however, it is suspected that the files related to Zheng's work for GE as employees are discouraged from using GE-issued electronics to conduct anything more than incidental personal business. GE investigators interviewed Zheng in 2014 regarding this incident, and Zheng told them that he had deleted the files. GE had no additional information about the downloaded files, nor any corroboration about whether the files had been deleted or shared with any third parties.

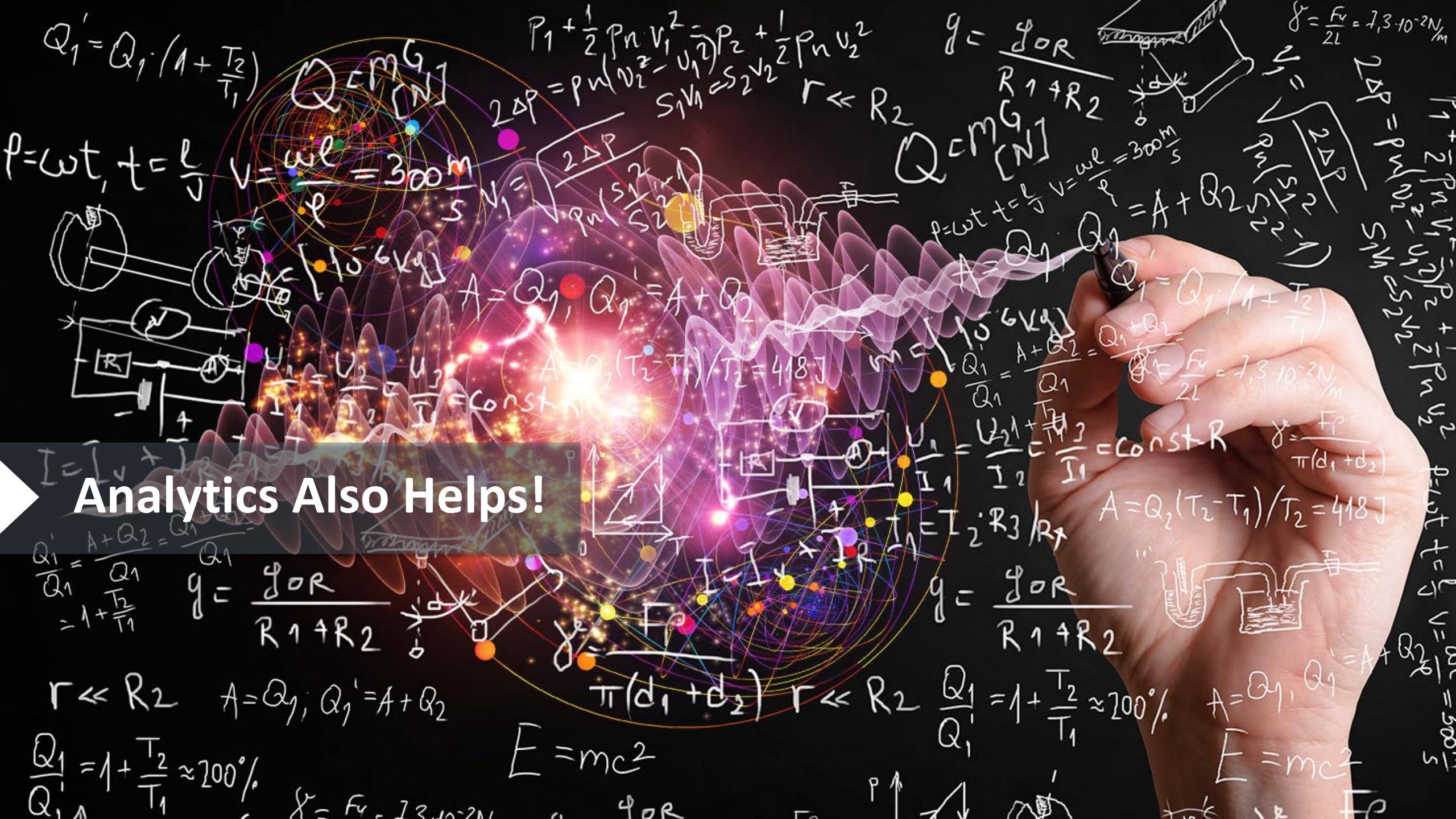
20. In November – December 2017, GE discovered that approximately 400 encrypted files had been saved on Zheng's work (desktop) computer. The files were encrypted using a program called Axcrypt – a program not used by GE. This practice was not standard for GE employees, and GE did not know why Zheng would be encrypting files on his work (desktop) computer. Due to the encryption, GE was unable to view the contents of the 400 files that Zheng encrypted and saved on his GE computer.

Count 1: 18 U.S.C. § 1832(a)(1)

Theft of Trade Secrets

DLP Can Help





A large black dog and a small tan dog are standing on a ledge. The large black dog is on the left, looking towards the right. The small tan dog is on the right, looking towards the left. They are both standing on a dark ledge against a white brick wall.

Peer-based
Comparisons

Red Flags for Fraud



A photograph of two people in an office environment. A man with dark hair and glasses, wearing a green sweater over a plaid shirt, sits at a desk looking at a computer screen. A woman with blonde hair and glasses, wearing a red and blue plaid shirt, stands behind him, also looking at the screen. There are multiple computer monitors displaying code or data. A yellow rubber duck sits on the keyboard. The word "Developers..." is overlaid on the bottom left.

Developers...

Source Code Control Systems



Deploying an Insider Threat Program





A Diversity of Data Sources

Conclusion

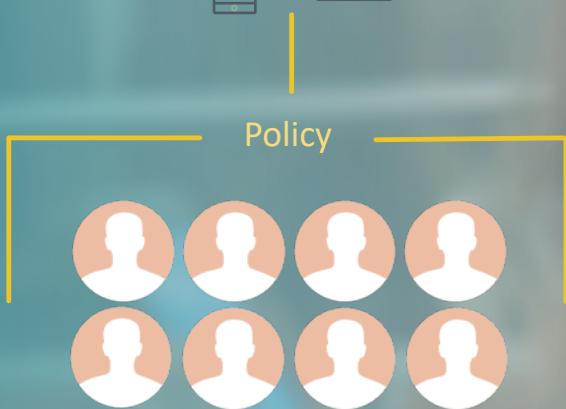
- Attacks like this are a matter of “when” not “if”
- Your best weapon is a diversity of data sources fused by analytics
- Don’t try and fix everything in one go, it’s a process.
- Your run rules: Transparency. Respect. Mission.



Q & A

Traditional Security

One-to-many enforcement of static, generic policies, producing high false positive rates.



Human-centric Security

One-to-one enforcement of different policies based on the risk, enabling automation.

