Forcepoint Insider Threat

Forcepoint

No One Wants To Be a Headline – But It Happens

SunTrust Bank Employee Steals Critical Data On 1.5 Million Customers

"In conjunction with law enforcement, we discovered that a former employee while employed at SunTrust may have attempted to print information on approximately 1.5 million clients and share this information with a criminal third party," SunTrust CEO William Rogers said in a press conference on Friday.

Apple employ ‘stole driveless car secrets’

An internal investigation revealed that he had copied **40GB** of information from various confidential databases.

Forcepoint Insider Threat

Broad & Deep Collection

Granular visibility of user and device activity

Unmatched Forensics

Understand intent for undeniable attribution or exoneration

Enterprise Scale

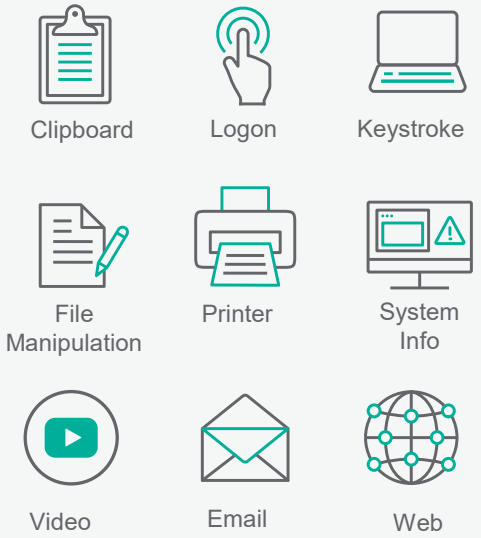
Proven effective and stable leveraging privacy and governance best practices

Broad & Deep Collection

Endpoint to Network Fingerprinting

Online and Offline Monitoring

Integrated with Forcepoint DLP



Granular visibility of user and device activity

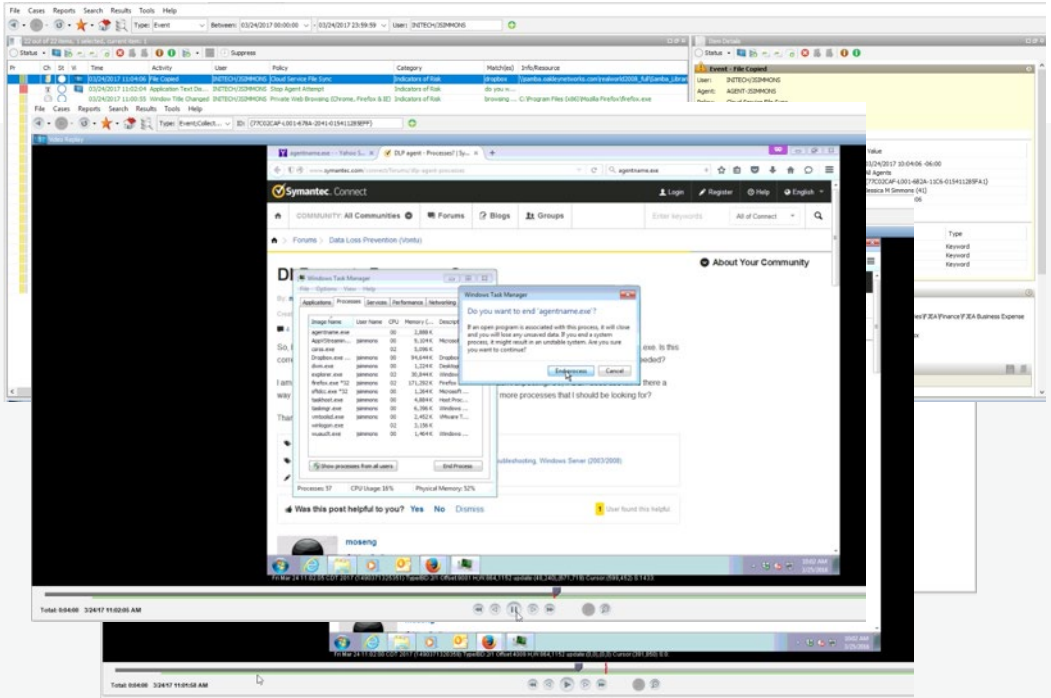
Unmatched Forensics

Policy Driven DVR-like Recording

Sequenced Event Time Stamp

Undeniable Attribution or Exoneration

Admissible in Court of Law



Understand intent for undeniable attribution or exoneration

Enterprise Scale and Proven Globally

Over 1 million endpoints protected

Protecting Fortune 500 and Government

Stopping Insider Threats since 2003


Energy


Financial


Government


Manufacturing


Retail

Protecting Leading Brands

What use cases could we help you understand?

Data/IP Exfiltration

Account Takeover

Flight Risk

Malicious User

Compliance Monitoring

Illicit Behavior

Sabotage

Harassment

Recommended Next Steps

- **Engage in a workshop with our executive security strategists**
- **Conduct a demonstration with your technical team**
-