Insider Threat Data Protection

GAIN UNRIVALED VISIBILITY INTO USER BEHAVIOR AND YOUR DATA

FORCEPOINT
POWERED BY Raytheon

Insider Threat Data Protection

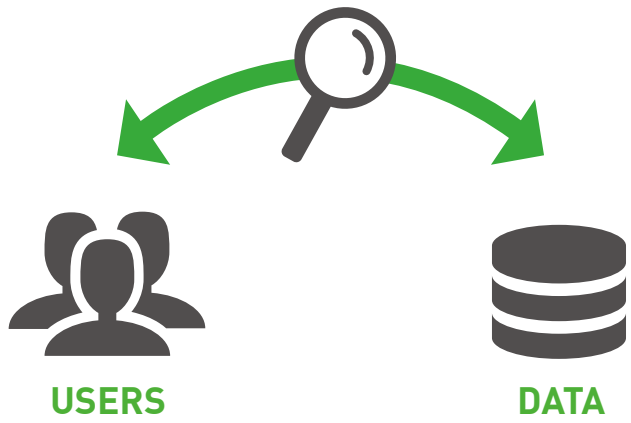
UNRIVALED VISIBILITY INTO USER BEHAVIOR AND DATA MOVEMENT FOR INDUSTRY-LEADING PROTECTION

FORCEPOINT'S "INSIDE-OUT" APPROACH

Forcepoint's innovative "Inside-Out" approach to cybersecurity will revolutionize how you protect your critical data. Our Insider Threat Data Protection delivers deep visibility into threats from within by linking data movement to your users' behavior, wherever they may be.

AN INSIDER THREAT EARLY WARNING SYSTEM

Early visibility into risky user behavior gives you advanced warning into threats to your data from within. Stop critical data from leaving your organization and identify both malicious and negligent users to minimize threat risks.



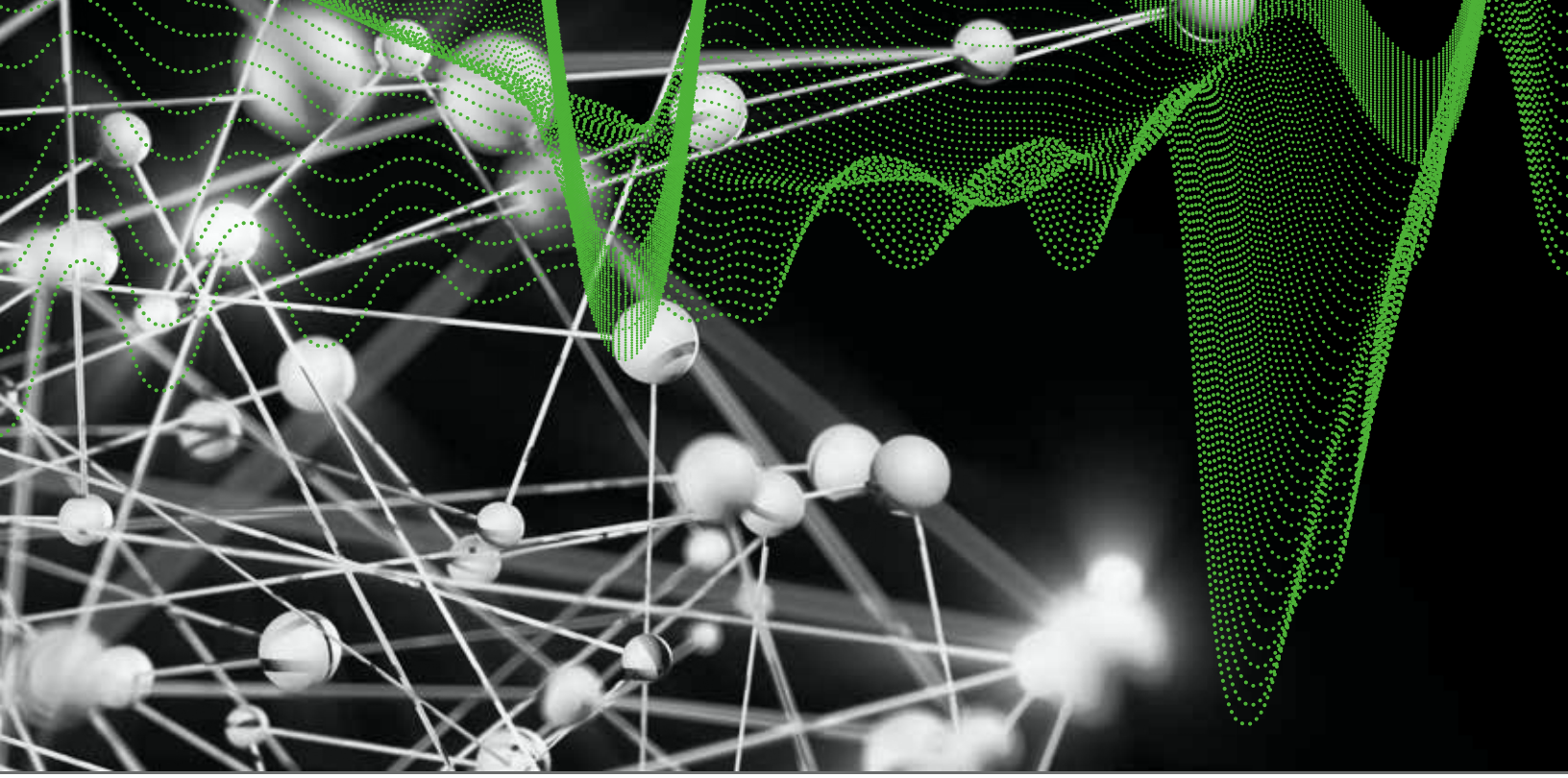
Why You Should Care

In 2015, the top three types of breached data were personally identifiable information (PII), authentication credentials and intellectual property (IP). What's more, 37% of these breaches were the result of insider behavior - either deliberate or unintentional.[1]

So how do you best enable your teams to access the data they need while keeping it safe?

Forcepoint™ offers the only early warning system to defend against risky behavior that leads to threats from within.

1 Forrester: Market Overview - Data Loss Prevention, May 2016



Challenges to Solving the Problem

THREATS FROM WITHIN

88%
OF ORGANIZATIONS RECOGNIZE THAT INSIDER THREATS ARE **CAUSE FOR ALARM**

69%
OF ORGANIZATIONS DO NOT HAVE ENOUGH **CONTEXTUAL INFORMATION**

56%
OF THEIR TOOLS YIELD **TOO MANY FALSE POSITIVES**

TOO MANY RELY ON DLP AND SIEM - TRADITIONAL TOOLS FOCUSED MORE ON EXTERNAL THREATS

VISIBILITY

42%
are not confident they have enterprise-wide visibility for privileged user access

16%
are very confident they have this visibility

BUDGET

88%
recognize budget as a **top priority**

Less than 40%
have a dedicated budget for insider threat protection

72% stated they use authentication and identity management tools to manage privileged user abuse - most use existing cybersecurity tools not designed to combat insider threat

Gain unrivaled visibility into user behavior and data

Our Solution – Forcepoint™ Insider Threat Data Protection

Forcepoint's Insider Threat and Data Protection is the industry's first solution that provides an early warning to an insider threat and prevents the exfiltration of your intellectual property and regulated data. It gives you visibility into your users and data and provides complete data protection by linking data movement to user behavior. Forcepoint protects your organization from hijacked systems stolen credentials, rogue insiders and accidental data loss. Proven to be highly scalable and trusted to protect the most sensitive organizations on the planet, Insider Threat Data Protection gives the needed visibility into your data, whether it is in the office, on the road, or in the Cloud and gives you the context around how employees are using your sensitive data.

Forcepoint's Insider Data Protection is the combination of our industry-leading Enterprise DLP solution, giving you visibility and control of data movement, with our unrivaled SureView Insider Threat solution that applies behavioral analytics and forensics to identify risky user behavior. This powerful combination stops more insider threats earlier than any other solution on the market.

The industry's most stable and scalable solution that grows with your organization

Data Movement + **User Behavior** = **Complete Data Protection**

Forcepoint DLP Advantages (TRITON AP-DATA and TRITON AP-ENDPOINT)

THE INDUSTRY'S MOST ADVANCE FINGERPRINTING CAPABILITY

- **PreciseID Fingerprinting** detects even just a fragment of unstructured and structured data, in the office, on the road or in the Cloud.
- **Best-in-class endpoint agents** give unrivaled visibility and control over sensitive data on Windows and Mac OS laptops - on and off the corporate network.

ADVANCED TECHNOLOGIES TO PROTECT SENSITIVE DATA

- **Optical Character Recognition** identifies text hidden in an image. Protect data hidden in legacy scanned documents, .jpegs, CAD designs, MRI's and screenshots.
- **Forcepoint's Machine Learning** lowers the barrier of entry to machine learning by not requiring a false positive during configuration.
- **Drip DLP** combats the slow and low attack when data is sent out in small volumes to avoid detection.
- **One-time policy configuration and deployment** for extending Enterprise DLP controls to common channels for exfiltration such as web and email.

Forcepoint SureView® Insider Threat Advantages

LINK DATA MOVEMENT TO USER BEHAVIOR

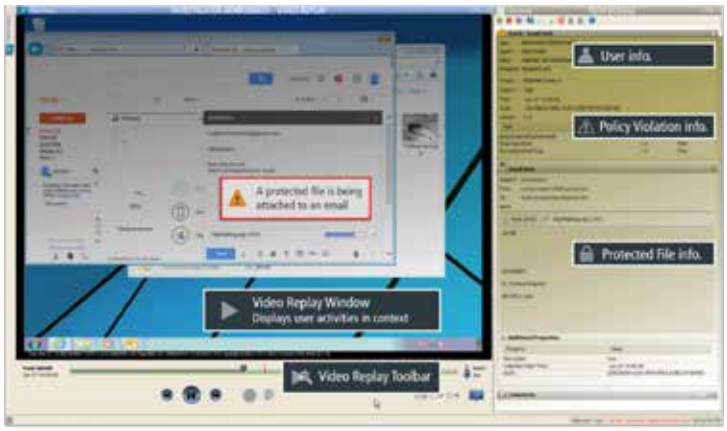
- **Early detection long before becoming a DLP Incident** such as an employee stockpiling data or creating back doors.
- **Quickly drive to smarter remediation decisions** after a risky user behavior is detected

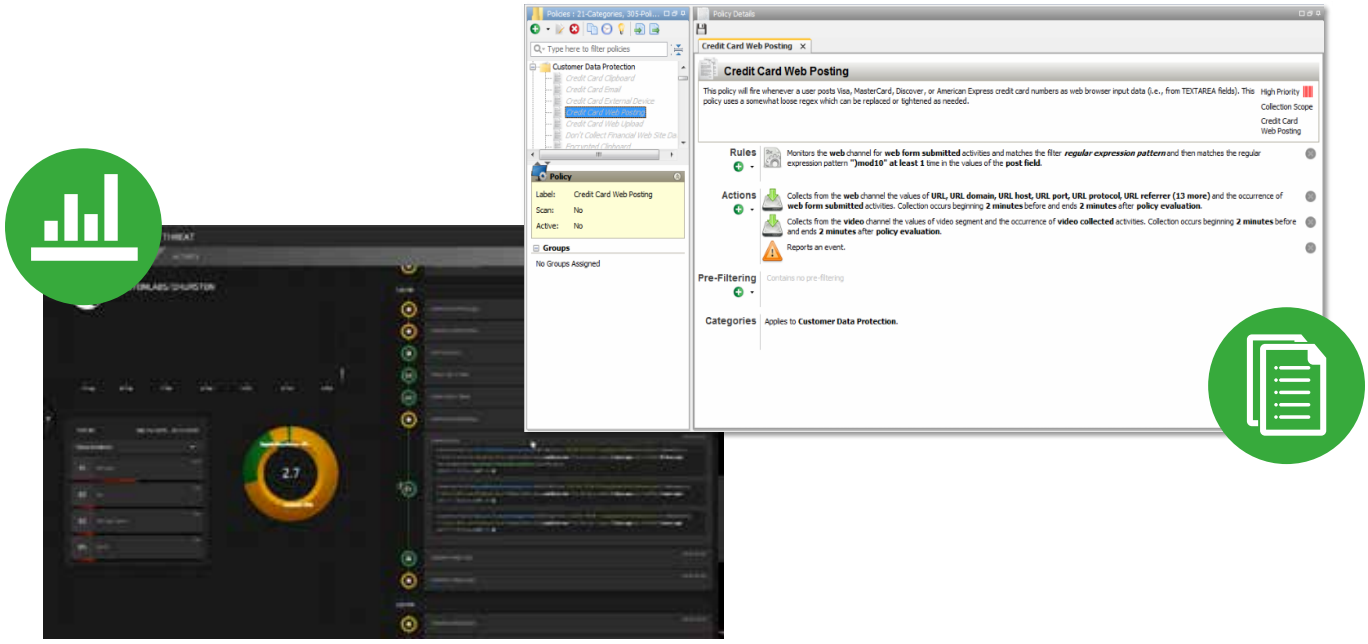
ANALTYICAL USER BEHAVIOR RISK-SCORING ENGINE

- Forcepoint gives you the early warning signs of a hijacked system, stolen credentials, a rogue insider or an employee just making mistakes - before sensitive data is breached or stolen.
- Saves you time and effort by automatically scoring and prioritizing your riskiest users, reducing the need to dig through thousands of alerts.
- Baselines both individual and organizational behavioral norms across channels to identify risky behavior.
- Provides a consolidated user risk score for each user on each day, as well as quickly highlighting 30-day risk trends.

VIDEO CAPTURE AND REPLAY WITH FORENSICS

- Screen shot capture and playback provide an "over-the-shoulder" view, giving you unparalleled visibility into suspicious behaviors before they become problems.
- Gain evidence for attribution and determine if the cause was from a hijacked system, stolen credentials, rogue insider or innocent mistakes.
- If necessary, SVIT forensics are admissible in a court of law.
- The SVIT Command Center automatically prioritizes your riskiest users, reducing the need to dig through thousands of alerts.
- An easy drill down into risky user behavior and an expandable time line shows you the activity that is making an employee a risky user.





Forcepoint is backed by 15 years of experience protecting data for commercial enterprises around the world, as well as the most highly secure government, military and intelligence organizations.


Trusted to protect the most sensitive organizations on the planet for over 15 years.

CONTACT
www.forcepoint.com/contact

[BROCHURE_INSIDER_THREAT_DATA_PROTECTION_EN]
400012.072916

FORCEPOINT
POWERED BY Raytheon