Moving Left of Loss

Operationalizing Human-centric Security to Reduce Risk Exposure
About the Authors

HOMAYUN YAQUB
GLOBAL SECURITY STRATEGIST
Homayun brings more than 25 years of insider risk experience from both the U.S. military and private sectors to Forcepoint. He is the former head of the data and insider risk program at JPMC, where he spearheaded their proactive approach to security.

ROBERT MECHLER
PRINCIPAL SECURITY STRATEGIST
Robert came to Forcepoint after spending over 23 years as a security practitioner. He served over 19 years as the CISO of Verizon Wireless where he built and managed the data protection and insider risk program.

JASON KEMMERER
SALES ENGINEER - DATA PROTECTION
Jason is the former Data Protection Analyst at HM Health Solutions where he implemented and led their Data Protection strategic program for over 3 years.
Humans Are the New Perimeter

Decentralized data and the increased use of cloud services leaves organizations with blind spots in their security perimeter — fueling the drive to become better, faster and cheaper.

Employees now have many options to access their organization’s most sensitive data and IP. The perimeter, once neatly defined by on-premises security infrastructure, is no longer absolute. A network user can be at home, at a café, or even on a casual walk and have the same access and opportunity for direct interaction with data as they would sitting at a desk in a company office.

There is a pressing need for data protection strategies to evolve to meet the security challenges presented by this new reality. Once built on binary, block-or-allow policies that would be triggered by an act of potential compromise, data protection must evolve to accommodate today’s dynamic interaction between an organization’s users and its data. This interaction must be continuously evaluated, shifting the lens of focus from a policy-centric to a risk-centric worldview, thereby moving the unit of measurement to where the opportunity for risk contribution exists—at the individual level. In this way organizations can work towards a cybersecurity approach that is better, faster, and cheaper.
Improving ROI Through a Proactive Strategy

**Better**
Continuously evaluating and identifying indicators of risk at the individual level and at their earliest point of detection is a foundational step in developing a better approach to improving an organization’s security posture.

**Faster**
Deploying a behavior-based approach to security not only automates the manual process for detection and response, but also virtually eliminates the associated level of human effort spent on such activity—thereby freeing up analysts to focus on more critical security issues.

**Cheaper**
Business value can be derived by showing cost savings and revenue protection results in three key areas: Reduced level of effort in Mean Time to Detect (MTTD) behavior-based risk indicators, faster Mean Time to Respond (MTTR) to those indicators, and a reduction in overall risk exposure related to data loss events.

---

Mean Time to Detect
- Decrease Mean Time to Detect through continuous risk evaluation.
- Shift detection paradigm from IOCs to IOBs.
- Focus on risk rather than event triage.
- Anticipate malicious activity.

Mean Time to Respond
- Decrease Mean Time to Respond through risk-adaptive enforcement.
- Obtain meaningful visibility.
- Understand entity history.

Detect
- Move “Left of Loss.”

Respond
- Gain meaningful visibility.

Reduce Your Exposure to Risk
- Focus on risk rather than event triage.
- Anticipate malicious activity.
- Understand entity history.
Evaluating user risk begins with understanding behavior. Typical data protection approaches begin with establishing multiple rules (e.g. a DLP policy) that are designed to alert an analyst once a potential data loss event has occurred. More formally, these are known as Indicators of Compromise (IOCs). These IOCs may indicate that a policy has been triggered, but they are inherently delivered to analysts “after the fact” and require research and validation. The net result of relying only on IOCs for data protection is time-consuming investigations that are often challenged with false positive indicators before a true understanding and context of the risk can be understood.

Investigators have the power of hindsight to substantiate an allegation, often discovering “breadcrumbs” that help provide important insight and context to their fact-finding efforts. Incumbent security policies are not typically structured to uncover these predictive data points, given their often benign and seemingly innocuous nature. But by merging these more established IOCs with behavioral indicators of risk, security leaders can more effectively detect, prioritize, and respond to areas of concern well before a data loss event has occurred. Indicators of Behavior (IOBs) are the evolution of legacy IOC approaches and better enable a proactive approach to data protection management.

Benefits of IOBs:

→ Composite risk-score, which can be leveraged in risk adaptive protection (RAP) policy decisions. This marks a shift in classic event matching security signatures, to a risk-centric approach, where each IOB receives its own risk score. These risk scores can be assigned via severity mappings or baseline calculations, which offer numerous methods for asking an analytical question.

→ IOB baseline calculations do not occur in a centralized location. Computing baselines in a centralized architecture requires an unreasonable amount of computational resources, without yielding a level of fidelity that most organizations require. Instead, IOB baseline calculations occur on the endpoint and enable a broader and more specific application of baseline calculations.

→ IOBs do not require endpoint event data to be collected and shipped to a centralized location. However, the option of collecting an event for evidentiary purposes does exist and can be tied to a specific IOB risk-score threshold. This flexibility allows the organization to only collect the most critical endpoint data, which reduces the cost of ownership when compared to a classic UEBA approach of maintaining two copies of a given event.
Operationalizing the full functionality of a DLP solution is foundational to a data protection program. With policies in place and blocking enabled, organizations are already on the right path towards reducing data loss risk exposure. But only focusing on IOCs is not enough and blocking every potential compromise incident is not practical or conducive to business productivity and efficiency.

Rigid DLP policies may not easily accommodate the very legitimate reasons why one or more users may need an exception to a policy in order to perform their job. In most organizations, accidental, non-malicious mistakes comprise a large number of risk alerts—but such events should not lead to negative action taken against the user making the mistake. Another important challenge presented by legacy DLP is the volume of alerts generated, which is a function of the number of policies in place and the size of an organization.

For IT security teams, these challenges are real. Competing requirements, resource constraints, and limited hours in the day make both detecting and responding to potential data loss events that much more complicated. As a consequence, organizations often unwillingly accept risk by remaining reactive through a labor-intensive process. This involves detecting or validating each alert to determine if it’s worth further analysis or deeper scrutiny. And then responding by investigating the alert by gathering other data, performing analysis and ultimately determining whether the alert was substantiated, with the intent of remediating the issue. This risk acceptance translates into a corresponding monetized risk exposure that companies may be responsible for paying in the event of a breach.

Reducing Risk Exposure While Improving Productivity and Operational Efficiency
Let’s walk through an example of a large healthcare organization’s data protection metrics*

A large healthcare organization with 50,000 employees needs to protect their critical data and records and is struggling to respond proactively to insider risks. A major breach could cost them millions of dollars and leave them vulnerable to legal and compliance problems.

*The figures depicted in this example are based on Forcepoint client data and market research.

### Traditional Security Approach using IOCs

#### COMPANY SECURITY PROFILE

Employees: 50,000

| Total Daily Security Incidents: | 5,088 |
| Average Incidents Allowed Daily: | 2,733 |
| Average Incidents Flagged Daily: | 564 |
| Average Incidents Blocked Daily: | 2,733 |

#### DATA LOSS INCIDENT

**TIME →**

- Detect
- Respond

**MTTD**

Mean Time to Detect
- # Minutes per DLP event
- #DLP events leading to investigation

**MTTR**

Mean Time to Respond
- Mean volume of investigations
- # Minutes per investigation

**RISK EXPOSURE**

**Continuous User & Data Interaction**

**INDICATORS OF COMPROMISE (IOCs)**
The organization suffers from blind spots and lacks understanding around how their employees and contractors are interacting with their critical data. This highlights the need for a new approach that offers better visibility into how data is being used by focusing on the behaviors leading up to a breach, versus the indicators of a breach after-the-fact.

So how does a change in approach affect the bottom line? On average, a single lost data record will cost the healthcare organization $150 per incident. The security team has 50,000 users to continuously monitor, any of whom could potentially cause an incident. Based on the company profile, here is what a shift in approach would look like if the organization switched from an incident-centric to a behavior-based approach.

Behavioral-Centric Security Approach using IOBs

**MTTD**
Mean Time to Detect
- # Minutes per DLP event
- #DLP events leading to investigation

**MTTR**
Mean Time to Respond
- Mean volume of investigations
- # Minutes per investigation

Detect 0 MINUTES  Respond 0 MINUTES

Risk Exposure

Continuous User & Data Interaction

Indicators of Behavior (IoBs)
By leveraging IOBs through an automated and continuous evaluation approach, organizations can virtually eliminate their manually driven level of efforts on detecting and responding to data loss incidents.

INCIDENT-BASED APPROACH

- Monitoring Incidents: 2,733
- Annual Risk Exposure: $14,963,175
- Potential for Loss: 10%

BEHAVIOR-BASED APPROACH

- Monitoring Incidents: 500
- Annual Risk Exposure: $2,737,500
- Potential for Loss: 10%
Moving Left of Loss

Driving ROI Through Reduced Risk Exposure

Along with preventing a breach, organizations must also try to maximize productivity by investing in the technology solutions needed to maintain a hyperconnected workforce. By enabling easy, always-on access for users to the people and data they need to work with, the ways users in an organizational environment will interact with data only becomes more diverse and complex over time—for example, with different cloud-based tools that may or may not be validated by the organization. This growing complexity of data interactions is challenging even the most mature security environments. As the example of the healthcare organization demonstrated, the legacy approaches to detecting and responding to potential data loss events cannot keep pace with growing risk exposure associated with today’s workplace needs. Organizations must evolve their methodology, shifting from an event-centric model reliant on IOCs to one that is risk-centric, leveraging IOBs through a continuous evaluation approach.

This allows organizations to proactively identify risk indicators at their earliest point of detection and automate a response by instrumenting controls across their security environment. The appropriate level of security friction at the user level can be introduced, moving the data protection posture “left of loss” without negatively impacting the rest of the organization in terms of unnecessarily hindering productivity. And of course, automation also reduces the overall level of effort for the security team.

Lastly, organizations can now realize and report on tangible value that protects revenue and reduces risk exposure. The value of this risk reduction can be calculated and used in TCO and ROI formulas to help bolster the case for this human-centric approach. Forcepoint has resources that can assist your organization in understanding your individual risk assessment and help reduce exposure.
Identify and Mitigate Risk With Forcepoint’s Dynamic User Protection

Dynamic User Protection (DUP) is a User Activity Monitoring (UAM) solution designed to alert organizations of risky behavior, so they can protect critical data and reduce the risk associated with insiders. The solution collects user behavior data and Forcepoint DLP incidents (through DLP 8.8 integration), and then computes a user’s risk score using Forcepoint’s Indicator of Behavior (IOB) analytic models. This risk score is actively communicated to DLP to automate policy enforcement based on a user’s risk level.

Forcepoint can deliver insights that vastly improve analyst efficiency and automate data loss policies with risk-based thresholds. Our cloud-based User Activity Monitoring solution provides actionable insights and automated responses for risky behavior that can save your organization time, money, and anguish.

Contact us for your own personalized risk assessment evaluation.
About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint’s humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

© 2021 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners. Moving Left of Loss eBook 19JAN2021