Forcepoint’s Approach to Zero Trust (ZTX)

A data-centric security architecture, protected by behavior-based controls

Victor Martinez
Sales Engineering Manager, Forcepoint Global Governments
The Current Mission for Data Security

Protect important data wherever it resides without Overwhelming Administrators, Frustrating Users, Mistaking for.
Data Protection Point of View

Data Discovery & Classification
Discovery across network, endpoint & cloud apps
Partnerships: Microsoft, Boldon James, Titus, Seclore

Data Detection
Machine Learning, Fingerprinting, Compliance Policies, Image Classification, OCR

Deep Forensics
Unified Endpoint Insider Threat Cloud Apps

Analytics
Behavioral Analytics Module Risk Adaptive Protection

SaaS App Protection
API Integration Inline Cloud Proxy Infrastructure Data in motion, in use, at rest
Legacy DLP

- **Strong policy enforcement** prevents data exfiltration but can reduce workplace productivity
- DLP policy management is **static, set for an entire group**, must be **manually** changed if users is identified as high risk
- Organizations forced to adjudicate DLP alerts with **no context**, making determination of false positives difficult
- Most DLP deployments forced into **monitor only** mode

Dynamic Data Protection (DDP)

Leverage User Behavior Analytics to:

- Provide **full operational context** to more effectively adjudicate DLP alerts
- Automatically escalate more stringent policy deployment and enforcement for users **based on data exfiltration risk indicators**
- Dynamic mapping of policies with multiple enforcement options
- Maximize workforce productivity
Data Protection – Pathway to Blocking

Problem

- DLP implementers are concerned with being viewed as a strain on user productivity in the event their policies result in too many false positives.

The Security Requirements

- Having the ability to forensically audit their alerts if important data leaks.

Result

- Many large enterprises have deployed DLP in audit only mode. The security team can mine alerts to identify data exfiltration, but they don’t actively block it.
Moving Beyond Auditing Alerts

Business as usual

For Risky Adaptive Protection users, determine actions according to the source’s risk level:

<table>
<thead>
<tr>
<th>Risk level 1</th>
<th>Risk level 2</th>
<th>Risk level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Only</td>
<td>Audit Only</td>
<td>Audit Only</td>
</tr>
<tr>
<td>Risk level 4</td>
<td>Risk level 5</td>
<td></td>
</tr>
<tr>
<td>Audit and Notify</td>
<td>Block All</td>
<td></td>
</tr>
</tbody>
</table>

Result
- Bad users are blocked, good users are unaffected
- Confidence in the system allows admins to deploy blocking posture
- Policies are now user specific based on individual behavior

Blocking the riskiest users

Still non-blocking, but notify the admin
Better Understanding of Intent

An employee tries to print an FOUO document and the DLP solution blocks it. Is this employee a risk?
Analyze & Model For Insights

DATA SOURCES

- EMAIL
- VOICE
- CHAT
- NETWORK
- ENDPOINTS
- PHYSICAL ACCESS
- HR DATA
- 3RD PARTY FEEDS

ANALYTIC ENGINE

- Pattern Recognition
- Outlier Detection
- Sentiment Analysis

Entity Risk Scoring

INFORMED NARRATIVE

1. Patterns Change
2. Complains Frequently
3. Sends Many Emails at Night
4. Prints Out Confidential Files

Understand Intent Through Deep Context

© 2019 Forcepoint
In the 24 hours prior to 23:00 8/2/17, Chad Pursley’s risk score is 99, which is higher than their average of 50 over the past week. Currently, their highest score is on the Compromised User (CU) scenario, with a score of 99.
DDP - Risk-Adaptive Protection

Risk-adaptive protection dynamically applies monitoring and enforcement controls to protect data based on the calculated behavioral risk level of users and value of data accessed.

This allows security organizations to better understand risky behavior and automate policies, dramatically reducing the quantity of alerts requiring investigation.

How Risk-Adaptive Protection Works

1. Each user has a unique and dynamic Risk Level
2. Risk levels are driven up and down based on changes in behavior
3. Risk Levels drive different outcomes
4. Security adapts to Risk Levels as they fluctuate
Improved Visibility and Reduction of Noise

- Total Incidents (30 Days) - ~400,000
- Top 2 Policies ~ 65% of incidents
  - Office Files Sent over Time ~170,000
  - Large Files ~74,000
  - Requires thresholds

- Total Incidents (30 Days) - ~165,000
- Visibility into all file types
- Visibility into all file sizes
- Simplification of DLP policies
# DDP Results In The Real World

<table>
<thead>
<tr>
<th>User 1 – Product Development Engineering</th>
<th>User 2 - Security Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td></td>
</tr>
<tr>
<td>• User injected numerous DLP policy violations and exfiltration events over 12 hours</td>
<td>• User injected small amount of DLP policy violations and exfiltration events with critical data</td>
</tr>
<tr>
<td>• High Volume, important data</td>
<td>• Low volume, critical data</td>
</tr>
<tr>
<td><strong>Risk Score / Level</strong></td>
<td></td>
</tr>
<tr>
<td>95 / 5</td>
<td>93 / 4</td>
</tr>
</tbody>
</table>

## Analytics

| DDP Matches Sum – Total amount of incident | 1,378 | 158 |
| DDP Incident Score – Type of data being moved | 75 | 81 violations with “Confidential and Proprietary Content” |
| DDP Event Count – Total number of exfiltration events | ~130,000 | ~9,000 |
| DDP Bytes Sum – Total amount of data exfilled (GB) | 75 | 9 |
| DDP Event Score – non incident type of data being moved | 85 | 85 |
Immediate Benefits of Dynamic Data Protection

- **Intelligent DLP**
  - Reduce the amount of DLP alerts that need to be triaged; transition DLP from broad to individual policies.

- **Increased Productivity**
  - Provide greater flexibility in policies, and adapt enforcement based on calculated risk.

- **Proactive Security Management**
  - Detect and respond to high-impact events in a shorter amount of time.
Multilevel Risk Adaptive Protection

Problem:
- Protect sensitive data across multiple networks
- Discover and inventory critical data and IP every place users collaborate.

Solution:
- Forcepoint’s Multilevel Risk Adaptive Protection Solution integrates the market’s most powerful data protection suite, user behavioral analytics, next generation firewall and cross domain transfer technologies to provide secure data sharing and comprehensive user visibility. The solution provides multilevel end-to-end security utilizing Behavior Analytics by and securely sharing user risk levels across multiple networks for adaptive and consistent enforcement.

Benefits:
- From a single pane of glass, multilevel Risk Adaptive Protection significantly reduces time to discovery, alerts and false positives, across domains to enable better use of resources for holistic forensic investigations, stronger security, and automated risk responses.
Forcepoint’s Zero Trust Multilevel Risk Adaption Solution

Data Vetted Through Forcepoint:
- DDP Policies
- DLP
- UAM
- Web Gateway
- Email Gateway

Endpoint Monitoring
- Forcepoint DLP
- Forcepoint UAM

High Speed Guards and NGFW move data to high-side for analysis and to move actionable risk data to lower levels.

All data viewable on one desktop on high side.
Cross Domain Solutions Suite

Facilitating your mission while maintaining the highest degree of network and data security

- Trusted Thin Client
- High Speed Guard
- SimShield
- WebShield
- Trusted Gateway System
- Trusted Print Delivery
- Trusted Mail System

Export Controlled
Zero Trust – Forcepoint Portfolio Today

- Highly distributed networks (micro-segmentations, perimeters)
- Limit excessive user privileges (risk-based, identity-aware)
- Enable secure connectivity (scalable, identity-aware)
- Protect data where it resides and in use (risk-based, frictionless)
- Improve security detection and response (analytics and automation)

- Workload-focused (virtualized, containers, API-based)
- Cloud Access Security Broker
  - Insider Threat Behavioral Analytics
  - Email Gateway
  - Web Gateway
  - NGFW w/ SD-WAN
  - AMD
  - Dynamic Data Protection
  - Dynamic Data Protection
  - Cross Domain Networking
  - Automation and orchestration
  - Visibility and analytics
  - Devices
  - Networks
  - People
  - Workloads
Thank you!

Patricia.Colpitts@forcepoint.com

Data at the Center
Everywhere—cloud, on-prem, endpoint

Behavior-based Controls
Automated ZT protection via risk-adaptive enforcement

Unified Cloud Solution
Dynamic Security Platform