



Monitoring web, mainframe and key enterprise applications with Record & Replay for Helix

Monitor users in ways more advanced than you ever thought was possible

2024

Agenda

Record and Replay Overview

- About Bottomline
- Technology Overview

How Bottomline + Trellix Work Together

- User Monitoring with Bottomline's Record and Replay
- Detecting Compromised Users with Trellix Helix

Highlighted Use Cases

- Connect: User, Identity, Device, Transaction/Activity
- User Entity Behavior Analytics
- Ransomware

Wrap Up



Martin Holste

CTO | Trellix

As CTO for Cloud and AI at Trellix, Martin is responsible for shaping cloud security strategy, and passionately working with customers to improve their security outcomes. Prior to serving as CTO for Cloud and AI, Martin led teams working on machine learning and founded the cloud-native Helix XDR Platform at Trellix



Andrew Leon

Sales Executive, Partners & Alliances | Bottomline

Andrew Leon is a technology expert with over 20 years of experience focusing on various aspects of Cyber Fraud and Security

Why Choose Bottomline for Risk Solutions?

A simplified, unified view and management of risk across channels and applications.

Monitor applications in ways more advanced than you ever thought was possible.

- ✓ Customer-delight attitude
- ✓ Decades of experience in risk
- ✓ Innovative technology and patents
- ✓ Trusted innovation partner

MARKET LEADERSHIP

500+

Enterprise grade
customers

37

countries across
6 continents

500k

Employees
monitored

BOTTOMLINE CORPORATE HIGHLIGHTS

90%

of the top U.S. banks use
Bottomline solutions

2,400+

Employees worldwide

Billions

of transaction
s worldwide
completed each year

\$1T+

Transactions
face value

15%

of Global SWIFT
FIN traffic

Bottomline | Risk Solutions

Record & Replay

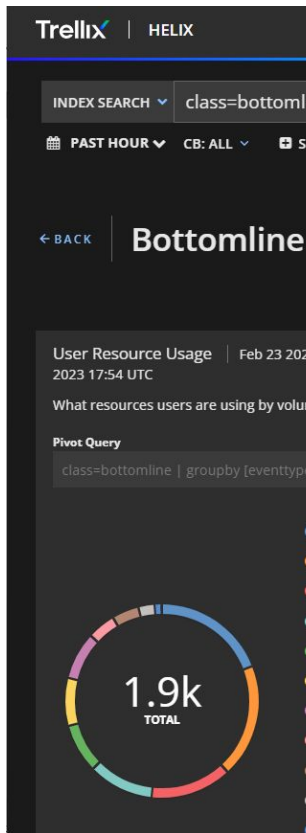
What We Monitor

APPLICATIONS

Banking cores
Payment portals
CRM
Payables solutions
Human Resources

PROTOCOLS AND TECHNOLOGIES

IBM Mainframe: 3270
IBM System i: 5250
Web: HTTP/ HTTPS
WS / REST API
Custom Parsers



Bottomline

Maximize details view

Session Details Step Details

General

Sequence	14
Name	Customer Maintenance
Timestamp	08/17/2009 09:05:13.894
User Action	[enter]
User Action Timestamp	08/17/2009 09:05:20.682

Fields

Last Name	Chou
Ssn	816261324
Customer Id	300549

BNKCSTF

Current Account Subsystem
Customer Maintenance

08/16/09
09:07:10

*Action (A,C,D,I,L,N,R)

Customer ID : 300549

First Name : Anne

Last Name : Chou

Customer Type (?) p SSN : 816261324

Address:

Country (?) : USA State (?) : NJ

City (?) : Lampeter

Street : 73 Sea road PostalCd: JU34

Telephone:

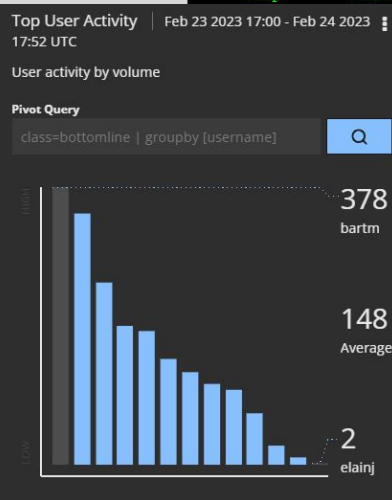
Type (?) Number Extension Preference

E-Mail:

Direct Command:

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12---

help retrn main ACCT



Sensitive Resource Access | Feb 23 2023 18:00 - Feb 24 2023 18:00 UTC

User access to sensitive resources

Pivot Query

class=bottomline eventtype=bnktrnf | groupby [username]

eventtype	username	Count
bnktrnf	bartm	36
bnktrnf	dalek	28
bnktrnf	elainej	18
bnktrnf	pamw	17
bnktrnf	jerry	16
bnktrnf	davidk	12
bnktrnf	michael	12
bnktrnf	johnk	8
bnktrnf	ilya	4
bnktrnf	barbaral	2

Technology Overview

PATENTED TECHNOLOGY



Non-invasive network
traffic sniffing



No impact
on performance



Highly scalable
architecture



Very short installation
process, with no risk to
normal IT operations



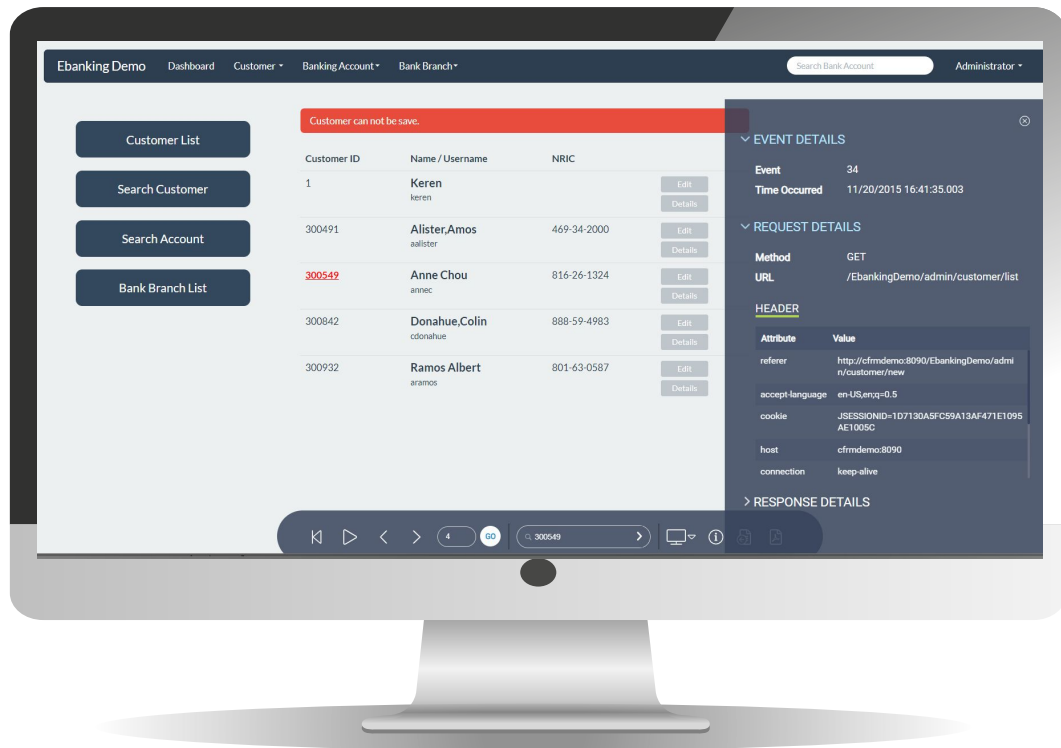
Recordings stored in
extremely condensed format



Recorded data is
encrypted and digitally
signed

Bottomline's Record & Replay

Patented technology offering next level visibility helping reduce investigation time and effectively identify suspicious behavior



Key Benefits

- Non-invasive recording focused on your most critical applications
- Capture user activity in real-time at a detail level – not just when a data extraction event occurs!
- Understand context of user actions by tracking every interaction from mainframe to web
- Visual audit trail increases investigation efficiency by up to 90%
- Detailed data capture allows for more refined analytics



Meet Trellix

Living Security.

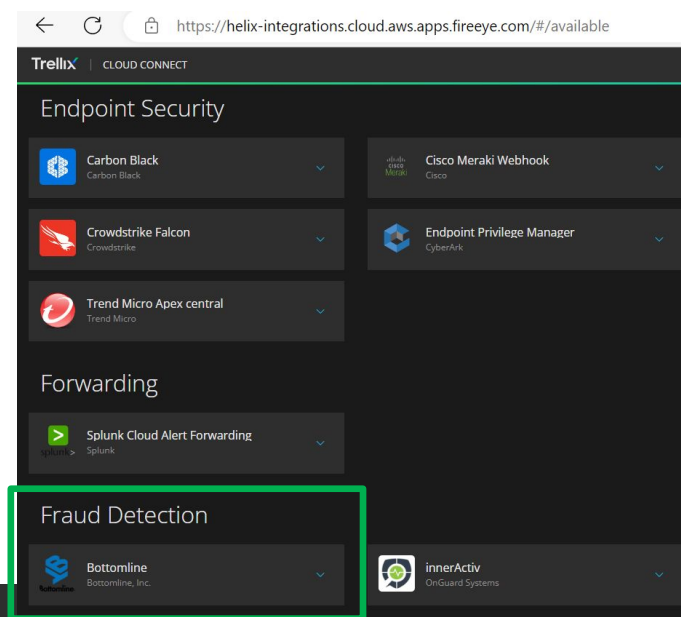
Our core values are open, tenacious,
curious, and fun!

We combined the strengths of
McAfee Enterprise and FireEye to do
security differently.

Bottomline is a certified SIA Partner

Record and Replay Integration with Trellix:

A simple S3 real-time log file connection via Cloud Connect



Trellix | CLOUD CONNECT

Cloud Connect

Add and manage cloud connections for Helix.

● ● ● ● ● Last Update: 2023-02-24T11:45:16-08:00 [Add Cloud Connection](#)

	Name All	Vendor Bottomline, Inc.	Identifier Search 1 records...	Sensor ID Search 1 records...	Helix ID Search 1 records...	Status All	Created [Ⓢ]	Last Event [Ⓢ]	Last Poll [Ⓢ]
Ⓢ	Bottomline	Bottomline, Inc.	trellixbottomline	1677200969137	hexzsq689	●	19 hours ago	Never	Listening...

INTEGRATION DETAILS

region
us-west-2

bucket
trellixbottomline

[Audit Events](#)

[View Logs](#)

[Disable Connection](#)

[Remove Connection](#)

User events parsed by Helix

INDEX SEARCH ▾ username=bartm 🔍

📅 PAST 24 HOURS ▾ CB: ALL ▾ 📌 Save as ▾

History ▾ Favorites ▾ Syntax Help

Filters Groupby ⚙

Layout List ☒ Table

Page Size 10 ▾

Highlight Raw ☒

Geo ☐

Meta ☐

Sort Newest ▾

Show All ▾

View Raw+Parsed ▾

Clear Selection

Add to Case 1

DOWNLOAD 

All Selected 1

⬅ Back to Top

🕒 2023-02-24 16:46:09 UTC rawmsghostname: helix-aws_s3-trellixsandbox class: bottomline

```
{"bottomline.mainframe.activity.type":"Access","bottomline.mainframe.activity.timestamp":"2023-02-24T16:45:00.056Z","bottomline.mainframe.activity.resource.code":"BNKLSTM","bottomline.mainframe.activity.resource.name":"Current Account Subsystem - List Menu","bottomline.mainframe.activity.resource.duration":1421000000,"bottomline.mainframe.activity.message":"bartm accessed the following resource: BNKLSTM","bottomline.mainframe.activity.customer.id":"","bottomline.mainframe.activity.account.id":"","bottomline.mainframe.activity.reference":"","bottomline.mainframe.activity.money.amount":0,"bottomline.mainframe.activity.money.destination":"","bottomline.mainframe.activity.money.source":"","bottomline.mainframe.activity.money.transaction_type":"","bottomline.mainframe.activity.money.reference":"","bottomline.mainframe.activity.money.destination.currency":"","bottomline.mainframe.activity.money.source.currency":"","bottomline.mainframe.activity.network.client.ip":"192.168.1.178","bottomline.mainframe.activity.network.destination.ip":"192.168.1.37","bottomline.mainframe.activity.usr.id":"bartm","bottomline.mainframe.activity.usr.action":"[enter]","bottomline.mainframe.activity.usr.duration":1365000000,"bottomline.mainframe.activity.session.id":"F9149FCC-CCAE-46E3-AF02-6C07AD51C956","bottomline.mainframe.activity.session.step":"7","bottomline.mainframe.activity.session.type":"3270","bottomline.mainframe.activity.session.source":"UNKNOWN","bottomline.mainframe.activity.session.timezone":"NULL","bottomline.mainframe.activity.session.replay":"http://35.87.210.81:30023/replay/cfrm_replay/replay.jsp?gxsessionid=F9149FCC-CCAE-46E3-AF02-6C07AD51C956&gxstep=7"}
```

action: [enter] ▾ **category:** access ▾ **dstipv4:** 192.168.1.37 ▾ **dstusagetype:** rsv ▾ **duration:** 1365000000 ▾ **event_epoch:** ("day":24,"epochtime_field":"eve...
eventtime: 2023-02-24T16:45:00.056Z ▾ **eventtype:** bnklstm ▾ **metaclass:** network.app.mainframe.financial ▾ **msg:** bartm accessed the following re... ▾
object: current account subsystem - list ... ▾ **process:** 7 ▾ **requestduration:** 1421000000 ▾ **sessionid:** f9149fcc-ccae-46e3-af02-6c07ad... ▾ **source:** unknown ▾ **srcipv4:** 192.168.1.178 ▾
srcusagetype: rsv ▾ **statuscode:** 3270 ▾ **timezone:** null ▾ **url:** http://35.87.210.81:30023/repla... ▾ **username:** bartm ▾

🕒 2023-02-24 16:46:09 UTC rawmsghostname: helix-aws_s3-trellixsandbox class: bottomline

URL launches Replay

Trellix | HELIX

INDEX SEARCH

PAST 24 HOURS CB: ALL Save as

Filters Groupby

Layout List ☒ Table

Page Size 10

Highlight Raw ☒

Geo ☐

Meta ☐

Sort Newest

Show All

View Raw+Parsed

Clear Selection

Add to Case

DOWNLOAD 

All Selected

Back to Top

Bottomline

Screen 13 of 21

Font Size

Maximize details view

Session Details Step Details

General	
Sequence	13
Name	Unidentified
Timestamp	15/08/2004 12:13:44.345
User Action	[pf3]
User Action Timestamp	15/08/2004 12:13:45.659

Record changed successfully

BNKTRNF Current Account Subsystem Transaction Maintenance

08/15/04 15:15:15

Customer 300569

Name Expon, Mike SSN 884-67-7872

Address 64 Second st, Barnsley, 899834, NJ, USA

Account 5180575 Branch 003 Date Open: 01/01/2004 Curr Balance:

*Action (A,C,D,I,L,N,R)

Transaction ID : 0000000012 Reference: A1232131344

Transaction Date: 08 / 08 / 2004 Remark:

Transaction Type(?): TT

Amount 1200.50

Fee

Check

Bank(?): Branch(?): Nbr:

Credit card

Type(?): Nbr:

Transfer

Bank(?): 21 Branch(?): 3133133 Account ID: 3234244

Direct Command:

Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10---PF11---PF12---

help retrn main CUST ACCT

6.8.0- 00-5 (2022-07-20 13:26)

Transaction amount

Many other session details such as username, IP, etc. available

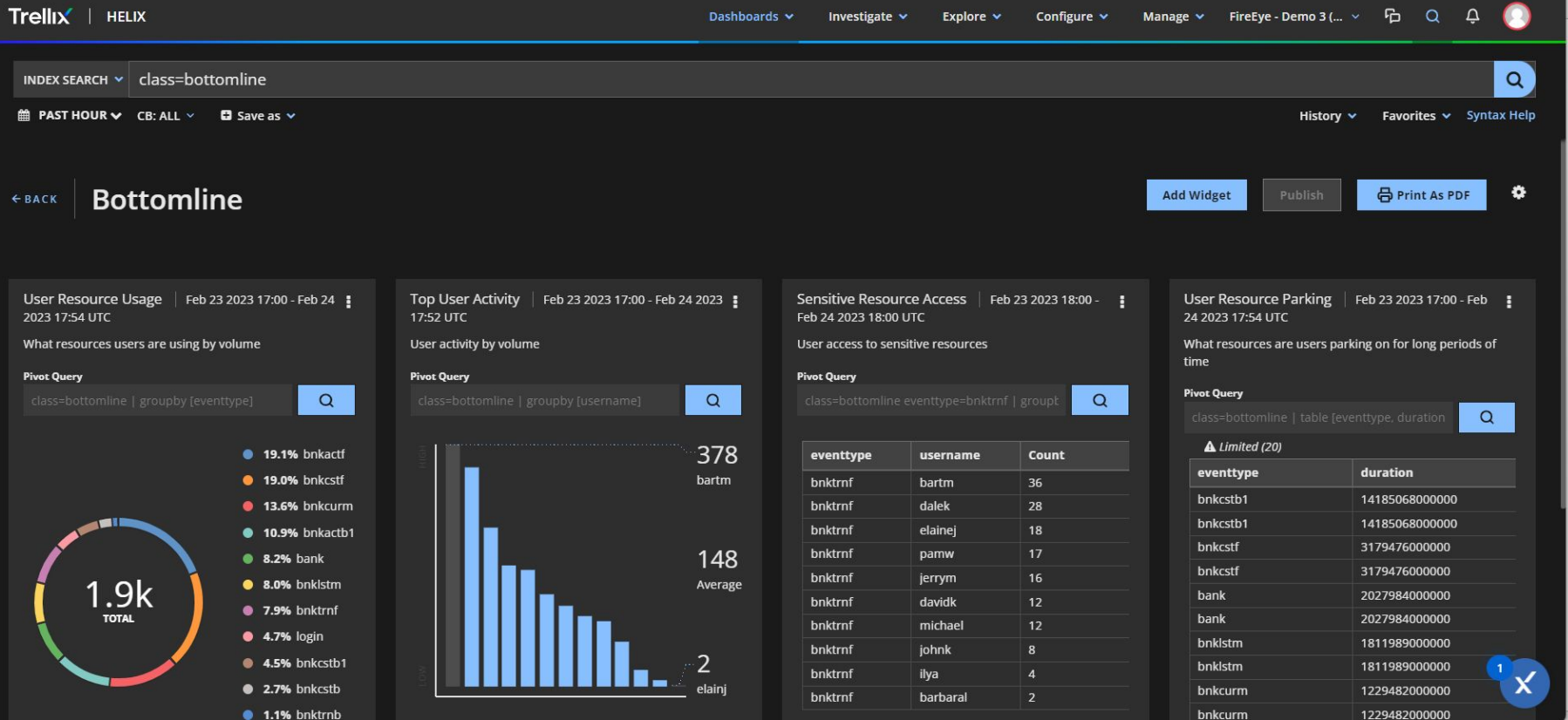
object: current account subsystem - list ... process: 7 requestduration: 1421000000 sessionid: f9149fcc-ccae-46e3-af02-6c07ad... source: unknown srcipv4: 192.168.1.178

srcusagetype: rsv statuscode: 3270 timezone: null url: http://35.87.210.81:30023/repla... username: bartm

2023-02-24 16:46:09 UTC rawmsghostname: helix-aws_s3-trellixsandbox class: bottomline

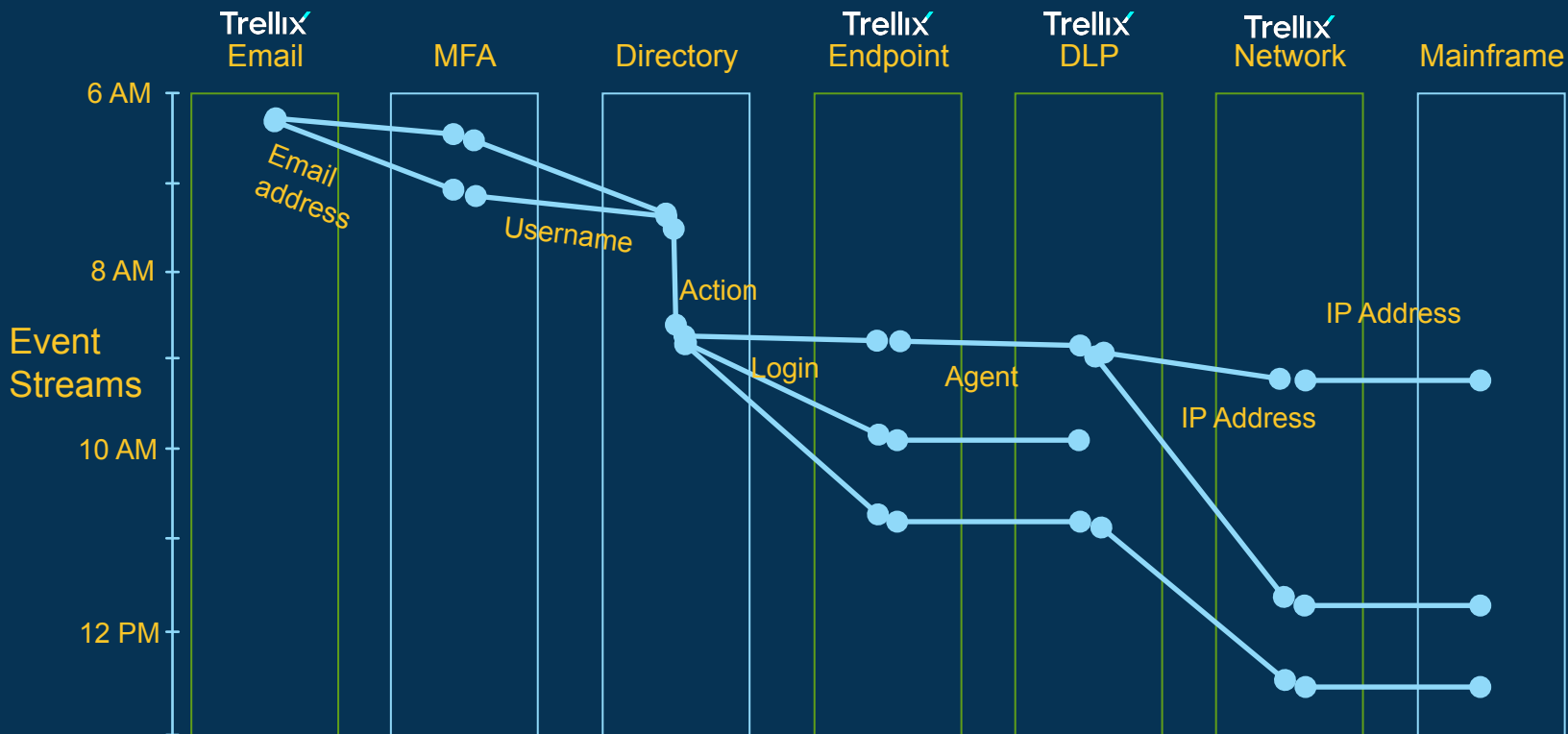
User events used in Helix for:

Rules | Reports / Search | Dashboards



Holistic protection tells the complete story

Phishing > 2FA reset > Service account creation > Endpoint compromises > Data theft > Mainframe



Trellix

13

Highlighted Use Cases

- Connect: User, Identity, Device, Transaction/Activity
- User Entity Behavior Analytics
- Ransomware

Connect: User, Identity, Device, Transaction/Activity



Monitor Application
Transactions & Activity

Go beyond the endpoint –
track user activity in sensitive
applications regardless of
application deployment and
user login location

Quickly expose which users
generated transactions or
accessed sensitive customer
/ proprietary information



Rich Data for Advanced
Analytics Capabilities

Field values from monitored
applications are parsed and
mapped

Enables key data points to be
utilized for analytic and
investigation purposes

User: js123 -> Emp: John S.

IP: 192.168. -> Geo: Jaco, CA

Resource: CCHA -> Tran: Address
Changed to - 321 NE 1st Street



Solve Security, Audit, and
Compliance Needs

Security Against Threats

- ✓ External: Compromised credentials or device, Ransomware, Data theft
- ✓ Internal: Fraud, misconduct, VIP

Audit / Compliance

- ✓ What employee accessed which data

User Entity Behavior Analytics



Analytics Examples

- **Data Theft:** compromised device/credentials to exfiltrate customer data
- **Misuse of Position:** opening accounts for money mules/deposit fraud schemes
- **Incentive Fraud:** opening accounts or falsifying applications to meet quotas/incentives
- **Embezzlement from Customers:** via, cards, ACH, wire, transfer
- **VIP and Vulnerable account access:** Executive, celebrity, elderly account access
- **Employee Self-Service:** servicing one's own account or the accounts of family and friends



Genuine User Behavior Analysis & AI/ML

- Compare user behavior to historical actions to search for differing suspicious activity
- Rich data to drive Artificial Intelligence and Machine Learning

Risks and the Challenges to Prevent Ransomware with Mainframe



Mainframe is a massive exposure

70% of enterprise data resides on mainframe

71% of fortune 500 companies have the core business located on the mainframe



Limited Audit Trail

Less than 40% of organization have a full record of access to their systems



Few Unscathed

29% of firms indicated compromise, while an additional 44% indicate suspected compromise



Ransomware and other threats are in process long before impact

Average time to detect a compromised user is 287 days

Average time to complete a ransomware attack has dropped from over two months in 2019 to less than 4 days today

Traditional Monitoring Approaches Often Fall Short



Log-Based

Traditional monitoring solutions are often overly reliant on audit logs, but audit logs don't capture all of the detail – for instance, user queries are not always logged



Agent-Based

Hard to manage deployment – versions and BYO devices, unreliable data inputs for driving analytics and not able to be run utilizing full capabilities all the time with large data storage requirements for replay



A Day Late is Too Late

Retroactive audits of activity may be sufficient for some purposes, but not when it comes to protecting your organization

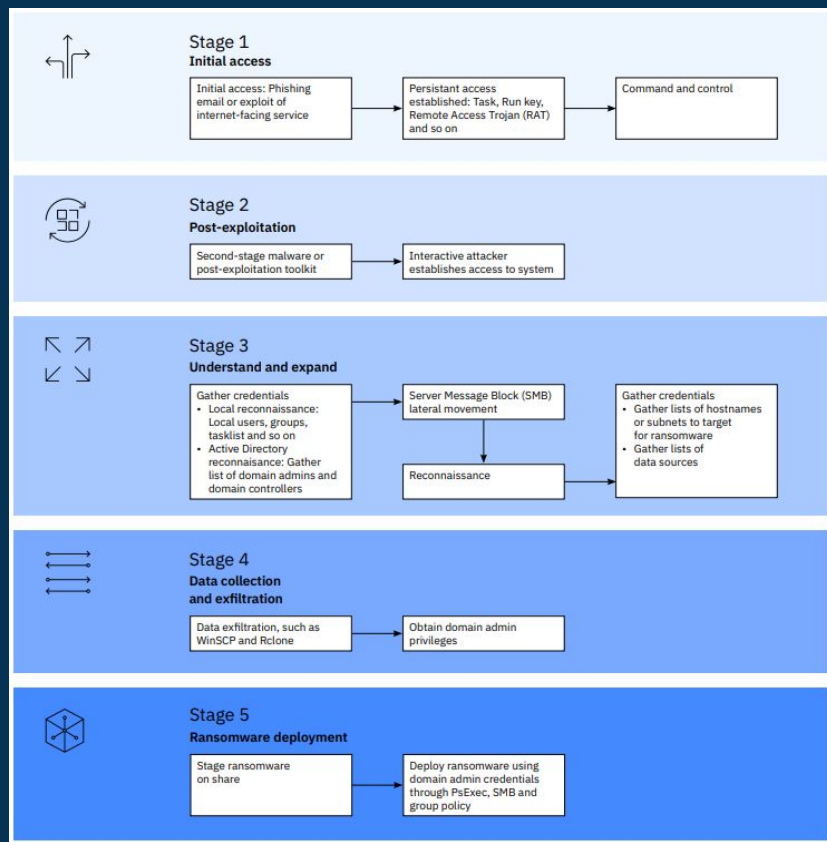
5 Stages of a Ransomware Attack

A process that used to take months...

...now takes days

...soon to take hours

...executed using internal user accounts





Partner.cfrm@bottomline.com

Andrew.Leon@bottomline



SIA@trellix.com

Nico.Devoti@trellix.com

Thank you!

Visit Us



Bottomline.com/risk-solutions



Trellix.com - Mind of the CISO



Video: [Bottomline Record & Replay](#)