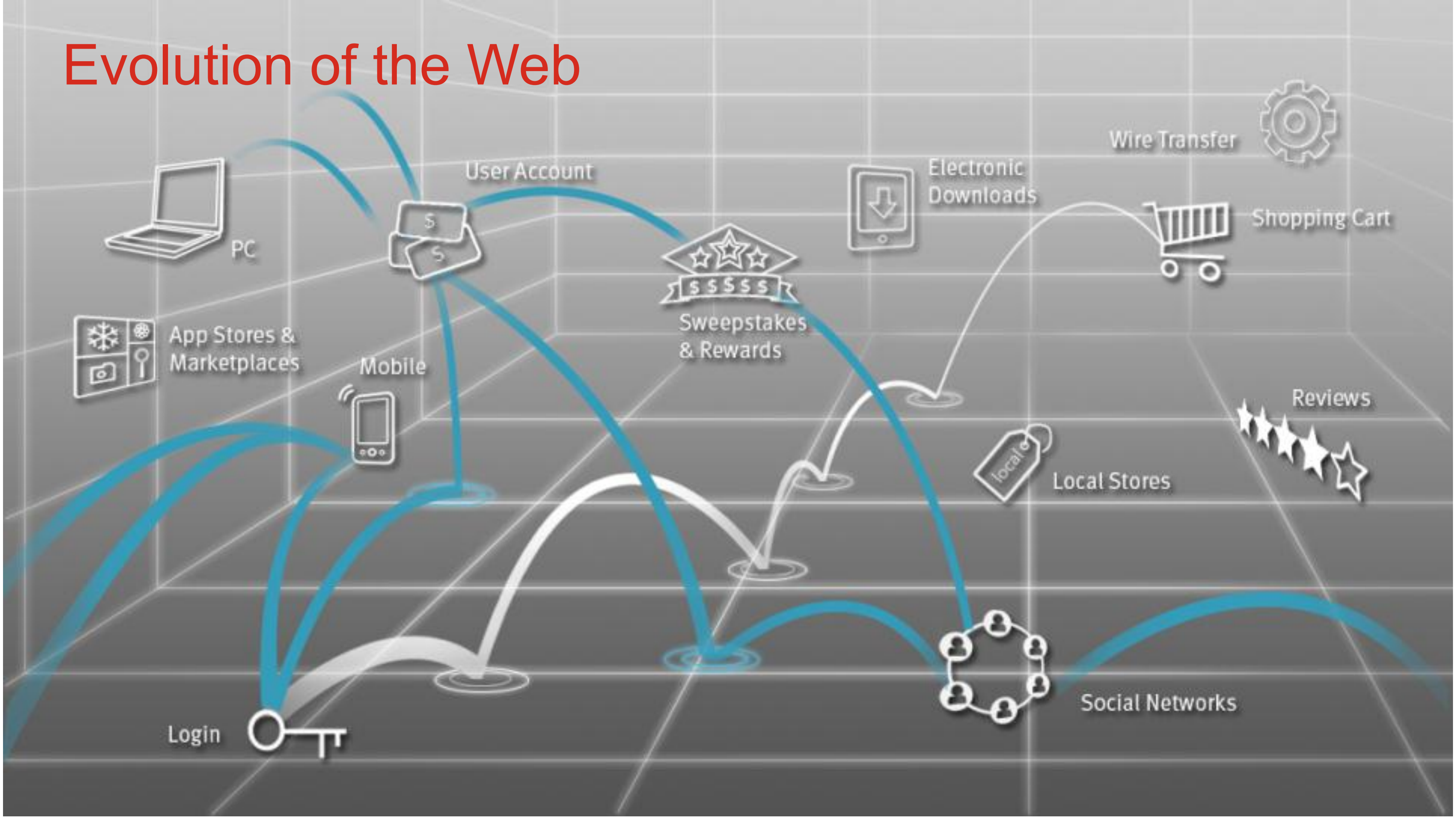
Evolution of the Web



Design Objectives

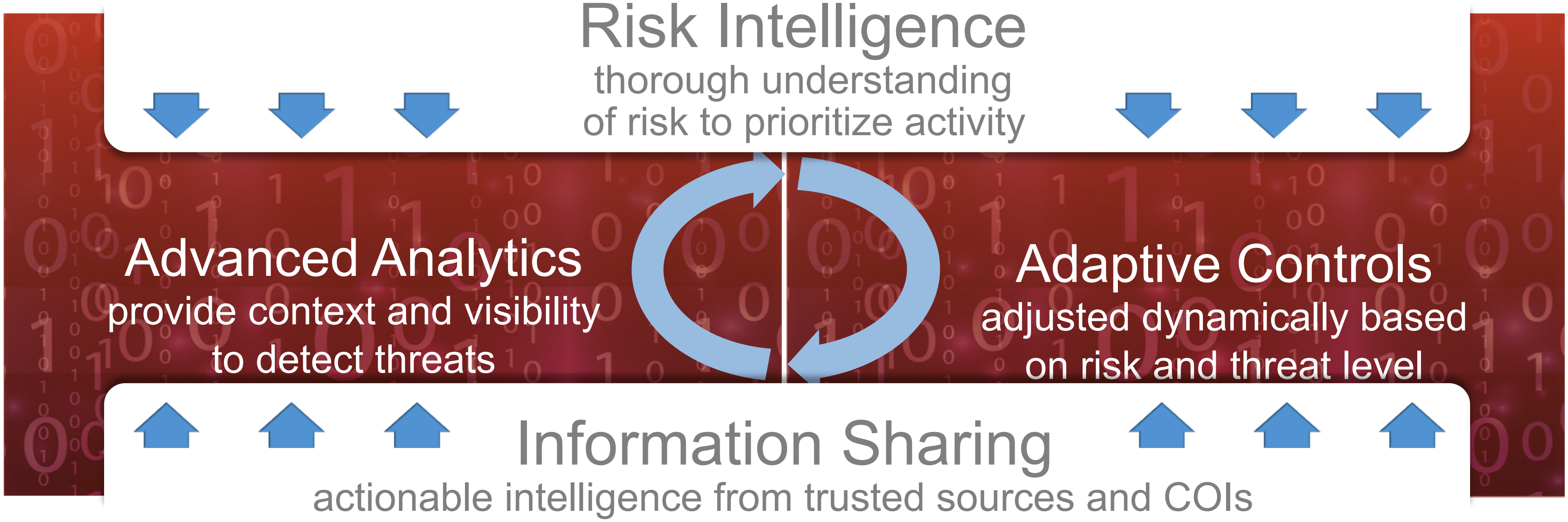
Security Goals

- □ High Accuracy In Real Time
- □ Avoid The End Point: Assume Compromised & Tablet, Smart Phone Growth
- □ Don’t Impact The User/Customer Experience
- □ Don’t Touch The Web Application/Rely On Logs
- □ Self Learning, No Tuning Required To Proactively Detect New Threats

Behavior

Intelligence-Driven Security Powered by Big Data

Risk-based, contextual, and agile



Risk Intelligence

thorough understanding of risk to prioritize activity

Advanced Analytics

provide context and visibility to detect threats

Adaptive Controls

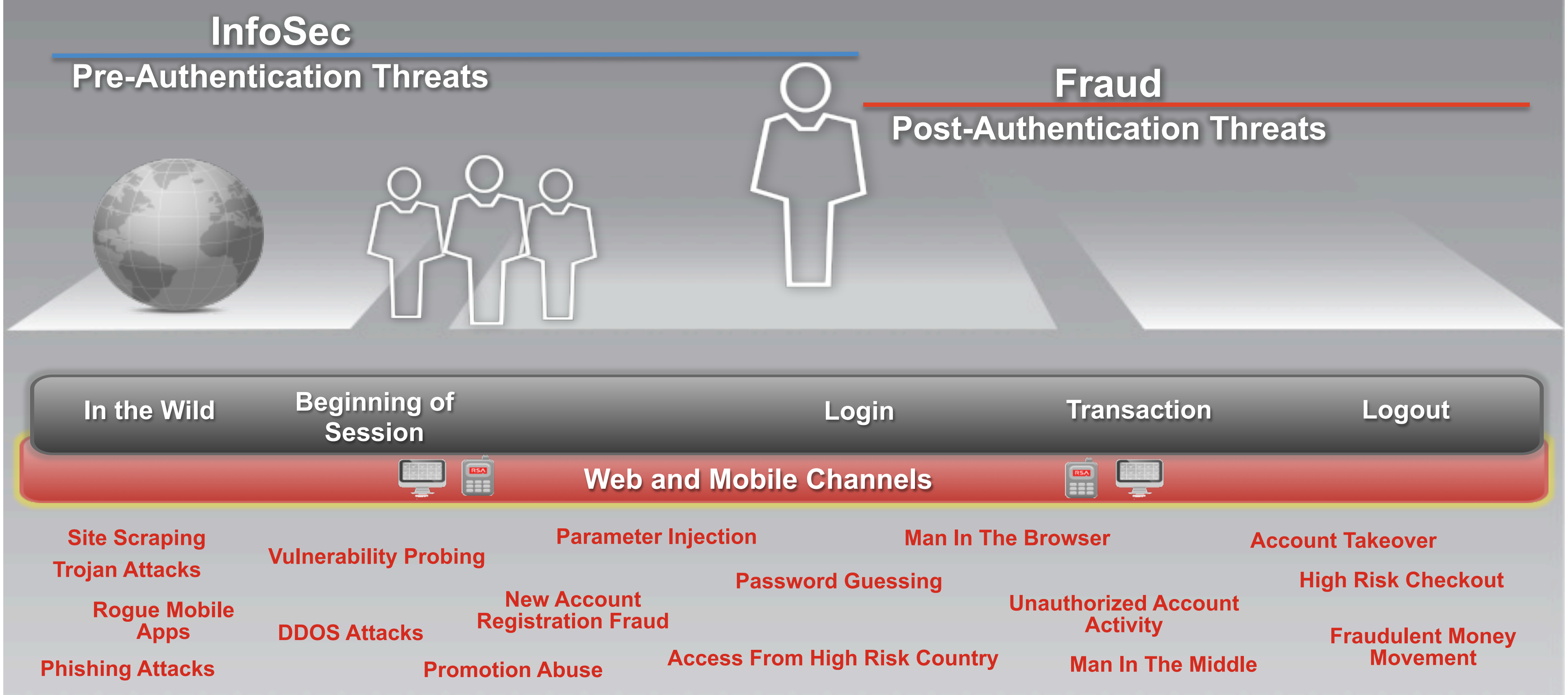
adjusted dynamically based on risk and threat level

Information Sharing

actionable intelligence from trusted sources and COIs

RSA EMC²

Threats Span Across Customer Interaction Points



InfoSec

Pre-Authentication Threats

Fraud

Post-Authentication Threats

In the Wild

Beginning of Session

Login

Transaction

Logout

Web and Mobile Channels

Site Scraping

Trojan Attacks

Rogue Mobile Apps

Phishing Attacks

Vulnerability Probing

DDOS Attacks

Parameter Injection

New Account Registration Fraud

Promotion Abuse

Password Guessing

Access From High Risk Country

Man In The Browser

Unauthorized Account Activity

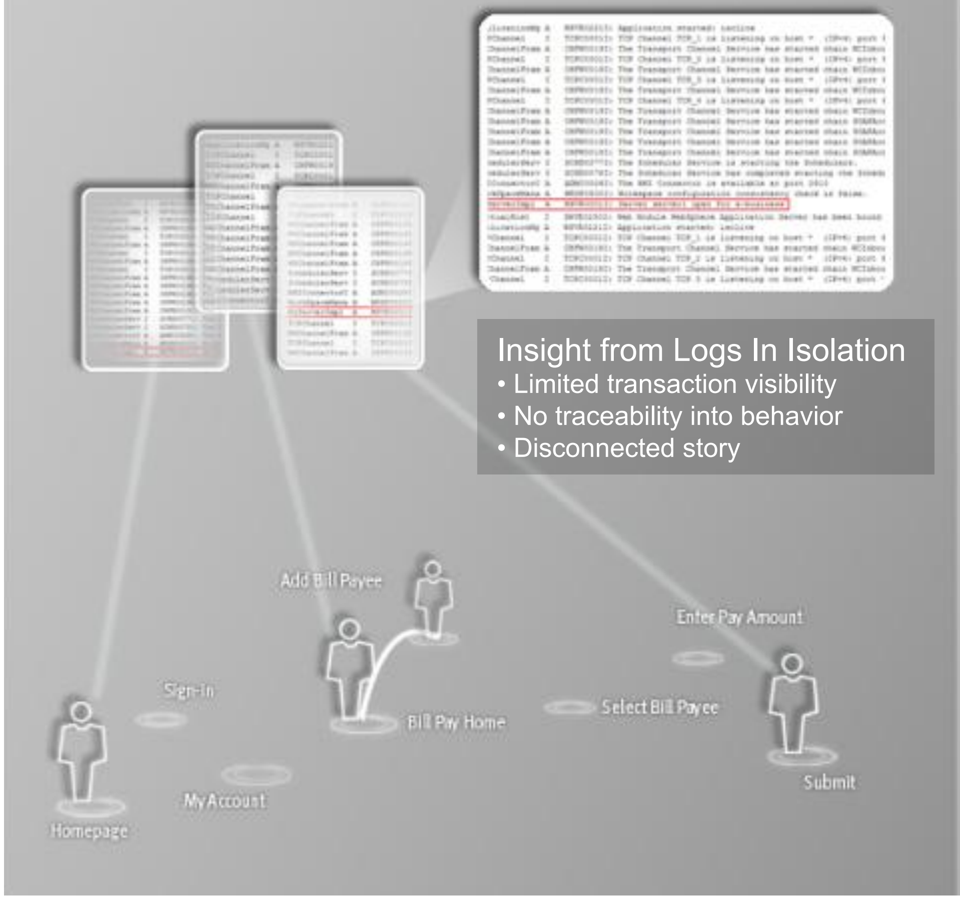
Man In The Middle

Account Takeover

High Risk Checkout

Fraudulent Money Movement

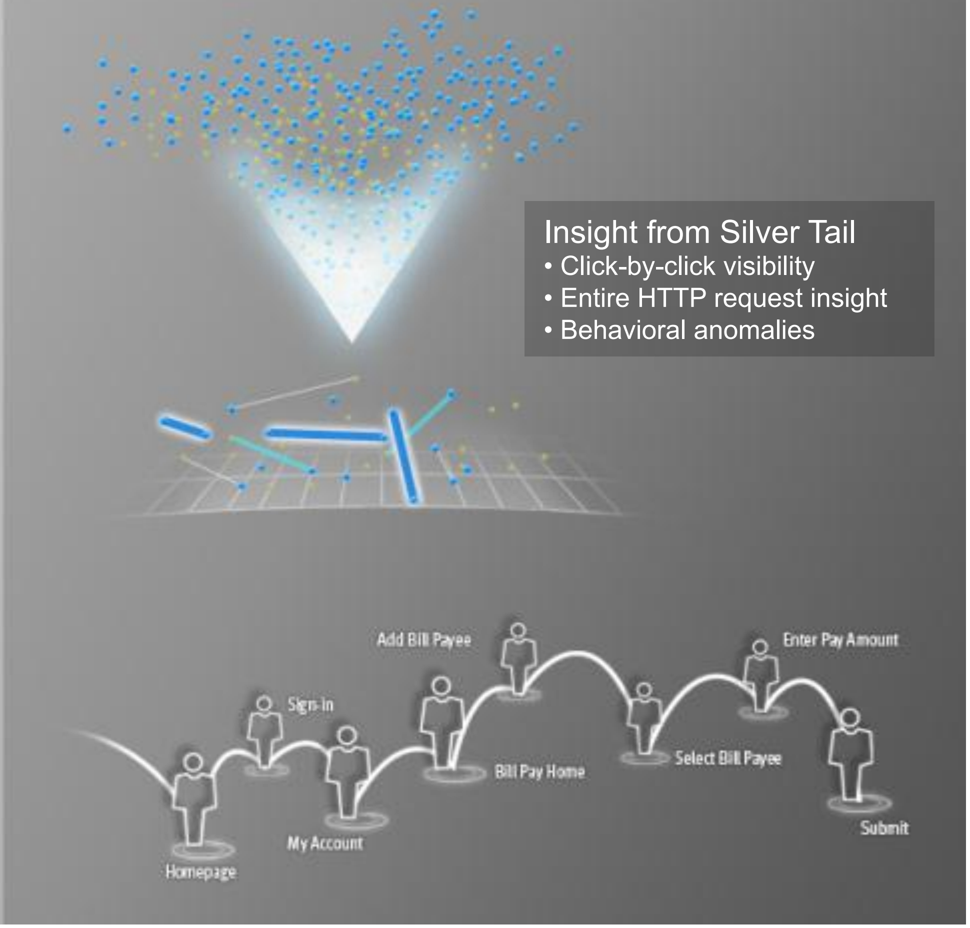
Big Data Approach To Security



```
[illegible] A  [illegible]: Application started: [illegible]
[illegible]Channel I  [illegible]: TCP Channel TCP_1 is listening on host *  (IPv4) port [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
[illegible]Channel I  [illegible]: TCP Channel TCP_2 is listening on host *  (IPv4) port [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
[illegible]Channel I  [illegible]: TCP Channel TCP_3 is listening on host *  (IPv4) port [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
[illegible]Channel I  [illegible]: TCP Channel TCP_4 is listening on host *  (IPv4) port [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
[illegible] I  [illegible]: The Scheduler Service is starting the Schedulers.
[illegible] I  [illegible]: The Scheduler Service has completed starting the Sched[illegible]
[illegible] A  [illegible]: The RMI Connector is available at port [illegible]
[illegible] A  [illegible]: Wilespace configuration consistency check is false.
[illegible] A  [illegible]: Server server1 open for e-business
[illegible] I  [illegible]: Web Module WebSphere Application Server has been bound
[illegible] A  [illegible]: Application started: isclite
[illegible]Channel I  [illegible]: TCP Channel TCP_1 is listening on host *  (IPv4) port [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
[illegible]Channel I  [illegible]: TCP Channel TCP_2 is listening on host *  (IPv4) port [illegible]
ChannelFram A  [illegible]: The Transport Channel Service has started chain [illegible]
[illegible]Channel I  [illegible]: TCP Channel TCP_3 is listening on host *  (IPv4) port [illegible]
```

Insight from Logs In Isolation

- Limited transaction visibility
- No traceability into behavior
- Disconnected story



Insight from Silver Tail

- Click-by-click visibility
- Entire HTTP request insight
- Behavioral anomalies

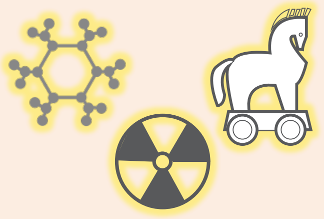
The RSA Silver Tail Approach

Theoretical

```
192.168.17.221
172.26.123.12
192.168.17.222
192.168.17.223
192.168.17.224
```

- The decision is based on deductive reasoning, such as, something happening against other possible things that could happen.
- For example, looking for a specific datapoint, such as a specific signature.

Empirical



- The decision is based on data that has been collected by experiments and direct observation
- A data scientist takes an empirical approach to analysis.

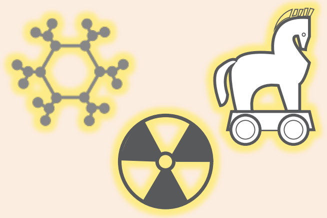
The RSA Silver Tail Approach

Theoretical

192.168.17.221
172.26.123.12
192.168.17.222
192.168.17.223
192.168.17.224

- Anomalies, detection, analytics
- We detect the current user/IP sessions to the statistically averaged user behavior for a site

Empirical

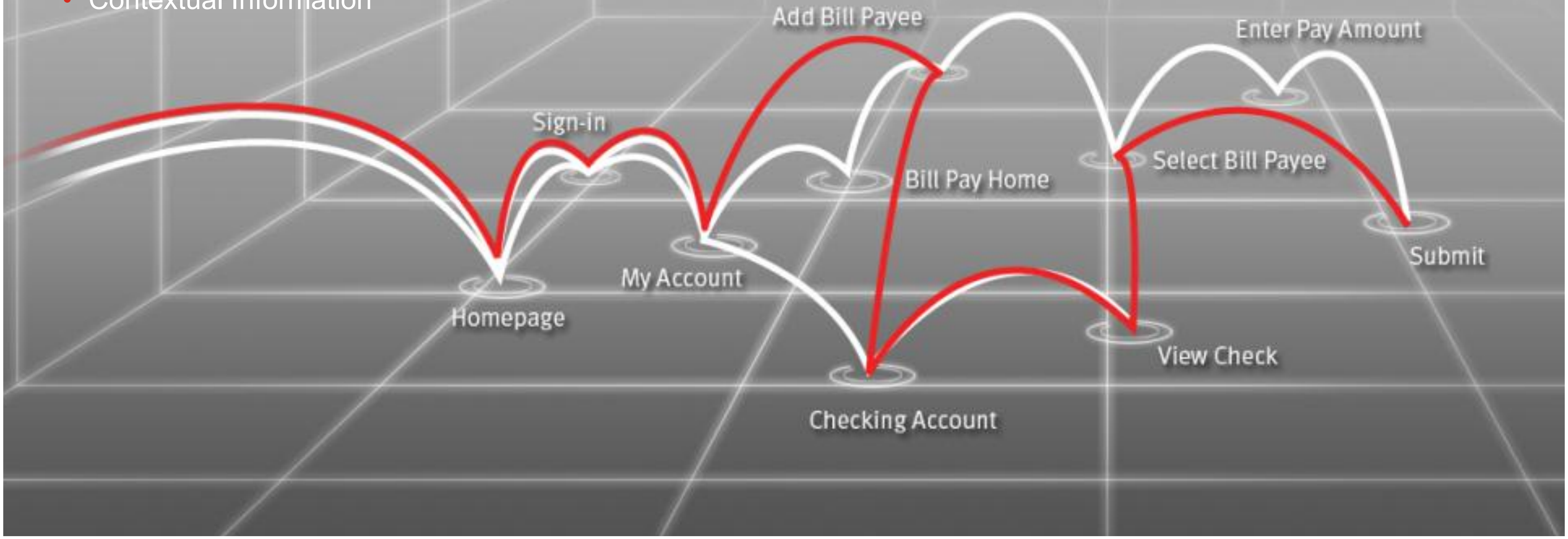


- The decision is based on data that has been collected by experiments and direct observation
- We examine known threats, rules, signatures

Anomalous Behavior Detection

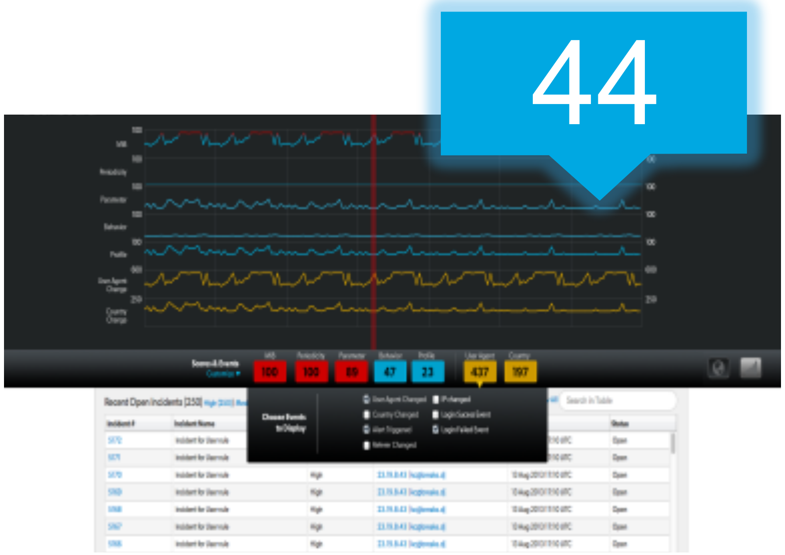
Criminals Look Different than Customers

- Velocity
- Page Sequence
- Origin
- Contextual Information



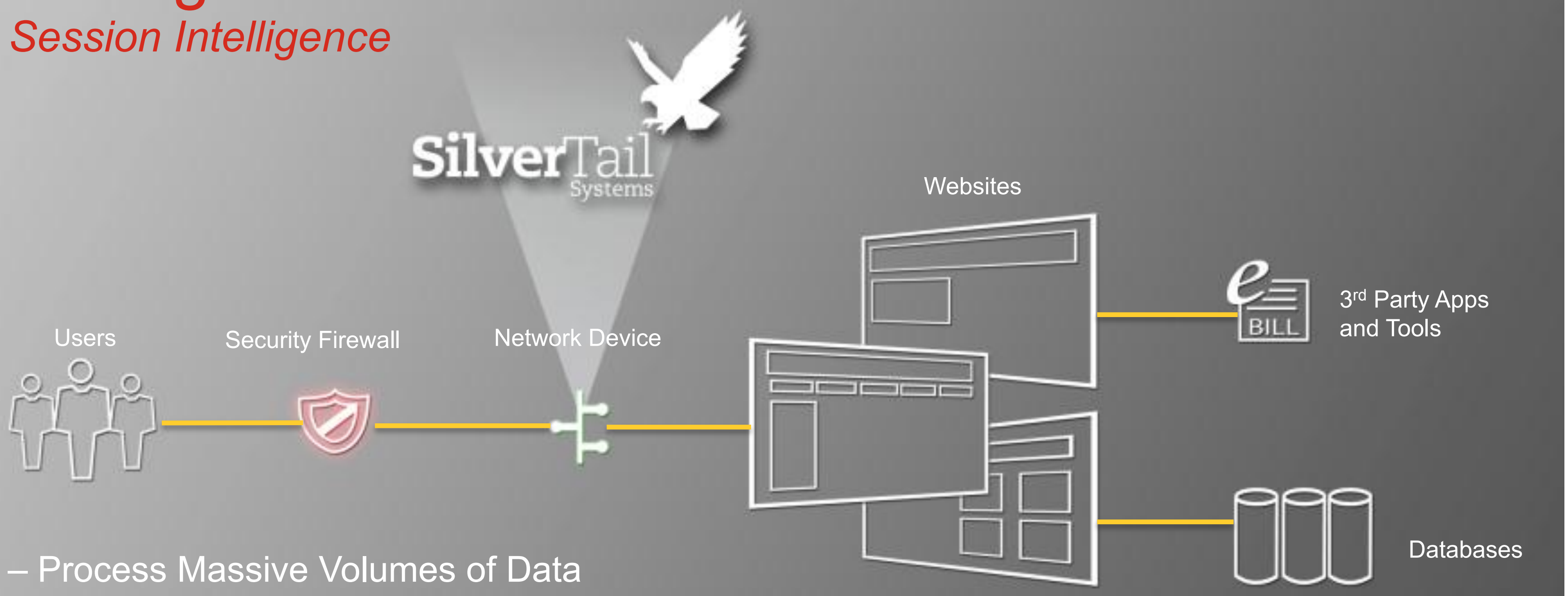
The Theoretical Approach

- Traffic patterns
- Profile of session compared to data model
- Anomaly ratio = difference between the data model and a current session
- Auto-tuning mechanism accounts for cyclical patterns
- Normalized score is calculated



Protecting Websites

Web Session Intelligence



Scale – Process Massive Volumes of Data

Monitor – Complete Visibility Into Web Sessions

Analytics – Behavioral Patterns of Crowd & Users

Real-Time – Threat Scores & Rules