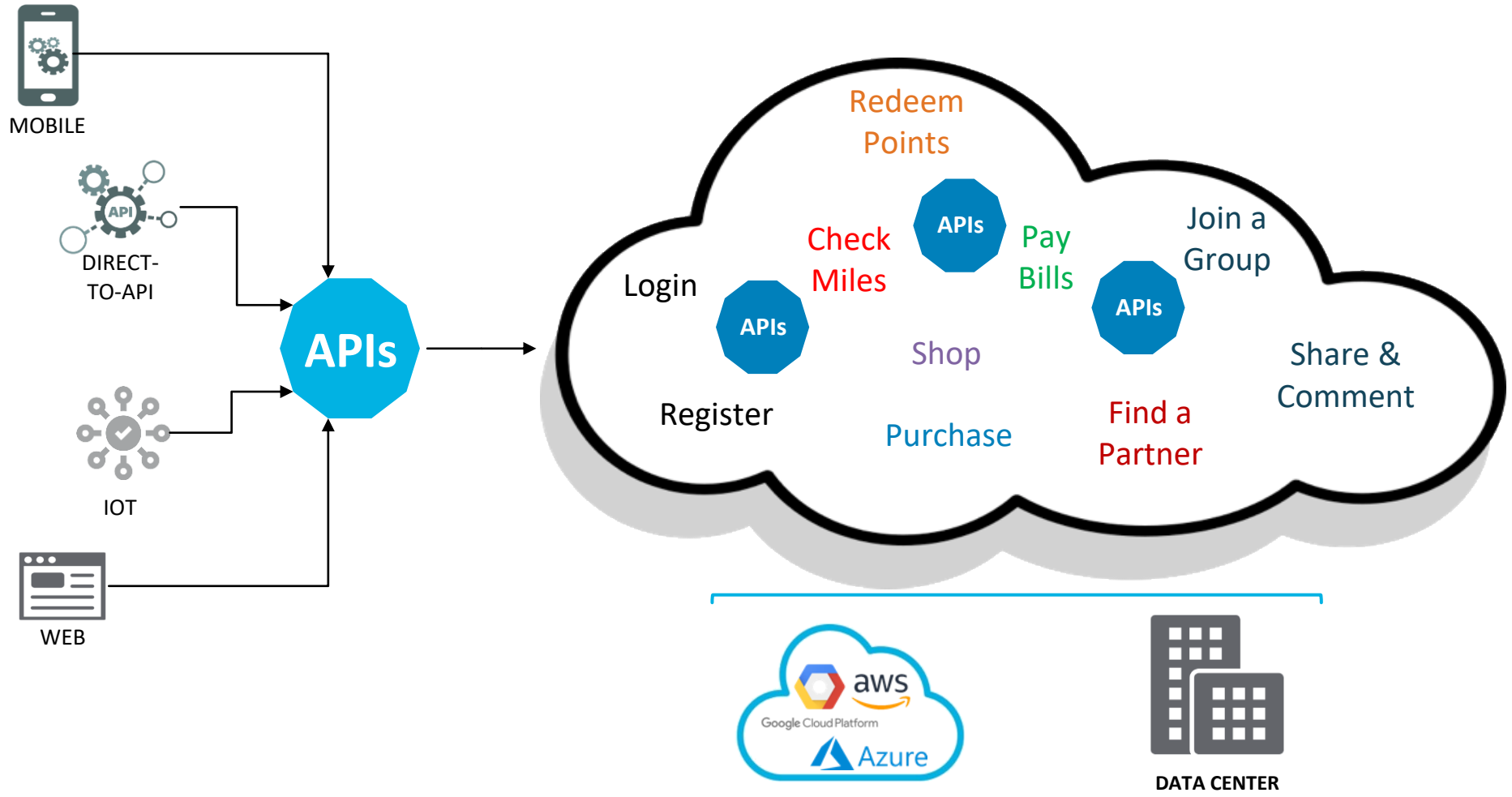
How APIs Simplify Automated Attacks:

Prying-Eye Direct-to-API Enumeration Attack

Shreyans Mehta
CTO and Co-Founder
shreyans@cequence.ai
www.cequence.ai

APIs Rule The World

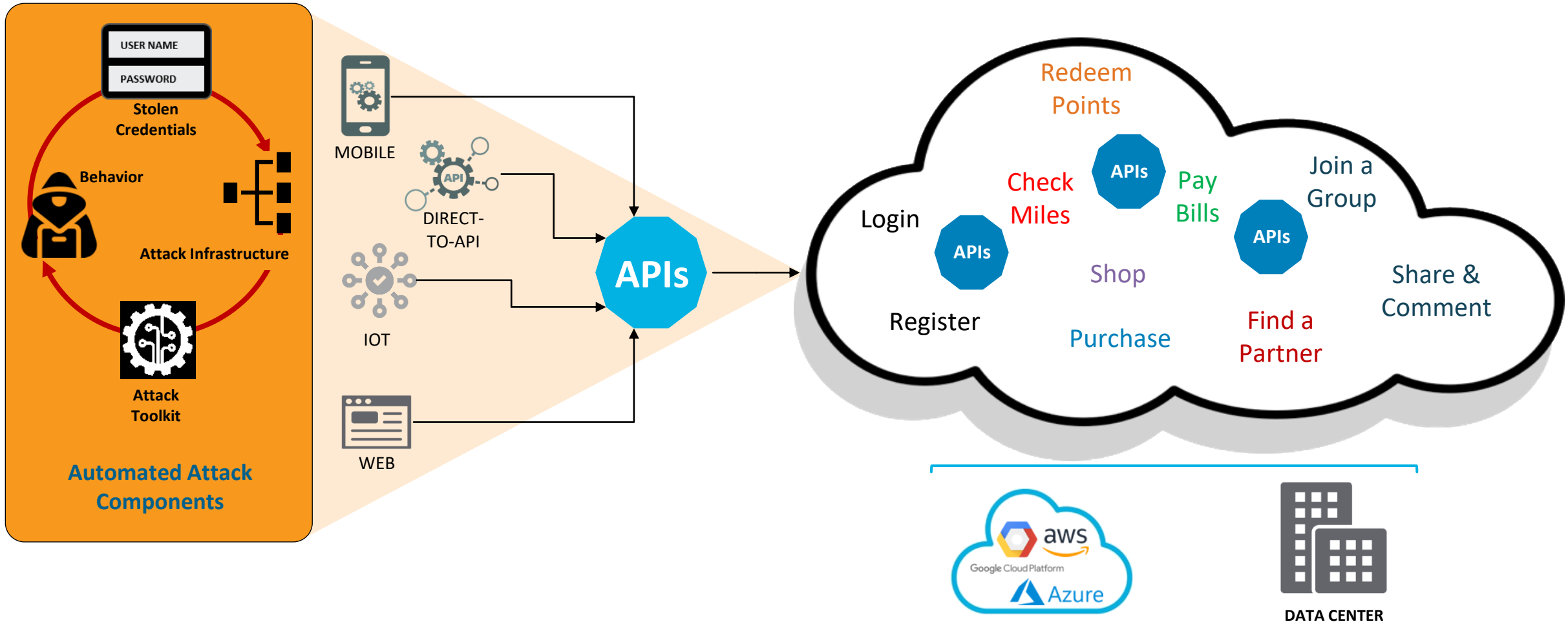
Drivers: Public Facing Apps, Microservices, Ecosystem Expansion, New Development Methods



CEQUENCE™ SECURITY

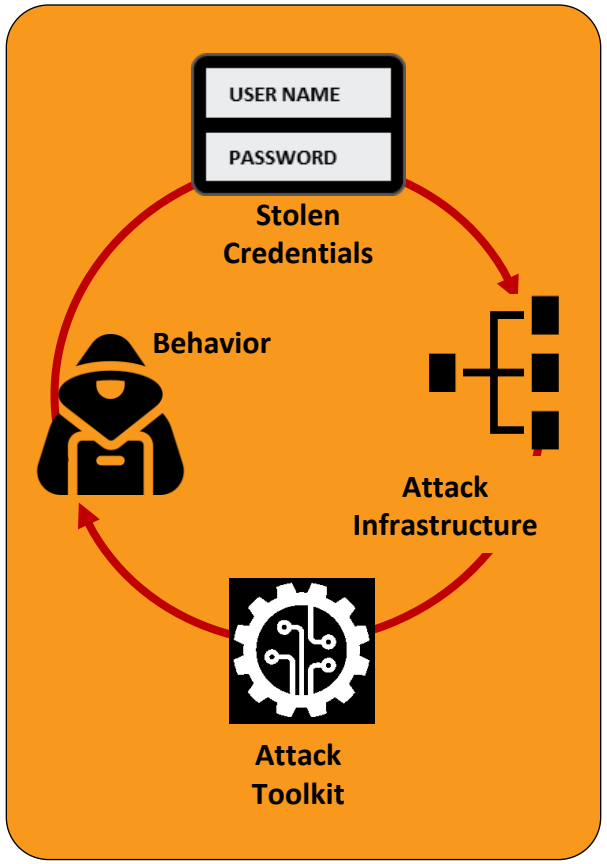
Public Facing Applications are Attack Targets

Bad Actors Leverage API Benefits of Automation, Flexibility & Ease of Use



CEQUENCE SECURITY

Automated Attack Components

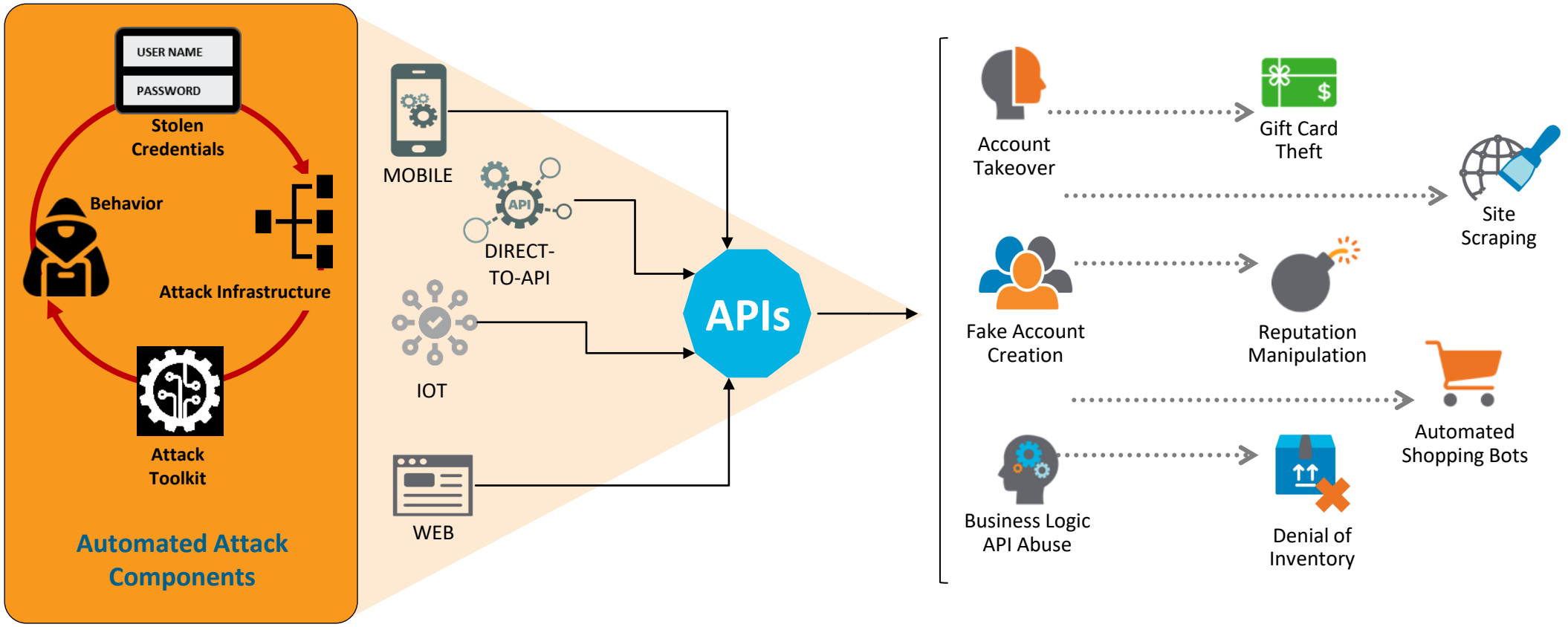


Automated Attack Components

- Tools: Code bad actors use to execute the attack
- Credentials: User information regularly refreshed via data breaches
- Infrastructure: Enable anonymous, large scale attack distribution
- Behavior: How bad actors react when discovered, blocked

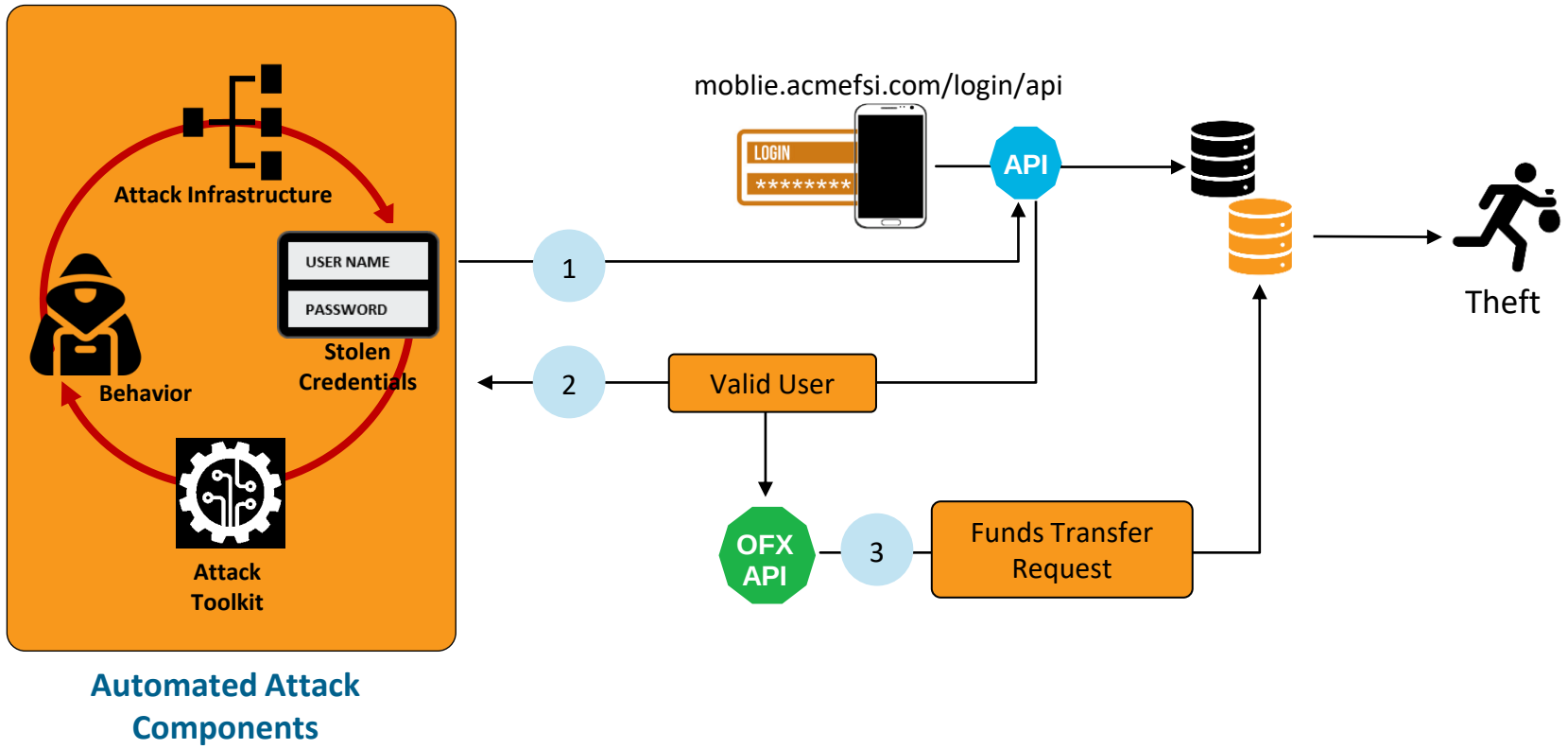
Ramifications: Fraud and/or Theft

Attacks are Highly Automated, Appear Legitimate



CEQUENCE SECURITY

Customer Attack Example: FSI Mobile Login API & Funds Theft Attack

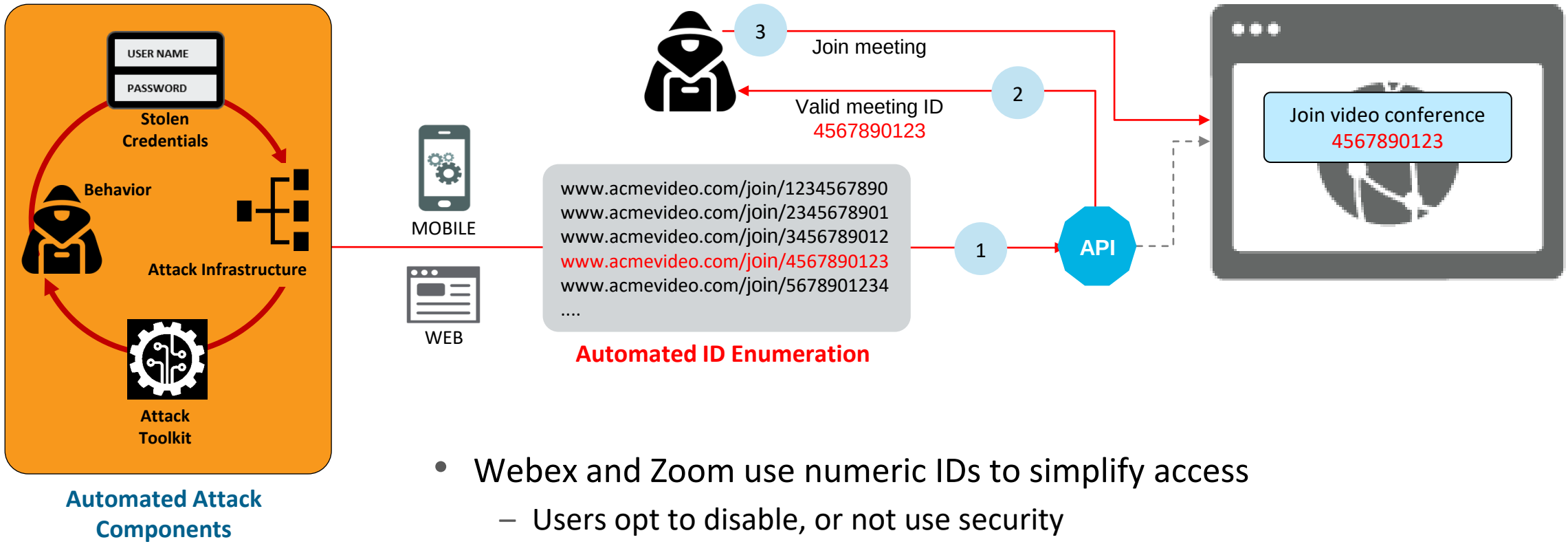


- Account take over attack directly against the mobile app login API
- Successful account compromise
- Funds transfer immediately initiated via OFX (funds transfer API)

CEQUENCE SECURITY

Prying-Eye Video Conferencing Enumeration Attack

Direct-to-API Attack



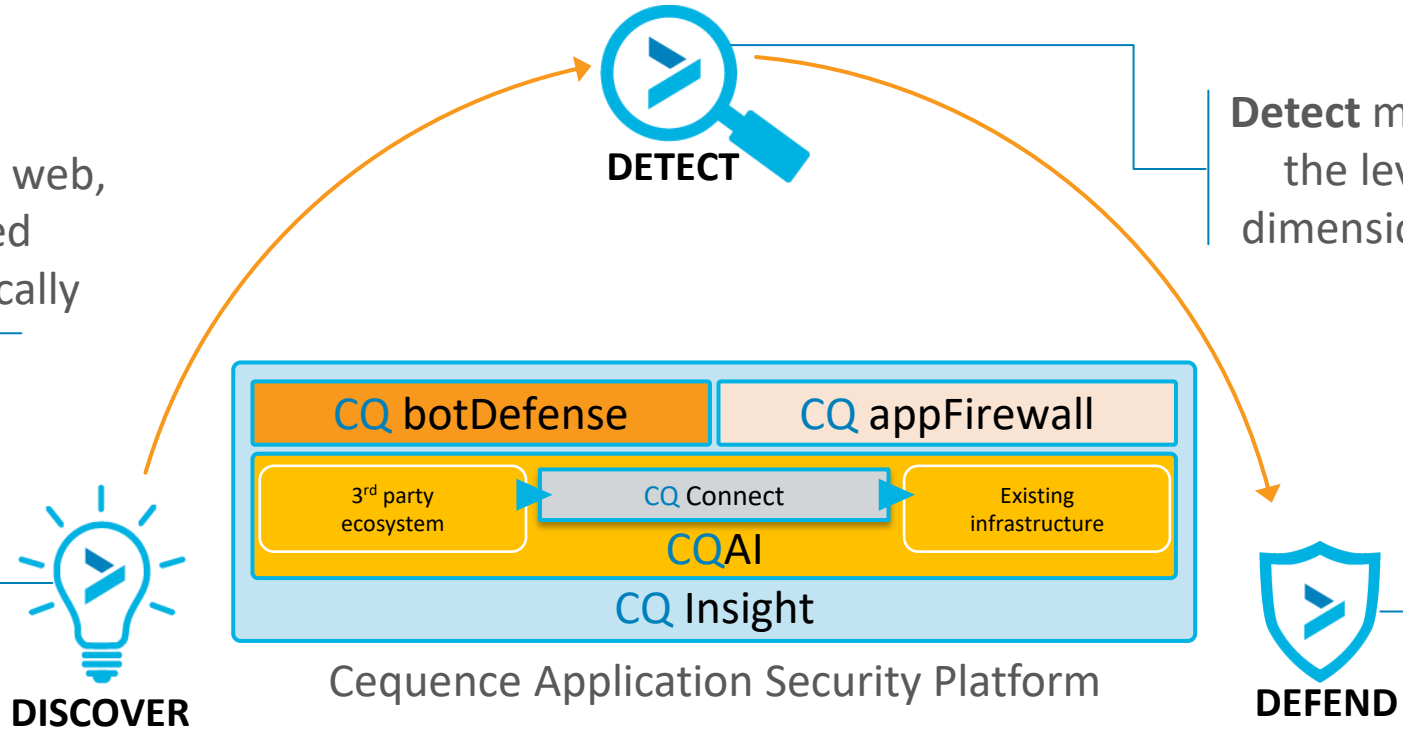
- Webex and Zoom use numeric IDs to simplify access
  - Users opt to disable, or not use security
- Automation can quickly cycle through namespace to find valid IDs
  - Web form fill can be automated - APIs simplify the attack
  - Mobile applications can be reverse engineered

PUBLIC SERVICE ANNOUNCMENT: USE PASSWORDS ON YOUR WEB MEETINGS!!!!

Cequence ASP: An AI Driven Approach to Automated Attack Prevention

Discover all public facing web, mobile, and API-based applications - automatically

Detect malicious requests down to the level of intent with multi-dimensional AI powered analytics



Defend using a range of options to mitigate threats and deceive attackers

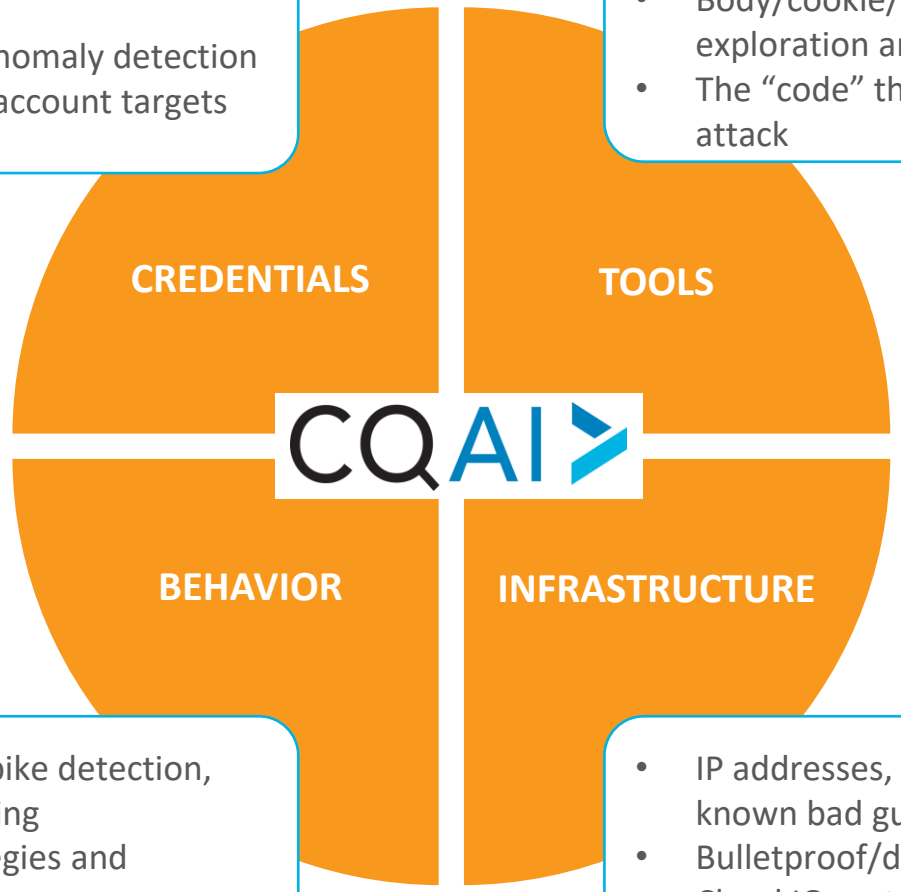
- **CQAI** discovers & analyzes all application transactions; renders verdict
- **CQ botDefense and CQ appFirewall** mitigates automated threats & exploits
- **CQ Insight** provides actionable information on attack in progress
- **CQ Connect** enables information sharing within your infrastructure

CEQUENCE™ SECURITY

Four Pillars of Detection

- Data breaches
- Username & anomaly detection
- The take over account targets

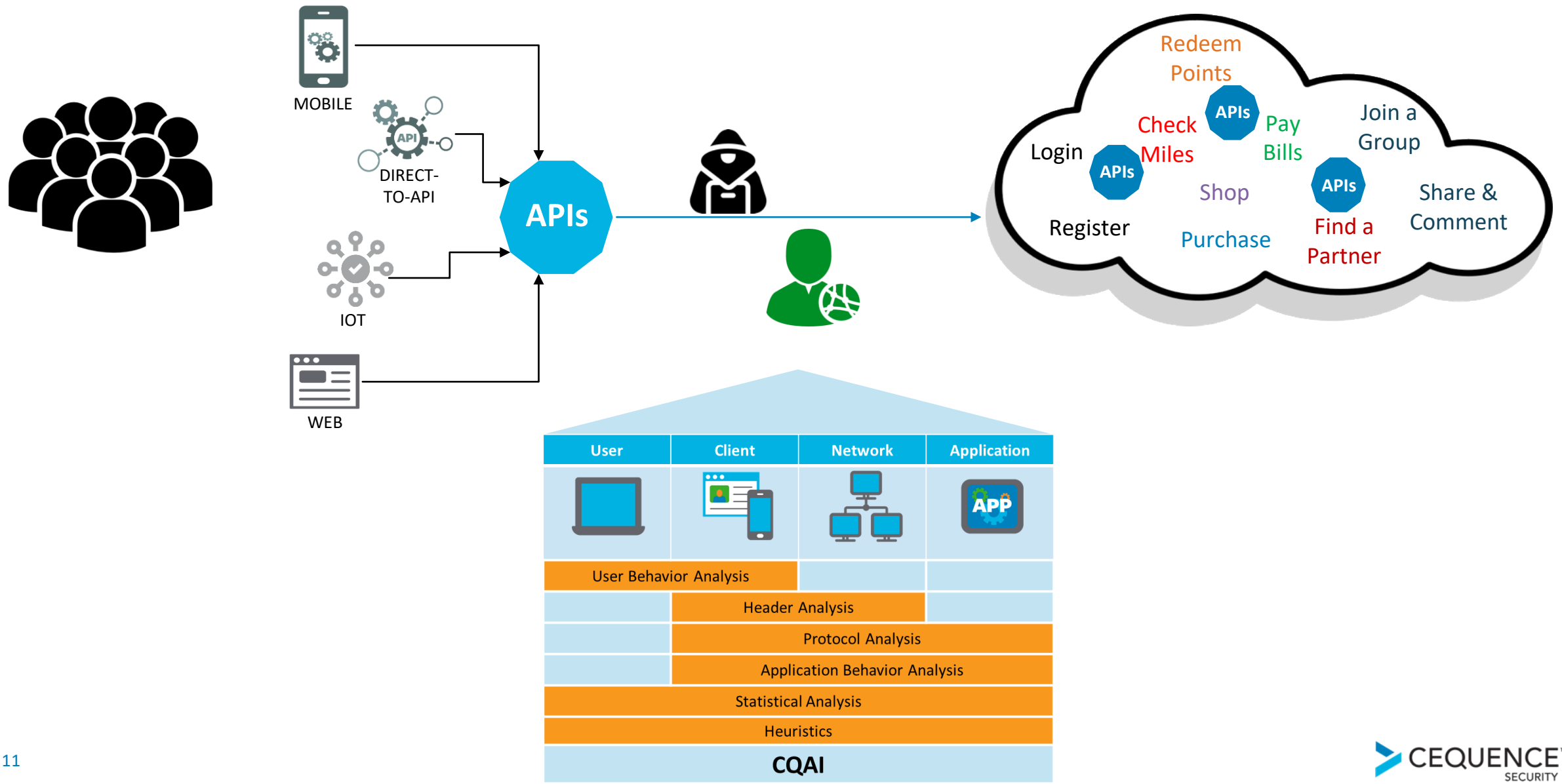
- HTTP/SSL Fingerprints
- Body/cookie/payload exploration and heuristics
- The “code” that executes the attack



- Time of day, spike detection, Machine learning
- Attacker strategies and methodologies

- IP addresses, Orgs/ISPs of known bad guys
- Bulletproof/data center Proxies
- Cloud IQ customer attack DB

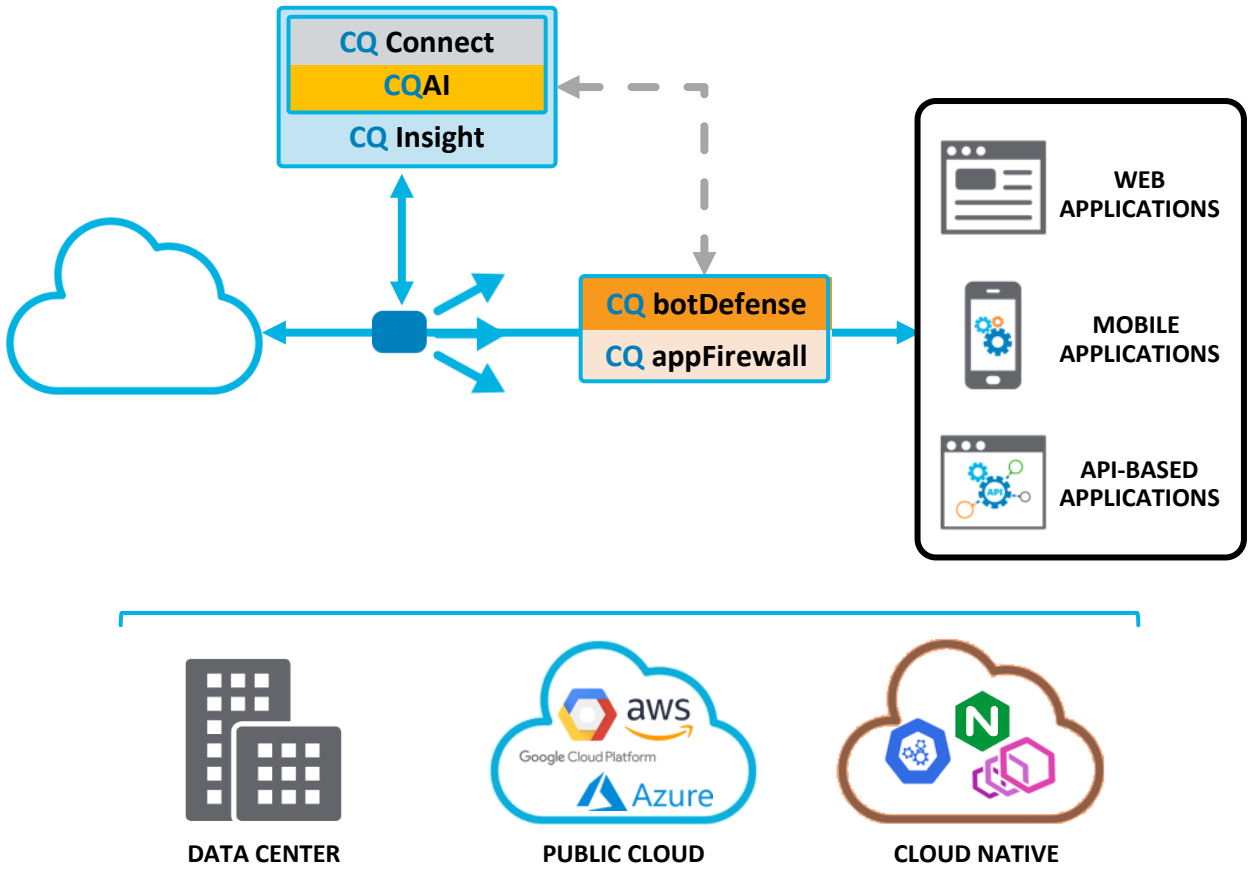
CQAI – Determining Malicious or Legitimate Intent



CEQUENCE SECURITY

Cequence Application Security Platform Deployment Options

- Flexible container-based, cloud-native architecture
- Integrates with and enhances existing security infrastructure
- Bakes security into the application infrastructure
- Non-intrusive, out-of-band deployment
- Data center, cloud, hybrid

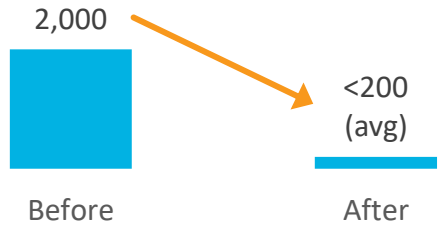


CEQUENCE SECURITY

Delivering Measurable Results at Scale

Fortune 100 Financial

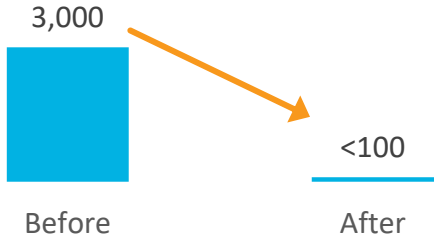
90% reduction in daily accounts compromised



~ 20 applications with **50-90%** of the logins from bots

Fortune 500 Retailer

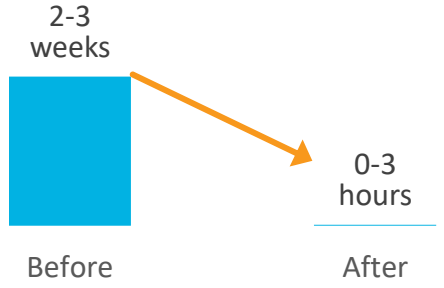
99.7% reduction in daily accounts compromised



~ 16 applications with **60-90%** of the logins from bots

Large Social Network

99.7% reduction in ATO campaigns response time



29 applications protected with **5-6x** efficacy improvement over incumbent*

Securing Applications Across Multiple Channels

*Shape Security

CEQUENCE SECURITY

About Cequence Security

- Venture-backed start-up bringing much-needed innovation to application security
- Award-winning AI-powered security platform that automatically protects web, mobile, API-based applications from bot attacks and vulnerability exploits
- Deployed across multiple F500, social media, retail, and financial services organizations
- Successful, veteran leadership team from Palo Alto Networks and Symantec
- Visit us at www.cequence.ai

CEQUENCE SECURITY

Learn More

- Open Talk: Protecting API based Applications from Automated Attacks - Thursday 9:00-9:50
- Visit us at booth #226
- www.cequence.ai

Thank You

Shreyans Mehta
shreyans@cequence.ai