cyber team six.

Cutting Edge Risk Management | Editor's Choice Fraud Prevention

AT A GLANCE

A software product company founded by former law enforcement, commercial and academic credentialed practitioners building tools to defeat the cyber enabled crimes of fraud, theft and espionage. | cyberteamsix.net

PATRICK WESTERHAUS
Chief Executive Officer

20+ years experience in financial and cyber crime at FBI and Wells Fargo, building new enterprise programs

JOHN LENKART
Chief Strategy Officer

25+ years experience in FBI counterintelligence creating government-wide platforms securing critical infrastruture

MAURICIO PEREZ
Chief Revenue Officer

20+ years experience in software sales, procurement, and supply chain acquisition supporting SAS and Wells Fargo C-Suite

JASON BRITT
Chief Technology Officer

15+ years in Computer Science with a PhD in data mining, AI and machine learning, developing software germane to cybercrime

US Army | Wells Fargo | citibank | KPMG | sas | UAB | Johns Hopkins University

cyber team six.®

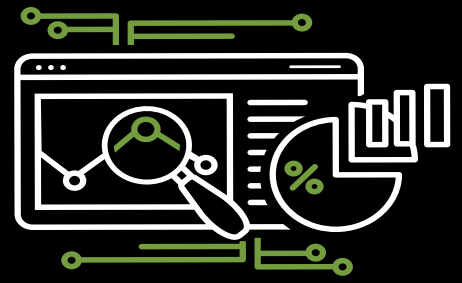
Market Differentiation

Our Solutions

Fraud Risk Identifier

An anti-fraud orchestration platform providing Indicators of Financial Compromise (IoFC)® to allow anti-fraud teams time to prevent the account and relationship takeover business cycle. The Fraud Risk Identifier (FRI) protects individual customers by determining if they have been compromised by cyber threats like active, semi-active, and passive malware; phishing; credential replay attacks; malicious proxies; and dark market card sales advertisement.

Current market offering & patent pending



Fraud Risk Identifier+

Empowers analysts to prevent fraud across the enterprise by utilizing the data learned from the Fraud Risk Identifier and adding point and click deep link analysis on common customer data attributions (e.g. phone numbers, IPs, device IDs, etc.). Through visualization, the Fraud Risk Identifier Plus will reveal the point of compromise, the actors, and money mules used by cybercriminals.

Developing with TEKsystems

Verify

Identifies external threats and defines the true risk for organizations when considering business engagement with vendors or persons who may have unseen ties to malicious countries or organizations. These proven threats pose enormous risk to a company's infrastructure and reputation through breaches and IP theft.

Developing with Johns Hopkins University, Applied Physics Lab

What makes our technology different?

// **Takes the initiative away** from the criminals whereas current market offerings wait and react after illegal acts have happened

// **Provides the ground truth** from external datasets of what the cybercriminals know and how they victimize an organization's individual customers

// **Enables institutions to build** true predictive machine learning models to advance fraud detection and prevention opportunities

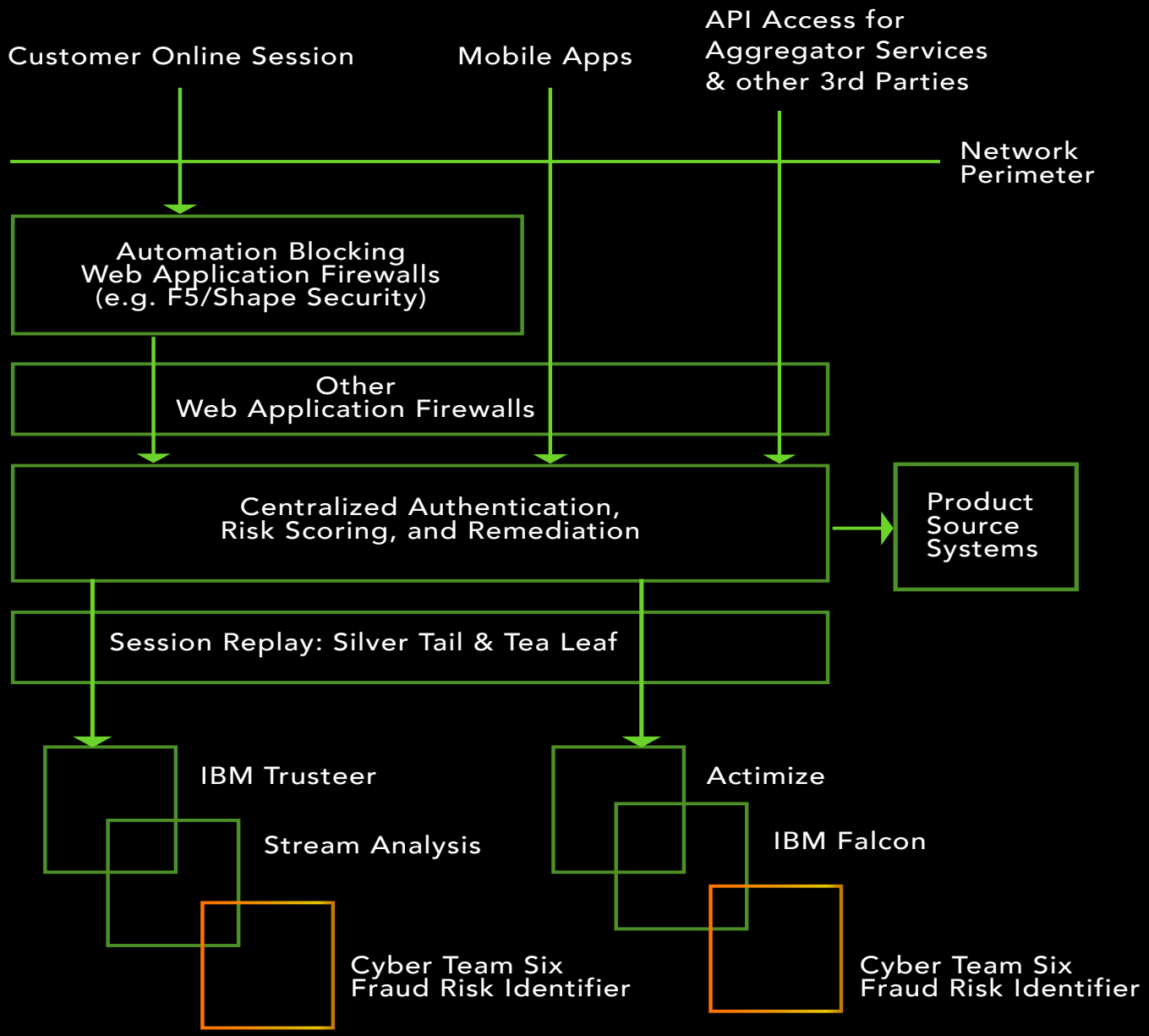
// **Adopts and seamlessly changes** with how hackers target people

// **Expands an organization's ability** to manage its attack surface by focusing on customer devices and data, and not employees and end-points

// **Connects data to investigate** cybercrime actors tied to fraud loss attempts, driving the use of threat hunting platform technology

// **Enhances compliance and reporting** for senior management, internal/external audit, and government regulatory agencies

// **Allows organizations to improve** customer experience and utilize security as a competitive advantage to gain market share



A Well Developed Authentication & Session Protection Stack

- Uses multiple layers.
- Defends against active attacks; such as credential replay and active malware (e.g.session injection).
- Provides remediation methods at login, throughout session, and during critical operations.
- Remediation measures include 2FA, captcha challenges, session termination, static information challenges, customer outreach, transaction holds, etc.
- Logging occurs at every layer for later review, as well as, in sessions replay and analysis software to speed up pattern detection.
- Transaction and authentication risk scoring is derived from past good and bad traffic/transaction patterns.
- Rule sets with complex triggering parameters can be placed into production to route sessions and transactions to any of the remediation measures.

The Fraud Risk Identifier (FRI) provides risk indicators on specific customers based on cyber threat intelligence. The FRI output should be incorporated into Authentication/Session Risk Scoring and Transaction Risk Scoring (both online as presented in this stack and offline). The FRI can also directly feed offline remediation measures outside of authentication and transaction attempts such as customer outreach, recredentialing, rebuilding accounts, etc based upon specific threats and customer sets.

The Cybercrime Ecosystem

Bad Internet Traffic
Malicious Software
Stolen Data
Malicious Marketplaces

Cyber Threat Intelligence (CTI)

Indicators of Compromise (IoC)

Indicators of Financial Compromise (IoFC)

SECURITY INCIDENT & EVENT MANAGEMENT (SIEM)

PREVENTS: NETWORK BREACHES

SPLUNK, AT&T Security, IBM

SERVER | NETWORK | ROUTER | MOBILE DEVICE

ACTIONED BY: INFORMATION SECURITY (CISO)

FRAUD INCIDENT & EVENT MANAGEMENT (FIEM)

PREVENTS: BAD CUSTOMER EXPERIENCE FRAUD EVENTS

CYBER TEAM SIX

CUSTOMER 1
Mobile devices

CUSTOMER 2
Tablets

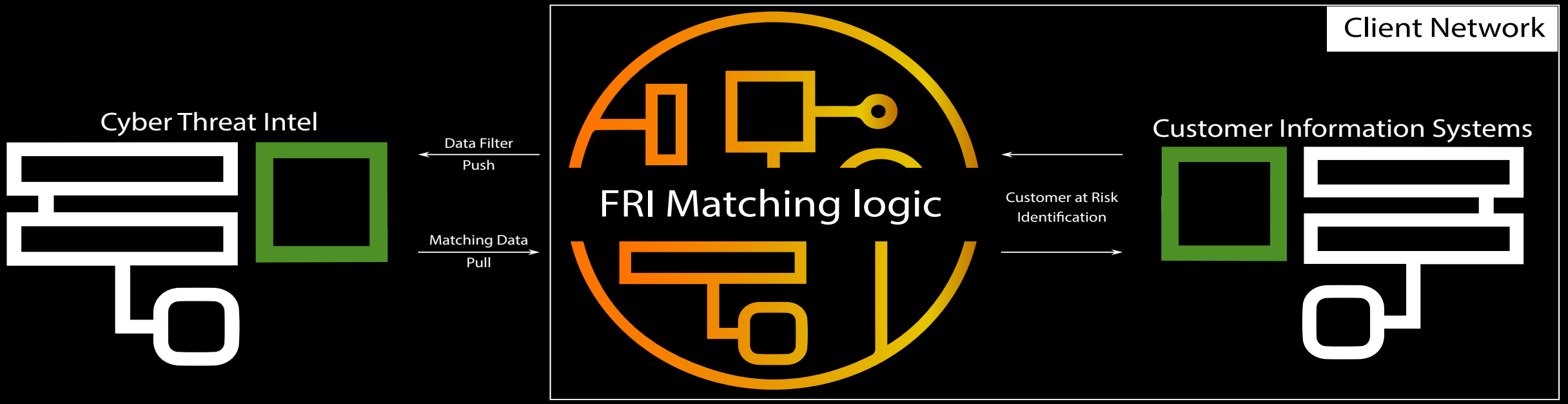
CUSTOMER 3
Laptops

CUSTOMER 4
Desktops

ACTIONED BY: DIGITAL CHANNEL BUSINESS LINES, FRAUD, ANALYTICS & COMPLIANCE TEAMS

Fraud Risk Identifier

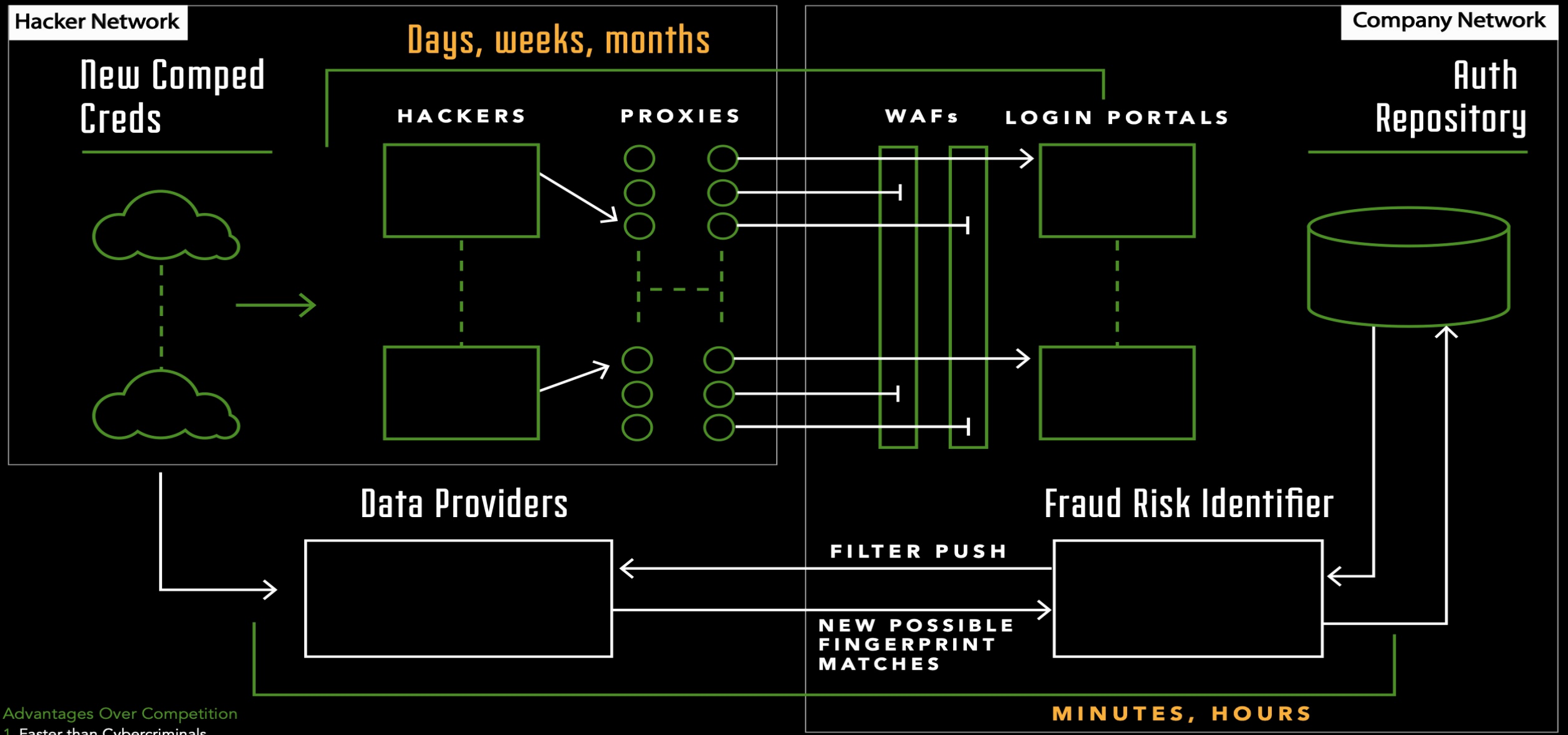
Utilizes external cyber data to identify customers targeted by specific threats like credential replay attacks, malware, darknet, and phishing before customers are victimized.



Advantages Over Competition

1. Complete Data Privacy => No customer information leaves the network only partial data fingerprints for filtering.
2. Quantity and Quality => Large data quantities from many sources and threats giving the best coverage.
3. Frictionless Touch => Doesn't add friction to customer experience as all identification occurs using existing on premises data.

Compromised Credentials Remediation Model



Advantages Over Competition

1. Faster than Cybercriminals
2. Complete Data Privacy
3. Quantity and Quality
4. Frictionless Customer Experience

Market Participants

Threats to Digital Customers	cyber team six	Spycloud	F5/ Shape Security	IBM Trusteer	Actimize	SAS	SPLUNK	Dark Web Monitoring Platforms
Identifies passive malware infected customers	X				X			X
Identifies active malware infected customers	X			X	X			
Identifies malware infected customers compromised when visiting non-company owned domains	X							
Identifies compromised customers before a login event occurs	X							
Blocks credential replay attack automation		X	X	X				
Protects customers from using compromised credentials associated with your brand	X	X	X		X			
Protects customers from re-using credentials compromised in 3rd party data breaches (not your brand)	X	X						X
Protects customers from re-using credentials compromised in old malware campaigns (not your brand)	X	X						
Protects customers from re-using credentials compromised in old phishing campaigns (not your brand)	X		X					
Protects customers from using credentials seen in current credential replay attacks (not your brand)	X*		X					
Identifies customers with payment cards for sale	X				X			X
Identifies customers with online account access for sale	X				X			X
Identifies customers accessed by a fraudster using a malicious IP spoofing service	X							X
Identifies customers likely to have provided information to a phishing website	X*			X				
Matches specific phishing websites and the actors who created them	X							

FRI credential remediation functionalities

* Building with partner

Market Participants

Technology Function	cyber team six	Spycloud	F5/ Shape Security	IBM Trusteer	Actimize	SAS	SPLUNK	Dark Web Monitoring Platforms
Financial transaction risk scoring engine					X			
Online session blocking or risk scoring			X	X	X			
Compromised customer identification engine	X							
Large volume threat intelligence aggregation	X	X						X
Anti-fraud analytics	X				X			
Software analysis tool set						X		
Security Incident Event Management (SIEM) Software							X	
Constantly surveys cyber threat intelligence market for fraud-relevant data upgrades	X							
Creates a platform to operationalize a Fraud Fusion Center	X				X			

Market Participants

Software Features	cyber team six	Spycloud	F5/ Shape Security	IBM Trusteer	Actimize	SAS	SPLUNK	Dark Web Monitoring Platforms
Customer data does not leave the company network	X		X	X	X	X	X	
Customer PII is not published to outside parties	X		X	X	X	X	X	X
Utilizes multiple data collection methodologies	X							X
Unique hashing mechanism to enable privacy and security during data exchange	X							X
Introduces a new step during login resulting in additional customer friction		X	X	X				
Provides investigative leads through attribution to specific fraud events	X							X
Point and click analyst driven link-analysis	X*				X	X	X	
Identifies likely connected cyber enabled customer incidents using unsupervised machine learning (AI)	X*							
Provides cyber point of compromise labeling to build anti-fraud models	X				X			X
Provides data required for compliance reporting	X			X	X	X	X	
Deployable to cloud service	X		X	X	X	unknown	unknown	
Deployable on-premises	X		X	X	X	X	X	
Software as a Service (SaaS)						unknown		
Hosted solution		X	X		X			X
Customize dashboarding to track customer trust metrics and fraud loss risk	X*				X	X	X	
Integrates with existing anti-fraud technology and/or analytical platforms	X	X	X	X	X	X	FRI credential remediation functionalities	

* Building with partner

Thank you!

cyber team six.