Securing Trusted Digital Banking
Effectiveness, Visibility, Security, and Trust

In an era of innovation, scale, and customer-centric enhancement of banking services, a financial institution's growth is dependent on their ability to automate, digitally engage, and provide new levels of AI-led services to its customers. Financial institutions that can "go to where customers are" are better able to generate new revenue models, drive better customer adoption, and increase loyalty.

Reimagine Trusted Banking

In order to drive growth-oriented innovation, financial institutions are in an ever-evolving effort to "reimagine" trusted digital banking. New customer experiences, innovative products, and new channels to markets offer a bold growth enabler for banks, but have to be rolled out with trust, resiliency, and security from design to execution.

Banking (Data) Effectiveness

Banking processes are complex, with sophisticated data models, event ontology, and schemas. The ability to consistently apply risk models across all data improves the effectiveness of a secure bank.

Banking Visibility

A key aspect of enabling trust in banking is end-to-end visibility of risk and threats. Banking processes, supporting applications, and processing gateways are often complex, typically not fully documented, and in many instances have complex data models.

Banking Security

Digital transformation within financial institutions drives business growth and acceleration. Success depends on aligning people, process, and technology to secure the digital supply chain.

Banking Trust

Trust is a key aspect for driving business growth objectives, customer experiences, and the rollout of digital banking services. Financial services organizations need to build a comprehensive cyber resiliency program from visibility to data protection in order to secure the value chain, drive end-to-end visibility, and enable institutional digital trust.

Financial services customers are becoming increasingly dependent on digital banking channels for their ongoing banking, investment, and financial needs. In an era of tech-savvy buyers, banking customers are much more comfortable conducting their transactions through mobile platforms, which is accelerating the digital transformation of banking. Innovations such as blockchain (DLT), machine learning, and deep learning increase the ability of the modern digital bank to expand services and deliver unique (differentiated) services to customers.

Banking (Data) Effectiveness

Securing the banking value chain (the entire flow of processes through the various lines of business) requires accurate analysis, use of machine learning, and cognitive for enabling advanced cross-channel cybercrime and financial fusion threat analysis. Security data lakes can easily become "data swamps" if the data that is injected into these repositories are not consistently modeled and processed. For example, machine learning models require consistent analysis of behavior, whether the log generator is an automated teller machine (ATM) or a payment processor. If the data is not processed consistently, the machine learning model will not be able to "stich together" activity from disparate banking processes that could be affected by a coordinated adversary.

Banking applications, fraud systems, and even traditional mainframe processors generate complex, multi-line, and esoteric data models for event schema. In most

instances, the message schemas are in binary and XML format, making it difficult to consistently parse, enhance, and add meta-data to the event schema. This limits the effectiveness of "fusion" (systems that fuse banking data across diverse processes, departments, and channels) risk and threat models, driving higher risk and lower effectiveness of a fusion center.

The CyberRes digital transformation is designed to provide one of the most mature and flexible models for addressing banking data complexities.

Banking Visibility

Securing the value chain for financial services is a complex, diverse, and expansive challenge. Banks must deal with a unique risk surface, from retail banking risk to account takeover at the edge. CyberRes Trusted Digital Banking offerings have an extended, integrated ecosystem structure that provides

a comprehensive solution to secure the entire banking digital value chain—from retail banking, online, foreign exchange, payment, and other functions within the financial services value chain. This means better trust, security, and resiliency.

The CyberRes Security Operations portfolio is designed to provide end-to-end visibility through the banking value chain.

Banking Security

Digital transformation is a strategic instrument for driving enterprise growth and market acceleration. Successful application of cyber resiliency to enable digital transformation requires technology, people, and process to align to the nuances of the business value chain. That is the ability to understand the goal for the specific digital transformation initiative and then align with those goals. The CyberRes offerings are designed to address the nuances of digital transformation specific

to the industry value chain, processes, and workflow. Our solutions include a holistic, solution-based view of empowering digital transformation through the precision of each industry solution.

CyberRes Adaptive Authentication and Application Security provides end-to-end security through the digital supply chain.
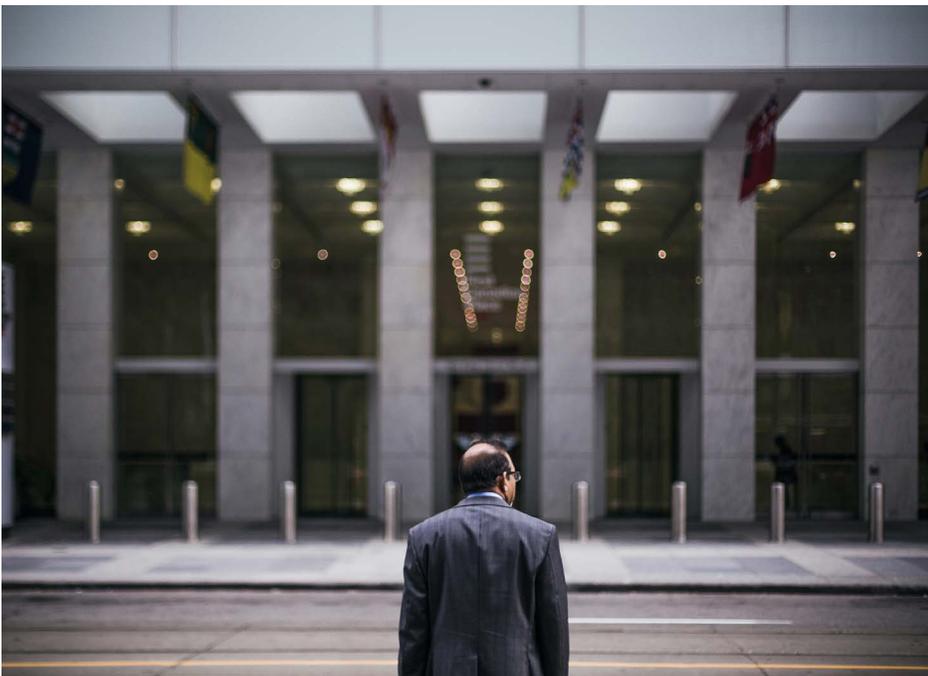
Banking Trust

Digital banking provides a limitless vision for financial institutions to create new markets, open a new customer base, and deliver unique services. This includes the use of artificial intelligence, cognitive, voice assistants, and smarter banking chatbots to provide "just-in-time" insights. For example, customers with sight limitations can use banking voice assistants to provide instant access to the key highlights of their spending account. As banks expand their digital platforms to provide new products and services, the complexity of data flow and access governance expands.

CyberRes Trusted Digital Banking provides a lifecycle-based, holistic solution that protects customer experiences from how data enters the value chain to how it is used with digital platforms. This helps drive visibility and trust to enable customer adoption.

CyberRes Capabilities for Securing Trusted Digital Banking

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world's largest security portfolios to help our customers navigate the changing threat landscape by driving both cyber and business resiliency within their teams and organizations. We are here to help enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility.

We are part of a larger set of digital transformation solutions that fight adverse

conditions so businesses can continue to run today to keep the lights on and transform to grow and take advantage of tomorrow's opportunities. CyberRes offers a host of capabilities for securing trusted digital banking.

Banking Cyber Data Platform

The CyberRes Data Platform provides a sophisticated, flexible, and scalable data platform that enables financial services to enhance their ingested events, logs, and other metadata. This includes a robust platform for parsing, normalization, and metadata enhancement. The platform is built on common industry-based standards that can be used in a provider/consumer architecture to drive better adoption and standardization.

Banking Fusion Operations

CyberRes Security (Fusion) Operations solutions for financial services provide a next-generation fusion detection and anomaly detection capability. The solution provides an integrated framework to enable shared data experience with a holistic fusion center platform—from machine learning to advanced threat detection, automation, and workflow. This extends from information, financial crime, and physical to integrated banking processing systems.

Banking Secure Development

At the core of banking modernization is the trust, integrity, and survivability of the microservices, banking application, and (in modern environments) infrastructure as code.

The CyberRes Secure Development portfolio enables financial institutions to shift left by moving security earlier in the software development lifecycle, which is the most efficient means of engineering secure applications. However, the velocity of development can make this a daunting task. Integrating security intelligence into development pipelines optimizes the power

of automation for agility, speed, innovation, and delivery to efficiently identify software risks, enforce policies, and remediate any found vulnerabilities.

Banking Secure Supply Chain

Banking applications have complex dependencies with upstream and downstream systems, repositories, NetBeans, and other dependent code farms.

Modern banking applications, like apps in other sectors, are subject to open source security issues. And since most organizations have implemented hundreds of open source solutions, CyberRes' Open-Source Scanning tools put a spotlight on general security risks associated with open source components. Susceptibility analysis enables banks to automate the workflow to determine if open source weaknesses can affect the banking value chain.

Banking Data Classification

A key aspect of addressing banking processes is to know your customer (KYC).

A core component of KYC is to trace and classify customer data through complex processing environments. CyberRes Voltage File Analysis Suite Data Discovery uses AI-driven analytics to build a rich inventory of data. CyberRes Voltage Structured Data Manager automatically discovers sensitive data across all repositories and acts on it to reduce the data footprint and lower TCO.

Banking Data Protection

Financial institutions today are hybrid IT and multi-cloud and need protection for high-value data that travels with the data. CyberRes Voltage encryption techniques encrypt or anonymize data in files, databases, applications, and analytics platforms so that business workflows continue to operate and data maintains usability and utility in its protected form. Yet, when exfiltrated, the encrypted data is useless to the cyberattacker. Voltage thus neutralizes the impacts of data breach ("safe breach"). Persistent data security enables privacy and safely increases data use to drive value for the business.

> "ESM reveals security events to us that we were never able to detect before. We're very happy with ESM and confident we can find threats before they compromise our network or disrupt business. ArcSight provides critical insurance against the damage modern cyberattacks can inflict on an organization."

MARK BEERENDS
Head of Security Operations Center
Rabobank

CyberRes

Contact us at **CyberRes.com**
Like what you read? Share it.

Banking Secure J2C

In order to drive on-demand and elastic banking services, financial institutions are accelerating their migration to the cloud in a secure manner. CyberRes Data provides insight into customer behavior, trends, and opportunities for new products and services that support Secure Journey to Cloud (SJ2C).

CyberRes Voltage Format-Preserving Encryption seamlessly integrates with big data analytics platforms on premises, in the cloud, and in cloud-native services to enable secure analytics on data in its protected form. Analytics teams, DBAs, and business users can safely access high-value data, perform most analytics on encrypted data, and produce faster insights and time to value.

Banking Secure Identity

Financial institutions are encountering an ever-expanding banking agent and employee landscape. With the increase in teleworkers, institutions are addressing the complexity of third-party labor providers, work-from-home risks, and other challenges.

CyberRes Identity Governance provides banks with a lifecycle-based, analytical, and machine learning-aided set of capabilities to provide visibility and control of roles, agent access, and certification of tellers and other bank employees.

Learn more at
cyberres.com/industry/financial

CyberRes
A Micro Focus line of business