Krontech

# Krontech Protects Finance Organizations Against Cyberattacks and Helps Them with Regulatory Compliance

The Covid-19 pandemic, natural disasters, the increasing wave of poverty, interest rate changes, and other factors leading to an unstable economy have contributed to the rising global cybercriminal activities. Yet, the truth is, even after the dust settles down, finance firms will still be among the top targeted organizations by cybercrime because attackers choose their targets to maximize impact and profit.

According to a report from the Boston Consulting Group (BCG), finance organizations are 300 times more likely to be targeted than other companies, and they fail to respond to these constant threats because cybersecurity is not emphasized strongly enough in the top ranks of these companies. The report also indicates that finance organizations primarily focus on preventing such attacks, and fail to guide their employees and partners in case of a security breach. IBM's 2021 X-Force Threat Intelligence Index report makes a similar argument, and shows that "for the fifth year in a row, the finance and insurance industry was the most attacked industry, underscoring the significant interest threat actors have in these organizations." The report also points out that in 2020, 28% of attacks on finance and insurance were server access attacks, and 10% were ransomware.

In recent years, the best known top data breaches in the Finance Sector are:

Experian, Equifax, Heartland Payment Systems, Capital One, First American Financial Corp., JP Morgan Chase, Desjardins, Westpac Banking Corporation, UpGuard Protects Financial Services. Millions of customers were affected by these breaches, and millions of financial records were stolen. The estimated cost of each breach is around $10 million to $100 million

Further statistics to the economic effects of these breaches are as follows:

Cyberattacks on banks in 2020 and beyond will result in them losing $347 billion. Insurers will lose $305 billion, and capital markets will lose $47 billion by 2024. (Accenture https://www.accenture.com/us-en/insights/financial-services/cost-cybercrime-study-financial-services )

- Financial services cyberattacks in 2020 resulting from data breaches cost organizations an average of $3.86 million, and took an average of 207 days to identify. (IBM https://www.ibm.com/security/data-breach )
- 86% of breaches in 2020 were financially motivated. (Verizon https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf )
- 36 billion records were exposed by data breaches in the first half of 2020. (RiskBased Security https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf)
- Due to the increasing number of cyberattacks on the financial sector, 70% of financial organizations rank cybersecurity as their biggest concern. (Conference of State Bank Supervisors https://www.csbs.org/newsroom/community-banker-concerns-shift-funding )

There are several sub-sectors under the Finance Sector, including Commercial Banks, Investment Banks, Insurance Companies, Brokerage Firms, Payment and Credit Card Companies, e-Payment Companies - all of which are looking for solutions to protect themselves against cyberattacks. With that said, several aspects of improving the cybersecurity posture include:

- Data protection of customer's sensitive information
- Protecting privileged accounts against internal/external attackers
- Protecting data/systems/applications to prevent access by bad actors
- Protecting financial records to avoid fraudulent activities
- Threat detection and prevention

## Information Security Compliance Regulations Related to the Finance Sector

### GDPR (General Data Protection Regulation)

General Data Protection and Law is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

### MAS-TRM (Monetary Authority of Singapore-Technology Risk Management)

MAS-TRM addresses technology risk management, including raising cybersecurity standards and strengthening cyber resilience in the financial sector.

### PCI-DSS (Payment Card Industry Data Security Standard)

The PCI Data Security Standards help protect the safety of payment card data. They aim to protect organizations and their customers against payment card fraud, and are comprised of 12 requirements or control objectives that comprehensively protect the payments ecosystem. They set the operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.

### CCPA (California Consumer Privacy Act)

The CCPA of 2018 (CCPA) gives consumers more control over the personal information businesses collect about them, and the CCPA regulations provide guidance on how to implement the law.

### SOX (Sarbanes Oxley)

SOX compliance refers to the annual audit in which a public company is obligated to provide proof of accurate, data-secured financial reporting. The  basics of SOX Compliance include:

- Keeping data secure and tamper-proof
- Track attempted security breaches and resolutions
- Keep event logs available for auditing
- Prove compliance for the past 90 days at least

## Finance Sector Use Cases

Krontech's Single Connect helps financial organizations often with the following eight use cases.

# CORE PAM USE CASES

**Protecting Privileged Accounts & Credentials Against Credential Theft**

**Preventing Credential Exposure and Building Zero Trust Access Management**

**Building Flexible and Smart Secure Trust Mechanisms for Safe Authentication and Authorization**

**Secure Password Management for Applications**

**Auditing and Regulatory Compliance**

**Rapid Integration with Accelerated DevOps Transformation (On-Premise or Hybrid-Cloud)**

**Improving Security Without Reducing Operations Effectiveness**

**Detecting Suspicious Activity, Eliminating Internal and External Threats**

# Protecting Privileged Accounts & Credentials Against Credential Theft

## Protect Privileged Accounts, Create Strong Credentials, Change Them Often and Automatically

Researchers say that a privileged account has been compromised in 81% of cybersecurity attacks.

## Store Credentials in an Encrypted Vault

Protecting privileged accounts' credentials and authorizations (password, tokens, SSH keys, certificates) is the most critical step. Companies must keep these accounts and credentials in the safest vaults compliant with FIPS 140-2, discover these accounts automatically, and control and record all access to these accounts.

## Change Credentials Regularly

Companies need a system to change credentials often and automatically, and there should be no interruptions in the system whatsoever.

## Create Complex Credentials

The new passwords should be created based on complex password rules.

## Don't Share Passwords

Companies should prevent employees from passing around their passwords, so that the responsible user is traceable when an issue arises.

# Solution

## Single Connect Secret Manager

Krontech's PAM platform Single Connect automatically discovers accounts in systems, applications, script files, and databases, and adds them to the vault after changing their passwords. After that, accounts are accessible only through Single Connect's Secret Manager, which allows companies to:

- Define who can access these accounts directly
- Configure one or two-level approval mechanisms to control access to these accounts
- Split the account password between two users
- Define the above rules and processes on a user group basis, or synchronize with AD to operate the processes automatically

The Secret Manager provides ready-to-use and comprehensive protocols, application, and database support. Single Connect's Secret Manager manages and rotates millions of accounts and passwords in a scalable architecture with high availability.

# Preventing Credential Exposure and Building Zero Trust Access Management

The finance sector organizations lack a central access control point for critical systems, applications on-premise, and cloud. They have hundreds of privileged users connecting to thousands of systems/applications on on-premise or hybrid cloud environments. These users are granted more privileges than needed, and there is minimal, if any, accountability for privileged accounts.

Third-party suppliers can access mission-critical systems in a trust relationship, without invisibility or control by the organization's admins. Outstanding privileges on the systems/applications increase the attack surface for bad actors. In some cases, even well-intentioned internal actors and third-party vendors may cause systems problems and disruptions due to the misuse of these outstanding privileges. The Privileged Access Management System should control and manage the least privileged principle to keep this ecosystem safe and secure from harmful activities.

## Solution

### Single Connect Session Manager

The Single Connect Session Manager secures access, controls commands and activities during the session, and records all privileged activities indisputably.

Single Connect's Session Manager isolates critical target systems from privileged users. Its agentless, man-in-the-middle approach eliminates the need for software agents to be deployed on target systems or user computers.

The Single Connect Session Manager provides the widest set of protocol support (CLI, RDP, HTTP, SFTP, SQL), allowing organizations to

- Implement live session watching and dual control options
- Enable personal accountability and provide VCR-like replay of sessions
- Report and/or prevent unwanted user behavior
- Prevent Credential Exposure
- Enable SSO - no one needs to know system credentials; the privileged users log in with personal AD credentials and can go about their daily tasks

# Building Flexible and Smart Secure Trust Mechanisms for Safe Authentication and Authorization

Organizations must ensure that privileged accounts are used for legitimate business purposes because in the wrong hands they can be used for malicious activities. In today's complex digitalized world and under remote working conditions, it is essential to check and verify the following to govern and manage all access securely:
a) who accesses where in which conditions and for what purposes
b) who is accountable
c) who are the participants

The Zero Trust Policy suggests that companies shouldn't trust anybody and must verify all activities and users. The extent of user authorization should strictly be limited to the scope of current tasks - no more, no less - and the granted permissions should be removed at the end of the access time. A Zero Trust Policy approach protects companies from malicious internal actors and prevents attacks from external actors - even if an external actor obtains the information of internal actors, they won't have the authority to perform activities in systems/applications.

Such policies look great on paper. However, putting these policies into practice, building a governance model, granting, restricting, and monitoring rights within the frame of approval management is another story. Building and maintaining a framework on such policies shouldn't be a burden to a company, and it shouldn't require any other solution other than a single PAM product. Companies should be able to easily update these mechanisms with configurations based on their business needs.

## Solutions

### Built-in MFA Module

Krontech's PAM platform Single Connect has a built-in MFA module. This module is part of the PAM solution and integrated with all business processes. Companies may prefer MFA authentication on several steps.

If a company readily uses a separate MFA application, it can be integrated with the Single Connect built-in MFA module. The company can continue working with the same features without needing any other integration.

### Approval Management

Krontech's Single Connect offers a PAM solution fully-compatible with Zero Trust Privilege Management principles.

- In the absence of outstanding privileges, when human or non-human entities attempt to perform a task or access a device, approving managers receive their requests.
- Users are granted access only if their managers approve, and approving managers can also revoke their approvals.
- Users can make instant or future-dated reservations to access devices.
- After the approved date and time expires, Single Connect removes the user privileges.

### Flexible Multi-Level Approvals

Approval mechanisms are configurable and can include more than one step. Krontech's Single Connect helps companies determine the approval mechanism they need based on their business processes.

### ITSM Integration (Ticket Validation)

Single Connect features integration with ITSM Systems to verify if there is an approved ticket to perform this privileged activity.

### Multi-Channel Support

Single Connect offers users an approval management experience on Web GUI, SMS, e-mail, and mobile app.

# Secure Password Management for Applications

In today's digital world, the finance sector demands collaboration with diverse technological infrastructures to fulfill increasing market requirements: legacy applications, core banking applications, credit and debit card applications operating 7/24, online transaction centers, mobile banking, payment applications, money transfer applications (Swift, EFT, etc.) integrated with other domestic and international finance companies, and so on.

All these applications require access to critical data (passwords, tokens, certificates, credentials). Most applications and scripts have embedded credentials used to access other servers, systems, and databases, which are also visible to users and not changed regularly. Hence this structure increases the attack surface, allowing hackers to leak to other systems once they compromise the embedded credential in an application.

## Eliminating Embedded Credentials

Credentials should be removed from the applications/scripts to reduce the attack surface. These credentials should be stored in an encrypted vault and rotated regularly.

The new solution should also be fast to integrate with the organization's application stack, and must support different applications. Fast and smooth integration is vital, as is uninterrupted service for 7/24 under an immense load with a solid backup procedure. In the event of a network outage (when the vault cannot be accessed), applications should be accessible with credentials provided by the local password vaults.

# Solution

## Application-to-Application Password Manager (AAPM)

Krontech's Single Connect eliminates embedded credentials by providing them on-demand to applications and scripts, therefore making those credentials invisible to users.

Single Connect's Application-to-Application Password Manager (AAPM) works efficiently with the Single Connect Secret Manager. Single Connect's AAPM offers an easy-to-use interface and fast integration alternatives, and meets integration needs for different technological applications with a single product.

The AAPM module provides SDK support for restful APIs and different programming languages, and offers customers different security levels based on the criticality of their applications.

# Auditing and Regulatory Compliance

The financial sector is subject to stringent regulations that differ by region. Some of them are PCI-DSS, Sarbanes-Oxley (SOX), GDPR, CCPA, and the list goes on. These regulations govern data protection, data security, data storage and confidentiality, and tamper-proof audit and recording of all access.

Companies need solutions that respond to regulation changes fast and efficiently. They also need to monitor compliance ratios regularly because ensuring compliance with regulations requires effort and time.

## Auditing

In addition to the in-house audit teams, finance organizations are regularly inspected by the government and independent institutions due to the regulations they are obliged to comply with.

Companies need to coordinate audit activities, schedule the tasks to distribute heavy workload to team members effectively, and manage the process while avoiding financial penalties.

They must be able to report all activities and answer who, what, where, and when questions with tamper-proof audit reports over a single system.

## Data Privacy and Data Protection

Being compliant with PCI-DSS and GDPR requires discovering sensitive data in systems/applications, defining business rules, and building a governance model for this system. The objective is to determine who can access this data, as well as how to store (clear/encrypted), archive and destroy the data, how to store the access logs safely, and how to improve the organization's response time without requiring extra manual effort to comply with audit requirements. To put it mildly, building and managing such a system can be difficult and time-consuming for operation teams.

Keeping the audit logs safe, secure, and unmodifiable against ill-intentioned actors is important to building trust. More than that, it is an obligation, especially if the organization opens itself to any public stock exchange or public audits. The organization needs to build a system for keeping these logs secure in a tamper-proof environment, and this system must guarantee that nobody can change/delete the logs.

## Solution

Krontech's PAM solution Single Connect PAM solution helps companies with compliance challenges.

### Effective and Effortless Response to Audit Queries with Smart Dashboards and Ready-to-Use Reports

Companies can easily track and report their compliance ratios from the Single Connect dashboard. Krontech's PAM solution features comprehensive ready-to-use reports, allowing companies to report all user activities, such as time and owner of all approvals, access time, and other details, including malicious attempts and violations. Companies can easily export reports to print or PDF format. The scheduling and distribution mechanism enables the organization to make these reports accessible to all audiences, without logging in to Single Connect.

### Discovering Sensitive Data

Single Connect can discover sensitive data in all of the organization's databases: financial data, customer address, tax ID, social security number, credit card number, etc., all of which are subject to the GDPR, CCPA, and PCI-DSS regulations. Once discovered by Single Connect, it protects this data, and all access requests (including DBAs, system admins, developers) are logged by Single Connect. Single Connect also manages and, if necessary, restricts access from its central PAM platform.

### Masking Sensitive Data (Dynamic Data Masking)

Dynamic Data Masking ensures that sensitive data is masked when a non-legitimate user accesses the data. Only legitimate users can access the data in cleartext. Both human and non-human entities are considered in this context.

### Keeping the Logs Tamper-Proof (Safe and Secure)

Single Connect stores the logs (authentication, authorization, activity logs, session logs, command logs, etc.) as tamper-proof. Using encryption techniques, Single Connect guarantees no one can change these logs.

## Rapid Integration with Accelerated DevOps Transformation (On-Premise or Hybrid-Cloud)

Increasingly more finance organizations are adopting DevOps practices, and DevOps transformation requires privileged access to critical sources. When working on hybrid cloud systems, new sources are created and removed continuously, which increases the surface and risk of security attacks. Organizations need not only a solution to protect themselves from such attacks, but they also need PAM providers to walk with them the whole way through.

Financial organizations often consider using hybrid cloud vendors to put their apples in separate baskets and become more agile and gain a competitive advantage.

## Solution

Krontech's PAM solution Single Connect helps organizations implement minimum access policies by controlling DevOps resources. Privileged users can access and limit what they are authorized to do with these features, based on their roles and tasks. Single Connect provides ready-to-use plug-ins for the most used DevOps platforms.

Single Connect protects the target endpoints whether they reside in private or public clouds. Single Connect also supports organizations on their multi-cloud implementation, such as AWS, Azure, and Google Cloud.

## Improving Security Without Reducing Operations Effectiveness

The finance sector races to keep up with the rapidly changing digital world and the pandemic circumstances, comply with the changing and new regulations, expand on security threats, and audit needs, and meet other business requirements associated with the globalization of the finance world, including the digitalization of money. Finding a solution to cover all these needs is as significant as it is tricky.

Companies need a comprehensive PAM solution that is fully compatible and integrated with their environments, without requiring extra work or additional licenses (all-in-one). They need to be able to work within their whole ecosystem – ticketing systems, SIEM, MFA, AD, IDM, IGA – at a plug-and-play level. This solution should discover privileged accounts, devices, and databases automatically.

The Single Connect PAM platform detects accounts and devices in on-premise and cloud environments, and onboards them with advanced discovery functions. Single Connect is a holistic PAM solution in which all modules are integrated: a single product that meets customers' PAM needs fully without the need for another product. The fastest to deploy, Single Connect ensures that companies implement PAM best practices at once. Single Connect also features ready-to-use integrations with applications in the ecosystem: ITSM, SIEM, Directory Services, CMDB Systems, IDM, IGA Systems, Analytics Systems, and more.

## Detecting Suspicious Activity, Eliminating Internal and External Threats

Companies need a PAM solution not only as a measure of prevention but as a means to detect suspicious activities. To protect themselves against complex cyberattacks, companies must protect and control all accounts and access.

- Governance of privileged account access and restriction of authorizations under the least privilege principle
- Control of all access with zero trust privilege management processes
- Solutions to increase authentication security (MFA, biometric authentication)

More importantly, companies need business partners to guide them in finding what they need, decide on the right solution, and apply cybersecurity practices on a day-to-day basis.

## Solution

Single Connect's Privileged Threat Analytics and Response module runs integrated within its PAM platform. This module runs a multidimensional real-time User, Session, Target EndPoint analysis. It detects credential theft, abnormal behaviors, unusual command executions, irregular access, and direct login attempts that bypass existing PAM servers. The Threat Analytics and Response module acts automatically on the results and responds to the threats based on the severity of the threat.

# Why Krontech?

## Business Benefits

- Full visibility and full control are achieved without compromising operational efficiency
- Network Automation for Security - Automation increases security while maintaining organizational agility
- Integrated User Behavior (UBA) Analytics & OCR
- Enforce security policies transparently
- Manage and record every user activity
- Centralized - Unified visibility and management of all privileged sessions
- Enforce role-based access controls centrally and silently
- Shared Account Password Management
- Compliancy with regulations, internal operations auditing, and screening
- Scalable - Supports tens of thousands of endpoints with a standard server
- Isolation of critical target systems from the user network
- Agentless - No agent software on endpoints
- Seamless - Admins continue to use their native client apps
- Transparent - Enforces security policies transparently
- Real-Time Prevention - Prevent malicious activities before they occur
- Comprehensive - Industry's widest support range for protocols
- Fastest to deploy - Fastest to deploy PAM solution available in the market
- Modular - Ready to add modules for your future needs
- After-the-Fact Records - Indisputable indexed logging and session recording
- Cloud - Supports Cloud platforms
- Least Privilege - Best-in-class, real-time, least privilege management
- Accountability - Enables accountability and records for investigations
- Segregation of duties & Least privilege functions, including command or application-based restrictions, managerial approval, geo-location confirmation, time & date-based access
- Password Management - Eliminates password sharing and strengthens credentials
- Security - Securely stores passwords in a vault

## About Krontech

Featuring innovative approaches needed to achieve the digital transformation goals for infrastructure, operations, and security issues which have become the most current matters for all organizations today, Krontech offers its products and services in all global markets to those who need them. Increased its locations across the globalized world, in line with its objective of being close to its customers, to better understand them and supplying its services on a timely manner, Krontech currently carries on its activities with its offices in New Jersey, Istanbul, Ankara, and Izmir.

Being a high-technology company, Krontech consists of competent engineers and researchers respected in their fields, and united under the values of team spirit, innovation, curiosity, communication, passion, courage, sincerity, and anti-discrimination, within an unlayered organizational structure. The company has strategically determined that its human assets have the top priority value in the global race for developing new-generation technologies, and carries out successful projects in a free environment.

Trying to achieve a perfect balance among swiftness, reliability, flexibility, agility, sustainability, and quality in its activities, Krontech offers its high-technology, high-quality, and reliable products to its customers. Growing its workforce consistently by continuously analyzing sector dynamics in-depth, and without compromising on innovation, Krontech progresses swiftly towards becoming a global technology producer.

# Gartner Recognizes Krontech as a Niche Player in 2021

## What Does the Gartner Magic Quadrant 2021 Report Say About Krontech?

### Rapid Response Ability

“Good support for the majority of common service account management use cases and high performance for bulk credential rotation, such as when all credentials need to be changed rapidly in response to a breach.”

### SQL Filtering and Data-Masking Controls

“Database controls: Krontech goes further than other PAM vendors by supporting extensive SQL filtering and data-masking controls for monitoring and controlling privileged database access.”

### Scalability

“Krontech is well-positioned for large, heterogeneous environments, such as those of telcos, and has a highly scalable architecture that supports massively parallel credential rotation.”

## Resources:


*Cost of Data Breach Report.* 2020, July. IBM Security.
https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf,
*Data Breach Investigations Report*. 2020. Verizon.
https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf,
*2020 Q3 Report Data Breach Quickview.* 2020. Risk Based Security.
https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf,
Community Banker Concerns Shift to Funding. 2019, Oct 1. CSBS.
https://www.csbs.org/newsroom/community-banker-concerns-shift-funding
*Kost, E.  2022, Feb 03. The 8 Biggest Data Breaches in Financial Services (2021 Edition).* UpGuard.
https://www.upguard.com/blog/biggest-data-breaches-financial-services,
Krishna, D. 2017. *The Future of Regulatory Productivity, powered by RegTech.* Deloitte.
https://www2.deloitte.com/us/en/pages/regulatory/articles/cost-of-compliance-regulatory-productivity.html
*What is MAS-TRM?* 2021, Jun 28. Panorays.
https://panorays.com/blog/what-is-mas-trm/
*Is Your Organization SOX Compliant for 2022?* 2022, Feb 15. Sarbanes Oxley.
https://www.sarbanes-oxley-101.com/
*What is SOX Compliance?* 2019, May 28. DNSstuff.
https://www.dnsstuff.com/what-is-sox-compliance
De Groot, J. 2021, Aug 12. *What is PCI Compliance?* Data Insider.
https://digitalguardian.com/blog/what-pci-compliance
Wolford, B. (n.d). *What is GDPR, the EU’s new data protection law?* GDPR.EU. Retrieved Feb 15, 2022 from
https://gdpr.eu/what-is-gdpr/
Thompson, C. 2019, July 15. *What will cybercrime cost your financial firm?* Accenture.
https://www.accenture.com/us-en/insights/financial-services/cost-cybercrime-study-financial-services