CYBERARK®

SOLUTION BRIEF

PRIVILEGED ACCESS SECURITY PROTECTS THE BUSINESS OF INSURANCE

Opportunities and Challenges

With penetration at a record low in the Life and Annuities market presents opportunities. "However, to accelerate growth, L&A insurers should consider simplifying their products and streamlining their application process to make policies easier to understand , underwrite, and purchase....In fact, unless the industry commits to integrating transformative technologies more rapidly into their operations, L&A companies could risk not only continued stagnation, but potential leakage to InsurTech innovators as well."

Source: 2018 Insurance Outlook Shifting strategies to compete in a cutting-edge future

Safeguarding Customer Information and Digital Innovation

Insurance executives face tough decisions stemming from changing customer needs, volatility in a crowded marketplace and accelerating digital innovation. The secure stewardship of increasing amounts of valuable digital data will be critical to remain competitive, protect revenues and achieve growth.

Even though the rate of decline is slowing, global insurance renewal rates fell for the 17th consecutive quarter in the second quarter of 2017.[1]

At the same time, insurance is more dynamic than ever. The increasing collection, analysis and application of digital personally identifiable information (PII) is changing traditional insurance models, spurring broader ecosystems – and new competition. Insurance organizations face new disruptions throughout their multi-channel business model, involving their relationships with consumers, brokers and reinsurance partners.

Greater digital maturity, including adopting DevOps processes and leveraging cloud deployments, opens revenue opportunities for the forward-looking insurance business. The more effectively insurers adapt to the new digital reality, the more they will differentiate themselves and remain competitive. "The value at stake from achieving a digital transformation is becoming increasingly clear—we know that property-casualty insurers in the top quartile for digital performance are growing twice as fast and are achieving higher profitability than their less digitally mature peers." [2]

Securing privileged access is critical to protecting customer data and ensuring a successful and secure transformation. Privileged access is meant to elevate, but strictly control access to systems that hold customer as well as sensitive and valuable organizational information. Privileged access can be compromised by external criminals, and malicious or negligent employees.

In fact, privileged access represent the keys to an insurers' IT kingdom. Strong privileged access security is key to protect differentiation and capitalize on new opportunities with confidence, without jeopardizing regulatory compliance or damaging the brand due to a security breach.

CyberArk is the recognized leader in protecting privileged access; and is used by 21 of the top 25 financial organizations worldwide. The CyberArk Privileged Access Security Solution automatically protects privileged account credentials, easily accommodating new applications and broader digital ecosystems. Only CyberArk has the history, experience and resources to secure privileged credentials across on-premise, hybrid and cloud systems, so you can effectively leverage the digital innovations key to success.

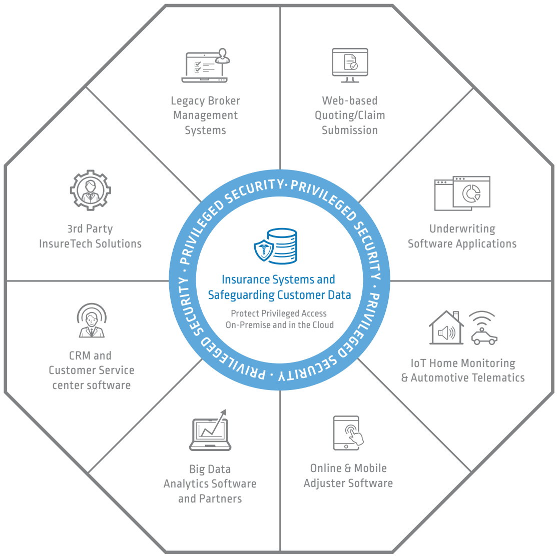
[1] Global Insurance Market Index – Q2 2017

[2] How insurers can get the most out of a digital transformation in 2018 February 23, 2018 – by Tanguy Catlin, Johannes-Tobias Lorenz, and Shannon Varney)

The Heightened Role of Privileged Access

Expanded ecosystems with vendors and partners that include connected on-premises, hybrid and cloud systems also encompass more privileged users and applications. According to the 2017 SANS Data Protection Survey, "User credentials and privileged accounts represented the most common data types involved in these breaches, spotlighting the fact that access data is prized by attackers. It is just as desirable to them as "sensitive" data being targeted for financial gain or destruction." Furthermore, the second most effective method to protect data on the network is implement proper access controls. The risk is not just external threats. In the 2017 SANS Insider Threat Survey, 49% of respondents cited concerns about compromise (by insiders) of privileged access information, including credentials.

"As the banks have tightened up their security and there's less opportunity there, [attackers] have found insurance companies, especially healthcare, have a lot of data."… "Privileged user accounts are more vulnerable," says American Family Life Assurance Company (AFLAC) CISO Tim Callahan. "That's what the criminals want."[3]


Legacy Broker Management Systems
Web-based Quoting/Claim Submission
3rd Party InsureTech Solutions
Underwriting Software Applications
PRIVILEGED SECURITY · PRIVILEGED SECURITY · PRIVILEGED SECURITY · PRIVILEGED SECURITY ·
Insurance Systems and Safeguarding Customer Data
Protect Privileged Access On-Premise and in the Cloud
CRM and Customer Service center software
IoT Home Monitoring & Automotive Telematics
Big Data Analytics Software and Partners
Online & Mobile Adjuster Software

Insurers have always been prime targets:

- Nationwide Mutual Insurance Company, 1.27 million consumer records, process and system improvement costs, $5.5m in State penalties, additional lawsuits underway[4]
- In the UK, a malicious insider at the international health insurance division of Bupa Global stole at least 108K records, perhaps as many as 1m, and offered them for sale on the Dark Web[5]

A study of 42 financial services companies across seven countries found the average cost of cybercrime has increased more than 40 percent over the past three years, from US $12.97 million per firm in 2014 to US $18.28 million in 2017. Despite extensive investment and mitigation efforts financial services, including insurers, leads the pack in terms of annualized cost of cybercrime by industry sector: US $18.28 billion; 6% higher than the next sector in line, utilities and energy.[6]

Strong data stewardship is key to achieving – and protecting – the business benefits of digital innovation. Who would choose to buy home insurance from an organization whose personal home information was compromised? What business would buy cyber-insurance from a company that's been hacked?

Called Upon to Do It All – Innovation and Protection

Not only must IT and security professionals keep systems running smoothly and cost-efficiently, they are responsible for protecting the data flowing through them. Security teams already have their hands full with more sophisticated attacks. In a survey of 343 qualified security professionals (including insurers) "51 percent of respondents claimed their organization had a problematic shortage of cybersecurity skills". And worse "70 percent of cybersecurity professionals claimed their organization was impacted by the cybersecurity skills shortage".[7]

Now IT is being called upon to protect expanded, complicated ecosystems supporting valuable new services. Data flowing from Internet of Things (IoT) devices are impacting insurance models from autos to homes. Two real-world examples include:

[3] Aflac CISO: Insurance Sector Ramps Up Cyber Defenses 5/8/2017, Kelly Sheridan, Dark Reading

[4] www.usatoday.com/story/money/2017/08/09/nationwide-mutual-insurance-agrees-5-5-m-settlement-over-data-breach/552687001/

[5] www.theregister.co.uk/2017/07/13/bupa_data_breach/

[6] www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-insurance-2018-outlook.pdf

[7] www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html

- The Vitality program at John Hancock, where policyholders are offered premium savings and rewards for completing health and fitness related activities, tracked by smartphone apps and fitness devices.[8]
- Liberty Mutual is offering discounts to customers who drive Volvos with active or passive advanced safety features, not only to encourage consumer adoption, but also to collect valuable data regarding the impact of these components on accident frequency and severity. By 2020, nearly 100 million drivers are expected to have usage based insurance (UBI) leveraging automatic telematics data.[9]

Such connectivity and applied data analysis can improve service offerings and identify new opportunities. But success will require automating more tasks. Security teams are increasing investments to better automate security functions. One study found that by 2021 spending on more automated fraud analysis and investigation will increase 47 percent, and for threat intelligence and prevention systems by 35 percent.[10]

Across IT the more that can be automated, the more resources are freed to address other issues: like innovation. An effective privileged access security solution has to be as automatic as possible, alleviating repetitive, time-consuming and error-prone "manual" processes. It also has to be adaptable, able to extend easily and quickly to accommodate new applications and third party services.

Digital innovation will continue to make securing privileged access more difficult. Beyond employee credentials, IT and security teams need to get their arms around vendor and contractor access to sensitive systems, as well as more application to application permissions.

New Insurance Ecosystems

"Progressive, for example, partnered with Zubie, a vehicle-tracking and engine-diagnostic device, to give customers visibility into how their driving habits affect their premiums. Nest partnered with Liberty Mutual to help offset the cost of a Nest Protect smoke detector and offer a monthly discount on homeowner's insurance in the United States. Manulife is collaborating with Indico Data Solutions to develop a deep-learning tool that analyzes unstructured financial data."

Source: Insurance beyond digital: The rise of ecosystems and platforms

The agile development of new applications – or modification and integration with existing systems – can introduce risks. Though not an insurance company, Uber developers were working in a private version of GitHub when their development code, containing privileged credentials, was compromised.[11] And as more services are outsourced a/or based in shifting, DevOps environments, securing privileged access end-to-end will become critical.

The Drumbeat of Compliance Obligations

Insurance has long been among the most heavily regulated industries. And legislators are showing no signs of slowing down:

US	23 NYCRR 500, effective March 1, 2017, mandates that insurers must have a CISO. The National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law adopted October, 2017, creates rules for insurers, agents and other licensed entities covering data security, investigation and notification of breach. The Department of Labor (DOL) Fiduciary Duty Rule related to the sale of retirement products. PCI-DSS 3.2 requires multi-factor authentication for safe keeping of payment data.
EU	The General Data Protection Regulation (GDPR) begins May 25th (silver lining might be revenue opportunities for insurers); Insurance Distribution Directive (IDD), replaced Directive 2002/92/EC, the Insurance Mediation Directive (IMD) Feb 23, 2018. European Commission's packaged retail and insurance-based investment products (PRIIPs) documentation, with defined key information documents (KIDs).
Global	International Financial Reporting IFRS17 Insurance Contracts…opened May 2017 and have until January 2021 to implement.

Broader financial regulations also impact insurance: the EU is moving to build a Capital Markets Union (CMU) and the Payment Services Directive 2 (PSD2); MiFID II, enforced by the European Securities and Markets Authority (ESMA), specifically mentions securing customer communication data and providing clear audit trails that include privileged access details.

Maintaining compliance will remain a challenge, but the value of strong privileged access security and management is a constant. New digital processes offer compliance efficiencies and cost savings. Automated and comprehensive protection of privileged credentials can protect existing system investments, and benefit organizations as they innovate.

[8] www.johnhancockinsurance.com/life/John-Hancock-Vitality-Program.aspx

[9] www.libertymutualgroup.com/about-lm/news/news-release-archive/articles/techsafety-insurance-discount

[10] "2018 Insurance Outlook Shifting strategies to compete in a cutting-edge future," Sam Friedman, Michelle Canaan, Deloitte Center for Financial Services, 2017

[11] Beach, David, "What Financial Services Can Learn from the Uber Breach when Preparing for GDPR," GT News, March 08, 2018.

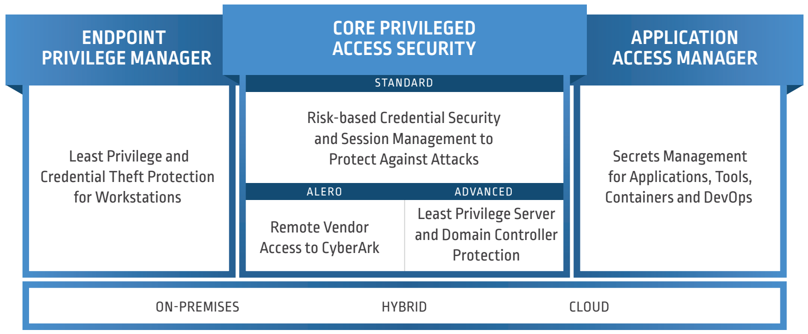
CyberArk Safeguards Insurance Innovation

Strong Privileged Access Security

Retail, commercial and reinsurance organizations require strong privileged access security to protect against growing external and internal threats to personal and proprietary information. CyberArk Privileged Access Security Solution allows the organization to move with greater agility so as to capitalize on new opportunities while protecting the organization against existing and future cyber attacks.

- End-to-end protection of all privileged access across on-premises, cloud, and DevOps environments.
- Only solution that can detect and prevent privileged attacks across on-premise, cloud, and DevOps environments.
- Detection and protection for 1,000,000+ malware variants and advanced attacks (including ransomware) on distributed endpoints with out of the box, comprehensive privilege security policy control.
- Full lifecycle management of both passwords and SSH keys, regardless of whether they are used by interactive users (employees, contractors or vendors) or applications, on-premise or in cloud-based applications.
- Fully hardened for on-premises and cloud deployments with centralized secure storage for privileged credentials, session recordings and secrets in a highly secure isolated vault.
- Mapping between suspicious privileged access activities and corresponding session recordings to proactively identify potential attacks including insider threats to compromise of critical credentials.

CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION


ENDPOINT PRIVILEGE MANAGER
Least Privilege and Credential Theft Protection for Workstations
CORE PRIVILEGED ACCESS SECURITY
STANDARD
Risk-based Credential Security and Session Management to Protect Against Attacks
ALERO
Remote Vendor Access to CyberArk
ADVANCED
Least Privilege Server and Domain Controller Protection
APPLICATION ACCESS MANAGER
Secrets Management for Applications, Tools, Containers and DevOps
ON-PREMISES
HYBRID
CLOUD

Future-Proofing Privileged Access Security

Rapid, secure innovation must be anchored by a comprehensive, time-tested privileged access security solution. Any solution must accommodate new DevOps processes and larger ecosystems that support emerging mobile and IoT applications and infrastructure. A mature solution should not be a series of siloed, unintegrated applications, but complete and cohesive, with a clear well-funded roadmap for future growth. The CyberArk Privileged Access Security Solution is built to accommodate new privileged credentials, whether on premise, cloud-based or in DevOps tools. .

- A comprehensive solution that's extensible and enables interoperability:
  - All functionality built to share common resources, a common UI, organically designed to work well together, including credential management and security, session monitoring, isolation and threat analytics from one platform;
  - Distributed architecture proven to scale in complex environments, including multiple network segments and multi-site deployments;
  - Wide variety of available integrations; with support from 170+ vendors out-of-the-box, with over 200 connectors and plug-ins;
- Time-tested and proven market leader:
  - 21 of the top 25 financial organizations worldwide use CyberArk;
  - 3,800+ customers globally, the greatest number of privileged access customers;
  - Nearly 20 years of experience and a strategic focus on privilege protection: 200+ dedicated R&D engineers dedicated to innovation;
  - Consistently rated as leader by analysts such as Forrester, IDC and KuppingerCole.

Prove Compliance More Easily

To demonstrate their efforts at regulatory compliance, insurance organizations must have documented, auditable proof of their efforts to protect privileged access. CyberArk Privileged Access Security provides rapid access to detailed and comprehensive user session activity, which is increasingly valuable for effective breach notification, and in some cases, avoidance of fines.

- Comprehensive monitoring, recording, and isolation of all privileged user sessions, and activity on any critical database or application —including across the ecosystem.
- Fully searchable audit logs (including meta-data) and DVR-style recordings of all privileged user session activities, including contractors and vendors.
- Full audit trail data protected by the same, hardened vault security as the credentials themselves.

Click here to read Rapid Risk Reduction: A 30-Day Sprint to Protect Privileged Credentials White Paper

Proactive and Automated to Enable IT

To respond to threats rapidly and free IT to focus on the digital innovations that strengthen customer loyalty and capture new sources of revenue, privileged access security must be as proactive and automatic as possible. The CyberArk Privileged Access Security Solution is the only solution to analyze end-to-end, privileged user and account behavior to detect, alert and respond to critical credential threats. Real-time session monitoring enables rapid detection of abnormal activity and remote termination of sessions to disrupt potential privileged access security attacks.

- Protect freedom to innovate and save time and money with CyberArk automated detection and protection:
  - End-to-end automation of privileged access security tasks across the insurance ecosystem;
  - Domain Controllers are prime targets, e.g. Kerberos attacks compromising authentication in Windows domains. Detect malicious activity on Domain Controllers in real-time;
  - Thwart attacks in real-time by automatic suspension or termination of privileged sessions based on risk analysis.
- CyberArk helps IT stays in control while maintaining productivity:
  - Enforces least privilege policies yet enables users to elevate privileges when needed for business purposes – in accordance with policies – strengthening security while keeping IT users productive;
  - Reduces risk by removing local admin rights while keeping users productive and limiting IT support costs;
- Leverage a deep bench of CyberArk privileged access security expertise:
  - CyberArk Services help expedite the development of a best practices privileged access security program by providing the expertise and experience where and when needed;
  - 500+ Trained CyberArk Delivery Engineers at CyberArk and leading system integrators.

Getting Started Fast

To help you get started building a best practices privileged access security program, CyberArk recommends that you:

- Run a cost-free CyberArk Discovery & Audit (DNA) scan to uncover potential sources of risk in your network right now. Identify all your privileged user and application accounts, including those used by third-party users;
- Find out how CyberArk's Privileged Access Security Hygiene Program helps you "think like an attacker." The program was developed based on CyberArk's engagement with thousands of customers who have implemented privileged account security programs. The CyberArk Privileged Access Security Solution focuses on the seven steps that reduce the most risk relative to the level of resources and effort you expend.
- Engage the CyberArk Red Team to simulate adversary behavior and test the security team's ability to respond to threats. By using a variety of tactics, techniques and procedures (TTPs) CyberArk Red Team services are designed to provide a safe way for security operations to uncover vulnerabilities in their cloud environments, test security procedures and identify areas of improvement.

For more information contact one of our sales consultants or visit us at: www.cyberark.com.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.