CYBERARK®

THE IDENTITY SECURITY COMPANY®

Presented by:
Hussein Sbeiti, Jon Fernandez
Ayele Kouevidjin, Chinyere Brown-McVitie

CYBERARK®
THE IDENTITY SECURITY COMPANY®

Agenda

1. Historical Background
2. Year 1
3. Year 2
4. Year 3
5. Zero Day Exploit
6. Laws & Regulations
7. Wrap up – Conclusion

Who We Are

Hussein Sbeiti

Jon Fernandez

Chinyere Brown-McVitie

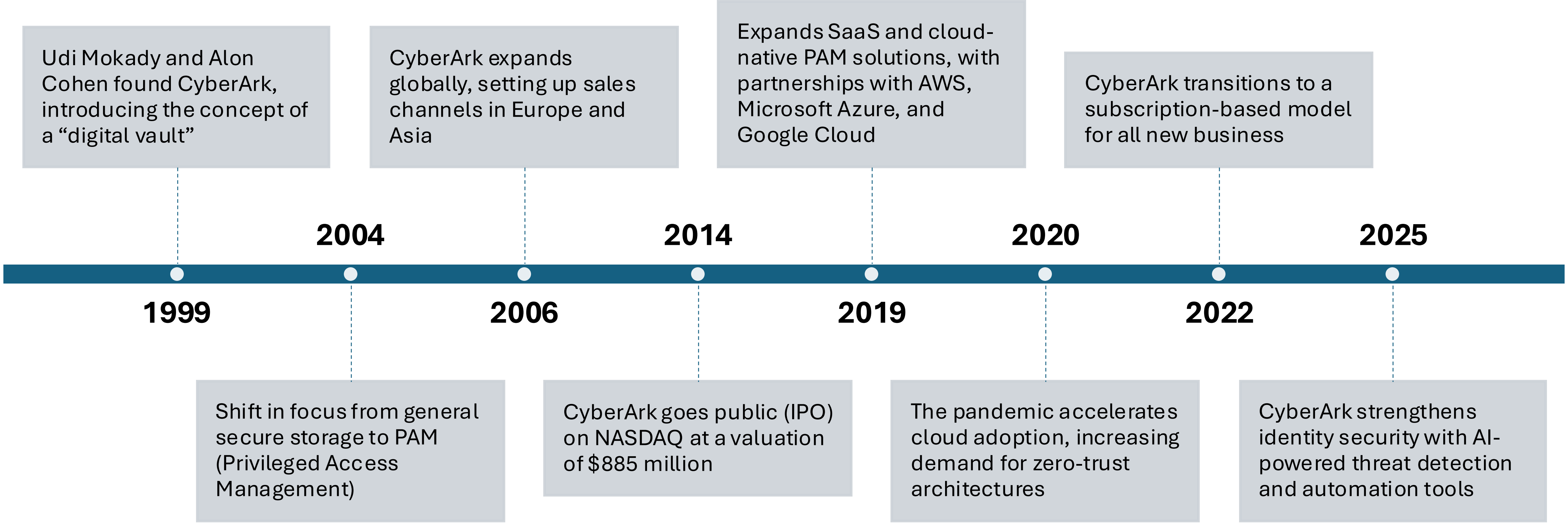
Ayele Kouevidjin

Historical Background

From securing identities to shaping the future of cybersecurity

CYBERARK®
THE IDENTITY SECURITY COMPANY®

Historical Background



1999 Udi Mokady and Alon Cohen found CyberArk, introducing the concept of a “digital vault”

2004 Shift in focus from general secure storage to PAM (Privileged Access Management)

2006 CyberArk expands globally, setting up sales channels in Europe and Asia

2014 CyberArk goes public (IPO) on NASDAQ at a valuation of $885 million

2019 Expands SaaS and cloud-native PAM solutions, with partnerships with AWS, Microsoft Azure, and Google Cloud

2020 The pandemic accelerates cloud adoption, increasing demand for zero-trust architectures

2022 CyberArk transitions to a subscription-based model for all new business

2025 CyberArk strengthens identity security with AI-powered threat detection and automation tools

Year 1

Laying the foundation for secure, scalable, and strategic growth

Year 1: Foundation and Trust Rebuilding

- **Form dedicated cybersecurity task forces** including incident response, threat hunting, and vulnerability management teams to immediately improve internal readiness and reduce exposure to active threats

- **Implement scalable quantum computing infrastructure** to test and prepare for quantum-era threats while beginning internal integration of post-quantum cryptographic algorithms into core PAM workflows

- **Launch and operationalize a Zero-Day Vulnerability Response Plan** that includes rapid detection, internal communication protocols, ethical disclosure processes, and customer-facing mitigation playbooks

- **Rebuild client trust and reinforce CyberArk's security reputation** through transparent third-party audits, improved service-level agreements (SLAs), and consistent communication around new security and compliance upgrades

Year 2

Enabling secure, scalable growth through seamless integration

Year 2: Expansion and Integration

- **Expand and integrate quantum-safe cryptography and AI-driven threat analytics** into CyberArk's Vault, Session Manager, and Endpoint Privilege Manager to enhance proactive defense capabilities and reduce false positives

- **Scale up cloud and hybrid infrastructure protection** by embedding PAM controls across major platforms (AWS, Azure, GCP) and enabling secure remote access with Just-in-Time provisioning

- **Develop and formalize strategic partnerships and industry alliances** with cloud providers, security vendors, and regulatory bodies to promote interoperability and drive adoption of CyberArk's zero-trust innovations

- **Enhance go-to-market strategy and global market presence** by tailoring solutions for underserved sectors, expanding partner channels, and targeting emerging markets with localized compliance offerings.

Year 3

Leading the future through innovation and strategic resilience

Year 3: Innovation and Strategic Resilience

- **Solidify CyberArk's position as the industry standard** by contributing to open-source security frameworks, leading global cybersecurity initiatives, and helping define post-quantum PAM best practices

- **Achieve operational excellence through automation and intelligence**, using machine learning to optimize incident detection, reduce human error, and implement real-time risk scoring for privileged access

- **Execute strategic acquisitions and R&D investments** to fill capability gaps in adjacent areas like CI/CD pipeline security, DevSecOps integrations, and privileged access in OT/ICS systems.

- **Future-proof infrastructure and product lines** by preparing for evolving regulatory demands, geopolitical risk, and advanced persistent threats — ensuring CyberArk's long-term resilience and customer trust.

Zero Day Exploit

Anticipating threats, responding with precision, and building resilient defense

Zero Day Exploit: PAM Session Token Hijacking

Exploit Method:

- A **malicious insider** or APT exploits a race condition during session initiation.
- Gains access to **valid session tokens** via man-in-the-middle (MITM) or through endpoint memory scraping.
- Reuses the token to **impersonate** a privileged user without needing credentials or MFA.

Impact:

- Full access to **vaulted credentials**, session recordings, and PAM audit logs.
- **Persistence** across sessions without detection.
- **Bypasses** behavioral analytics if the attacker mimics legitimate workflows.

Why It’s Critical:

- Directly undermines CyberArk’s **core value proposition**: secure and auditable privileged access
- Could lead to **high-profile customer breaches**, regulatory scrutiny, and **brand trust erosion**.
- **Difficult to detect** without deep session integrity checks or behavioral anomaly detection.

NIST Framework in Action – CyberArk’s Strategic Response

🧠 1. Identify

- Map and classify all PSM systems and privileged assets
- Evaluate risk exposure from CVE-2024-39708
- Analyze vendor and threat intelligence sources (e.g., dark web activity)

🛡️ 2. Protect

- Redesign session token validation to prevent hijacking
- Apply quantum-resistant entropy for future-proofing
- Enhance session monitoring and access control policies

🔍 3. Detect

- Monitor for anomalies in session behavior and access patterns
- Leverage dark web intel and APT behavior tracking
- Integrate AI/ML into threat detection pipelines

NIST Framework in Action – Incident Response & Recovery

🚨 4. Respond

- Activate emergency IR team and threat analysis workflows
- Engage bug bounty researcher and validate exploit
- Quietly develop and test patch before public disclosure
- Notify key customers under NDA; prep external comms plan

🧯 5. Recover

- Publish public disclosure and support documentation
- Assist customers with patch rollout and mitigation
- Conduct post-incident review and implement lessons learned
- Rebuild trust through transparency and industry leadership

Laws and Regulations

Navigating the evolving cybersecurity landscape with compliance, clarity, and confidence

Laws & Regulations

Global & National Compliance Frameworks

1. GDPR (EU General Data Protection Regulation)

- Requires strong protection for personal data of EU citizens
- CyberArk must secure sensitive data and user identities

2. SOX (Sarbanes-Oxley Act – U.S.)

- Requires strong internal controls over financial reporting
- PAM is essential for auditability & accountability in financial systems

3. FISMA (Federal Information Security Modernization Act)

- U.S. federal agencies must secure IT systems
- PAM aligns with CDM (Continuous Diagnostics & Mitigation) requirements

International Cybersecurity Standards

ISO/IEC 27001

- Global standard for Information Security Management Systems (ISMS)
- CyberArk is ISO 27001 certified, proving best-practice security

Laws & Regulations

Industry-Specific Regulations

1. GLBA (Gramm-Leach-Bliley Act)

- Applies to financial institutions handling consumer financial data
- Requires least privilege access & privileged activity monitoring

2. SWIFT CSCF (Banking/Finance)

- Protects global financial messaging infrastructure
- CyberArk supports secure access for SWIFT compliance

3. HIPAA (Healthcare – U.S.)

- Safeguards patient data and medical records
- PAM tools support HIPAA-compliant access controls

U.S. Federal Cybersecurity Guidelines

NIST Framework

- Cybersecurity best practices and risk management
- CyberArk aligns with:
  - NIST SP 800-63 (Digital Identity Guidelines)
  - NIST SP 800-207 (Zero Trust Architecture)

Recommendations

Driving decisions with data, strategy, and foresight

Our Recommendations

1. Deploy a Quantum Computer to Drive AI-Powered Security

Acquire and operationalize a quantum computer to simulate advanced threats, train AI models, and enhance breach detection. Use it to rebuild trust post-zero-day exploit and lay the foundation for future-proof security.

2. Integrate Quantum-Safe Cryptography Across All Systems

Embed post-quantum encryption (e.g. Kyber, SPHINCS+) into PAM, MFA, and cloud infrastructure. Protect machine identities, sessions, and secrets with quantum-resilient algorithms.

3. Establish CyberArk as the Industry Leader in Quantum-Enhanced Security

Lead global standards, form strategic partnerships, and publish cutting-edge research. Build quantum-first features into every product and set the benchmark for future cybersecurity.

Thank you

CYBERARK®

THE IDENTITY SECURITY COMPANY®

Citations

1. Harvard Business School Case – "CyberArk: Protecting the Keys to the IT Kingdom"
    - https://hbsp.harvard.edu/product/724406-PDF-ENG
2. CyberArk Official Website
    - https://www.cyberark.com
3. CyberArk Investor Relations & Reports
    - https://investors.cyberark.com/
4. CyberArk Blog: Threat Research & Updates
    - https://www.cyberark.com/resources/threat-research-blog
5. MITRE CVE Directory – CVE-2024-39708
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-39708
6. NIST National Vulnerability Database (NVD)
    - https://nvd.nist.gov/vuln/detail/CVE-2024-39708
7. NIST Cybersecurity Framework (CSF)
    - https://www.nist.gov/cyberframework
8. General Data Protection Regulation (GDPR)
    - https://gdpr.eu/
9. Sarbanes-Oxley (SOX) Compliance
    - https://www.soxlaw.com/
10. HIPAA Security Rule
    - https://www.hhs.gov/hipaa/for-professionals/security/index.html
11. Gartner Magic Quadrant for PAM (2023/2024)
    - https://www.gartner.com/en/documents/3988084
12. Forrester Wave: Privileged Identity Management, Q4 2023
    - https://www.forrester.com/report/the-forrester-wave-privileged-identity-management-q4-2023/RES178041
13. BeyondTrust (Competitor Website)
    - https://www.beyondtrust.com
14. ThycoticCentrify (now Delinea)
    - https://www.delinea.com
15. MITRE ATT&CK Framework
    - https://attack.mitre.org
16. CISA – Zero Trust Maturity Model
    - https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model
17. Splunk Security Blog
    - https://www.splunk.com/en_us/blog/security.html