



ARX

DIGITAL SECURITY SERVICES



Privacy as a Privilege

Welcome to the forefront of digital security with ARX DSS.

As a pioneering company in the realm of digital protection, we are dedicated to ensuring the safety and security of UHNWIs, UHNWFs and Family Offices in the ever-evolving digital landscape. Explore the essentials of digital security and discover how ARX can help you navigate the online world with confidence and peace of mind.

IN TODAY'S INTERCONNECTED WORLD, THE DIGITAL SPHERE IS FRAUGHT WITH VARIOUS THREATS THAT POSE RISKS TO PERSONAL DATA, REPUTATION, AND FINANCIAL ASSETS.



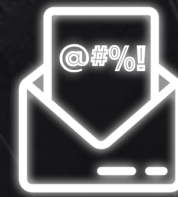
Personal Data Leaks

- Home Network Intrusions
- Account Takeover
- Physical Threats
- Identity Theft
- BotNets



Cyber Threats and Hacks

- Credential Harvesting/Reuse
- Social Engineering Attacks
- Communications Hijacking
- SIM Swapping
- Lateral Attacks



Online Defamation and Slander

- Man-in-the-middle attacks
- Malware/Ransomware
- Spoofing/Impersonations
- Cyberstalking/Harassment
- WiFi Attacks



Financial Risks and Fraud

- Personal email compromise
- Financial Digital Fraud
- Data Leaks
- Device Vulnerabilities

Cybersecurity for UHNWIs and Family Offices protection is more than just a perimetral service. In fact, in today's treacherous digital landscape, it's a basic requirement for privacy and security. ARX services with dedicated experts will help you secure digital life and home/yacht/residence networks. We offer a coordinated defense and solutions that rival consumer-grade options.

- Monitoring and security of all devices, including computers, tablets, and cell phones
- Identity theft protection and insurance
- Personal Privacy Kit
- Continuous deep/dark web scans for leaked usernames and passwords or sensitive account data,
- Internet data broker information removal

At ARX, we understand the unique cybersecurity needs of Ultra-High-Net-Worth Individuals (UHNWIs) and Family Offices. Our services, specialized solutions and expertise are tailored specifically to address the complex challenges faced by these audiences.

With a deep understanding of the digital landscape and extensive experience in protecting high-value assets, we offer unparalleled cybersecurity services that ensure peace of mind and confidence in an increasingly connected world.



ARX

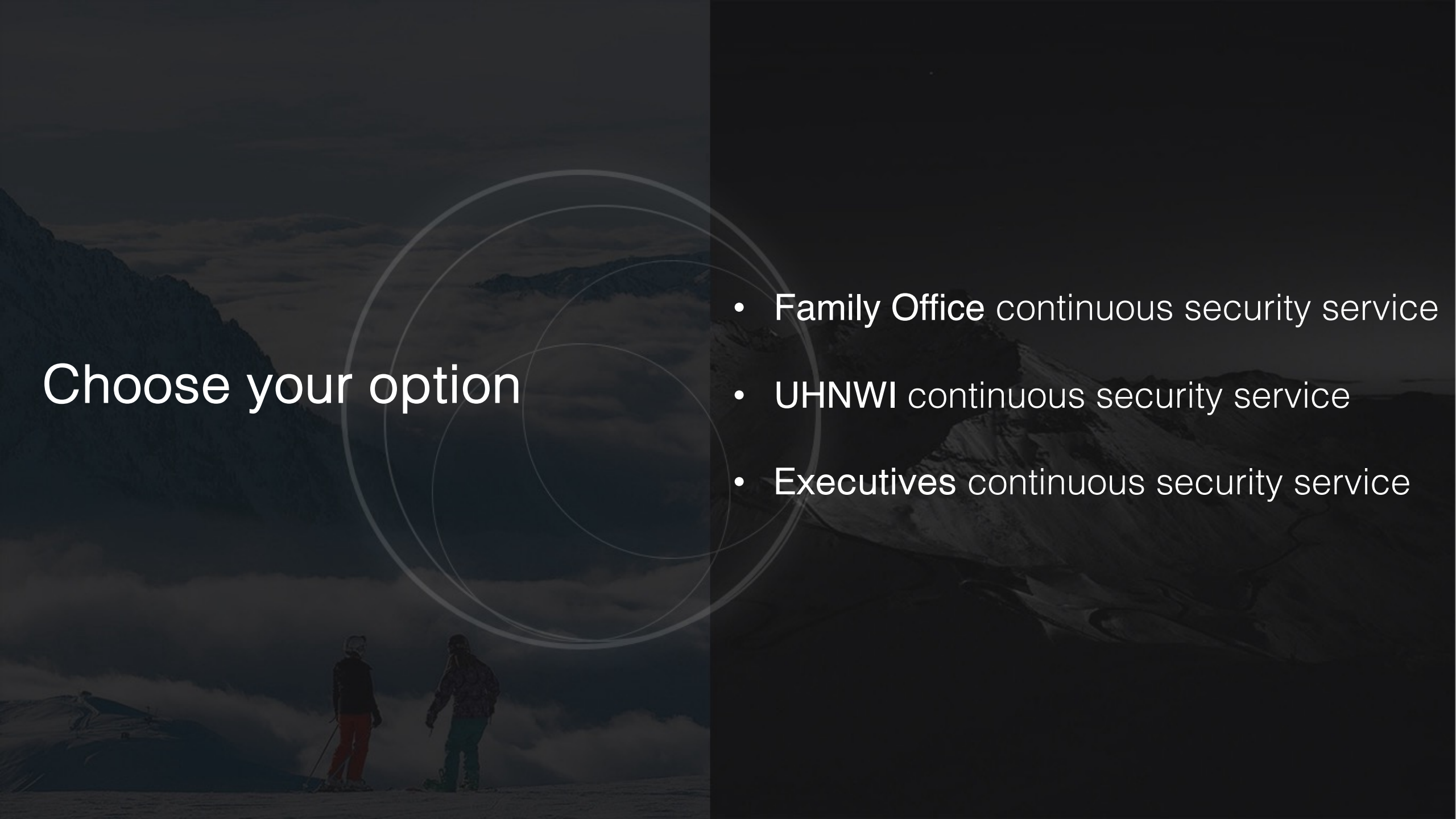
ASSETS

- **Smart Home Systems:** smart home automation systems installed in residences, controlling everything from lighting and HVAC systems to security cameras and entertainment systems. These systems can be vulnerable to cyber attacks if not properly secured, potentially compromising the privacy and security of the homeowners.
- **Yacht and Aircraft Systems:** yachts or private jets have onboard systems connected to the internet for navigation, communication, entertainment, and security purposes. These systems can be targeted by cyber criminals, posing risks to the safety and security of passengers and crew.
- **Artificial Intelligence (AI) Investments:** using AI technologies for various purposes, including wealth management, security surveillance, and personal assistants. Protecting AI systems from cyber attacks is crucial to prevent unauthorized access to sensitive data and ensure the integrity of decision-making processes.
- **Cryptocurrency Holdings:** Some UHNWIs hold significant investments in cryptocurrencies, which are inherently digital and susceptible to cyber theft, hacking, and fraud. Secure storage solutions, such as hardware wallets and cold storage, are essential to protect these assets from cyber security threats.
- **Personal Digital Footprint:** extensive digital footprints, including social media profiles, online shopping accounts, and personal websites. Cyber criminals target these digital assets to gather sensitive information, launch social engineering attacks, or impersonate the individuals for fraudulent activities.
- **Online Reputation Management:** Maintaining a positive online reputation is critical, as Individuals may be targeted by reputation-damaging attacks, such as negative press coverage, fake reviews, or social media smear campaigns. Reputation management strategies and online monitoring tools help mitigate these risks.
- **Family Office and Financial Systems:** UHNWIs typically rely on family offices to manage financial affairs, investments, and estate planning. These systems contain highly sensitive information that must be protected from cyber threats, including ransomware, phishing attacks, and insider threats.



Our cybersecurity services include

- Risk Assessments: Comprehensive evaluations to identify potential vulnerabilities and risks.
- Threat Detection: Proactive monitoring and analysis to detect and mitigate cyber threats in real-time.
- Incident Response: Rapid response teams and recovery strategies to minimize the impact of cyber attacks.
- Secure Communication: Encrypted platforms and solutions to protect sensitive conversations and data exchanges.
- Digital Asset Protection: Measures to secure digital assets, including cryptocurrencies, intellectual property, and personal information.



Choose your option

- Family Office continuous security service
- UHNWI continuous security service
- Executives continuous security service

FAQ

How can cybersecurity services help protect my digital assets and personal information?

Our cybersecurity services employ a range of techniques, including risk assessments, threat detection, secure communication platforms, and incident response strategies, to safeguard your digital assets and personal information from cyber threats such as hacking attempts, data breaches, and identity theft.

What types of threats do cybersecurity services for UHNWIs and family offices protect against?

Our services are designed to protect against a wide range of cyber threats, including malware infections, phishing scams, ransomware attacks, online defamation, data breaches, and identity theft incidents. We employ proactive monitoring and analysis techniques to detect and mitigate these threats in real-time.

How do you ensure the confidentiality of sensitive communications and data exchanges?

We utilize encrypted communication platforms and solutions to ensure the confidentiality of sensitive conversations and data exchanges. These platforms employ advanced encryption techniques to prevent unauthorized access and eavesdropping, providing a secure environment for your communications.

Comprehensive protection, with a focus on key service elements

Rapid Incident Response

- *Our dedicated incident response teams are available 24/7 to provide swift and decisive action. With our rapid response capabilities, we minimize downtime, mitigate the impact of the incident, and restore normal operations as quickly as possible.*

Cutting-Edge Technologies

- *We leverage cutting-edge technologies and tools to deliver best-in-class cybersecurity services. From advanced threat detection systems to state-of-the-art encryption techniques.*

Proactive Monitoring and Analysis

- *Our proactive monitoring and analysis capabilities allow us to stay one step ahead of potential threats. We continuously monitor your digital environment for any signs of suspicious activity, analyzing data in real-time to detect and mitigate threats before they escalate into full-blown attacks.*

Continuous Improvement

- *We are dedicated to continuous improvement and innovation. We regularly assess and refine our processes, methodologies, and technologies to ensure that we are providing our clients with the most effective and efficient cybersecurity solutions possible.*