Cyber Bodyguard Service

With growing usage of wireless LAN technology and Wi-Fi as well as with other applications such as smartphones, smart homes, and embedded devices, so grows our exposure to Cyber-attacks.

Even the immensely common mobile devices or smartphones, tablets and smart accessories are an incredibly profitable target for hackers since they hold vast amount of sensitive personal data on the user.

Cybe rcriminals target executives, high net worth individuals, celebrities, athletes, public persons and the families of all the above, due to their limited level of cyber protection and inability to access high level enterprise cyber solutions. Similarly, the interests and public brand of VIPs and family offices are growing increasingly vulnerable due to an ever-growing digital footprint.

So what can you do to defend your information?

Our cyber security services

We offer a special tailor-made package of advanced cybersecurity solutions to safeguard these precious digital interests.

Private VPN
With multiple locations worldwide.

Private Mobile Device Management
(MDM)/Endpoint detection and response (EDR)
 For mobile devices and computers.

**Managed security
operations center**
 (SOC) 24/7, 365 days a year.

Technical support
24/7, 365 days a year.

<u>Private VPN info structure</u>

<u>What is VPN?</u>

A virtual private network (VPN) is a setup of software and hardware, that creates a **safe, encrypted network** connection over a network with a lower degree of security, such as the public internet or public WI-FI.

- A VPN uses tunneling protocols to encrypt data at the sending end" and decrypt it at the receiving end. To provide additional security. The originating and receiving network addresses are also encrypted by the VPN.

  Our Private VPN service Includes:

- A private infrastructure for each client **to ensure 100% privacy and secrecy** with ability to unlimited locations around the world.

- The VPN is installed on the client's private devices to ensure full encryption and privacy.

<u>The Features:</u>

- Full end-to-end encryption.
- Cross platform clients (Windows, OSX, Linux, Android, iOS)
- Multiple locations worldwide.
- Easy Installation and setup.
- 24/7, 365 days technical support.

Our private VPN service works even in countries that block known VPN services and providers, this to ensure our clients to be able to work safely around the world.

<u>Private MDM/EDR</u>

<u>What is MDM ?</u>

Mobile device management (MDM) is a security software used by an IT departments to monitor, manage and secure employee's mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization.

Mobile device management software is often combined with additional security services and tools such as Mobile Application Management to create a complete mobile device and security Enterprise Mobility Management solution.

<u>What is EDR?</u>

Endpoint Detection and Response (EDR), also known as Endpoint Threat Detection and Response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

What is our Private MDM/EDR service Included ?

- Private MDM software and infrastructure for each client to ensure capsulation of encrypted data for each user; all infrastructure is installed on our private cloud or on client's private cloud.
- Enterprise level EDR software solution to match client's security needs.
- We provide enterprise level grade clients for each operation system (Windows, OSX, Linux, android, iOS) and device; we also provide setup and install service.
- Managing, maintaining and enforcing policies according to client's security needs.
- 24/7, 365 days a year incident response and mitigation operated by professional cyber analysts.

The Features:

- <u>All-encompassing device and operating system support.</u>
- <u>Hardening Device security and capabilities.</u>
- <u>Access control features with ability to fully control and set on/off physical components such as WIFI, microphone, camera, GPS, Bluetooth and NFC.</u>
- <u>Over-the-air (OTA) distribution of security updates.</u>
- <u>Remote Device troubleshooting.</u>
- <u>Remote wiping in case of lost or stolen device.</u>

- <u>Whitelisting/Blacklisting of apps, websites, IP's, and servers to prevent known attacks on our clients.</u>
- <u>Incident response with data search and investigation.</u>
- <u>Alert triage or suspicious activity validation.</u>
- <u>Suspicious activity detection.</u>
- <u>Threat hunting or data exploration.</u>
- <u>Blocking malicious activity.</u>