

MONOLITH⁺

Information Security



MONOLITH⁺

Information across the globe is seizing to be private. Your private and business data no longer belong to you.

We take the right for data privacy back.

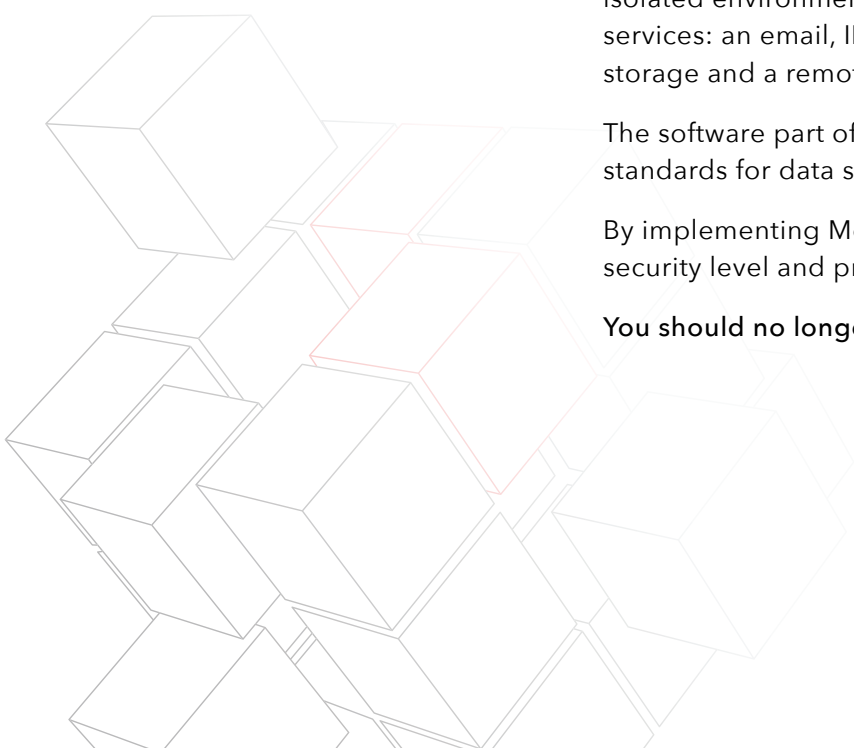
The long-standing need for an easy, efficient and reliable IT solution has brought us to creating a system you can actually trust both your private and business data to.

Monolith Plus is a hardware and software complex that includes a secure and isolated environment (a server infrastructure) and protected communication services: an email, IP telephony and messaging services, a personal cloud storage and a remote desktop service.

The software part of Monolith Plus is based on global enterprise-level standards for data security, utilizing cutting-edge open-source solutions.

By implementing Monolith Plus, you boost your confidential business data security level and prevent risks related to data leaks.

You should no longer worry about cyberattacks, tracking, or data theft.



MONOLITH⁺



Data protection from all types of threats

Zero compromise

Monolith Plus eliminates all kinds of IT threats

It disables data theft both by your employees and 3d parties

Monolith Plus allows you to establish processes within your IT infrastructure that eliminate any risks of data leaks.

It restricts access to your private data

Monolith Plus hides your authentication history, your geographic location and routes you take. It prevents unauthorized access to your private data.

It prevents both legal and illegal methods of espionage

Monolith Plus technologies eliminate the possibility of intercepting your data, such as text or voice messages and files you send, contact lists you use, or voice conferences you hold.

It allows for uninterrupted operation of your IT services

Monolith Plus establishes a resilient IT infrastructure. The system has a geographically spread architecture.

Protects against malware software

Monolith Plus detects any suspicious activities and blocks them, preventing the malefactors from gaining access to your data.

It resists data capture by force

In case of an obvious threat, Monolith Plus can mislead the attacker to alternative network resources while you apply the plausible denial strategy.



IT specialists always aim to improve data protection for the companies in the light of globally growing threat level with hackers extending their area of operation. And that may bring businesses to using solutions from different vendors.

All that is leading to data protection becoming more complex, as the number of devices, traffic volumes and access speed keep constantly expanding.

SOLUTIONS EASE AND INTEGRATION IS SOMETHING YOU SHOULD MAKE YOUR STRATEGY WHEN ESTABLISHING A SECURE IT ENVIRONMENT.



Cyberattack probability by industry.

There is no safe industry.

These graphics are showing trends in blocked traffic percentage: this type of traffic in smaller or larger quantities is present in all industries. The attacks intensity may vary with time, yet all business areas are affected.

Companies that have not been attempted to hack may think they have avoided the danger. But this confidence has no grounds.

Considering the variety of methods and tactics hackers can use, breaching your IT security is only a matter of time.

PERCENTAGE OF MONTHLY VERTICAL BLOCK RATES



Cisco 2018 annual cybersecurity report. The research involved more than 3600 respondents across 26 countries.

More and more companies suffer losses as a result of security breach.

The consequences of your infrastructure being hacked is not limited to interruptions in your IT services' operation. Data leaks may also result in financial, time, or reputation losses.

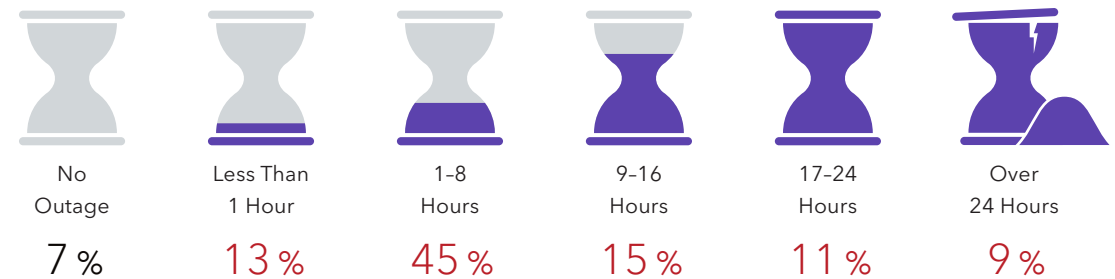
Time to restore the IT infrastructure is not the only thing to be considered when assessing the attack's severity.

There are worse consequences you should attempt to avoid by all means.

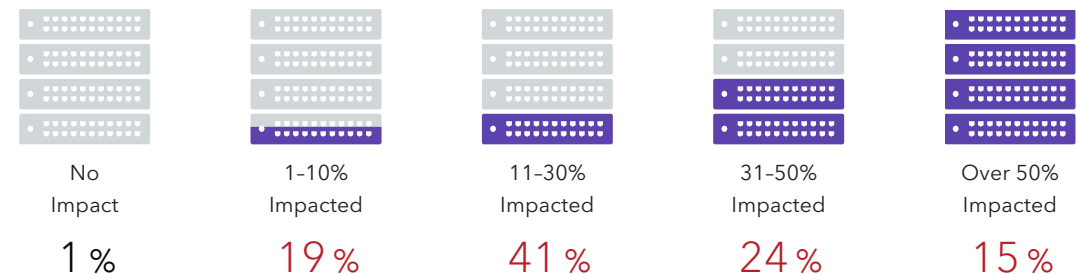
Neither organization aiming for growth and market success wants their department to fall victim of a malicious attack. By analysing the research report, the IT security professionals should ask themselves 'If our company suffers the damage due to a security breach, how this will impact the future business itself?'

LENGTH AND EXTENT OF OUTAGES CAUSED BY SECURITY BREACHES

Organizations' systems down time due to breach



Percentage of systems impacted due to breach



Functions most often affected by cyberattacks

36% of IT security personnel claimed that cyberattacks would first target the operations. This means the core business systems may degrade in performance or even become unavailable.

Except operations, security breaches may impact finance (30% respondents referred to it), reputation and brand loyalty (26% for both).



Operations

36 %



Finances

30 %



Brand Reputation

26 %



Customer Retention

26 %



Intellectual Property

24 %



Business Partner Relationships

22 %



Supplier Relationships

20 %



Legal Engagements

20 %



Regulatory Scrutiny

19 %



Have Not Had Any Security Breaches in the Past Year

10 %

Cisco 2018 annual cybersecurity report. The research involved more than 3600 respondents across 26 countries.

Losses for victims of cyberattacks may become catastrophic due to lost profit.

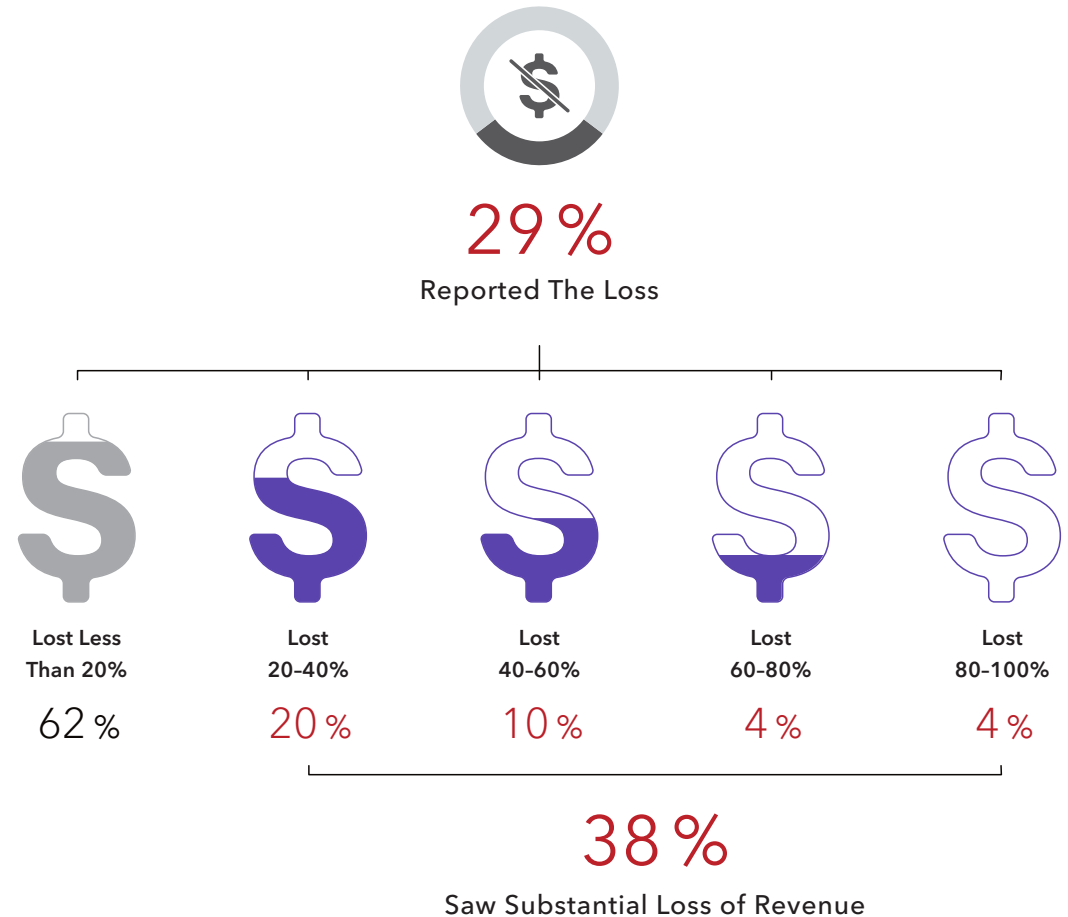
1. Many organizations can estimate the profit loss in monetary values.

29 percent of security professionals said their organizations experienced a loss of revenue as a result of attacks. Of that group, 38 percent said that revenue loss was 20 percent or higher.

2. Twenty-three percent of the surveyed security professionals said that their organizations experienced a loss of opportunity due to attacks. Of that group, 58 percent said that the total opportunity lost was under 20 percent; 25 percent said the lost opportunity was 20 to 40 percent, and 9 percent said the lost opportunity amounted to 40 to 60 percent.

3. Online attacks also result in fewer customers. 22 percent of organizations said they lost customers as a result of attacks. Of that group, 39 percent said they lost 20 percent of their customers or more.

1. PERCENTAGE OF ORGANIZATIONAL REVENUE LOST AS THE RESULT OF AN ATTACK

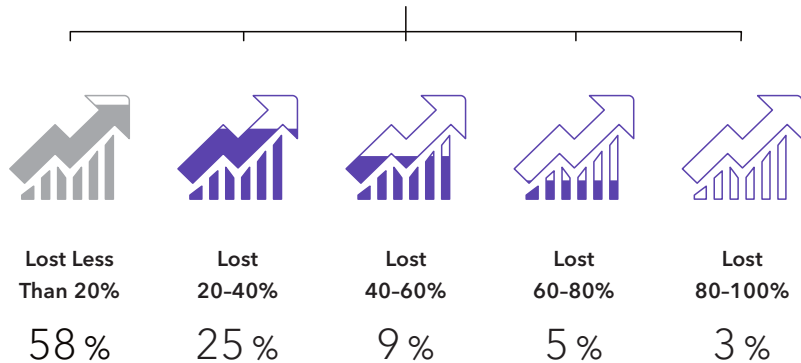


2. PERCENTAGE OF BUSINESS OPPORTUNITY
LOST AS THE RESULT FROM AN ATTACK



23%

Experienced a Loss of Opportunity



42%

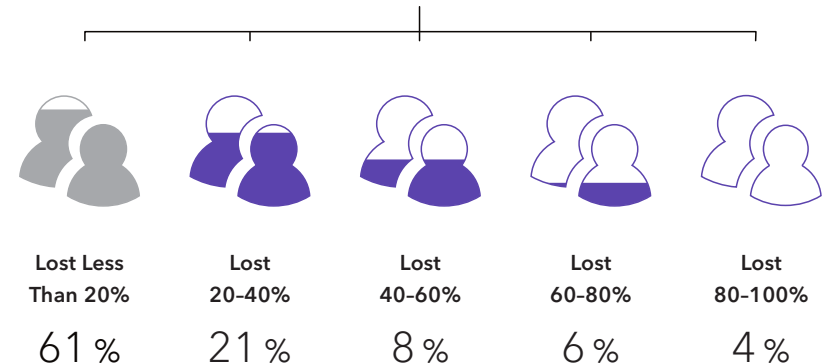
Saw Substantial Loss of Opportunity

3. PERCENTAGE OF CUSTOMERS LOST
BY COMPANIES DUE TO ATTACKS



22%

Experienced a Loss of Customers



39%

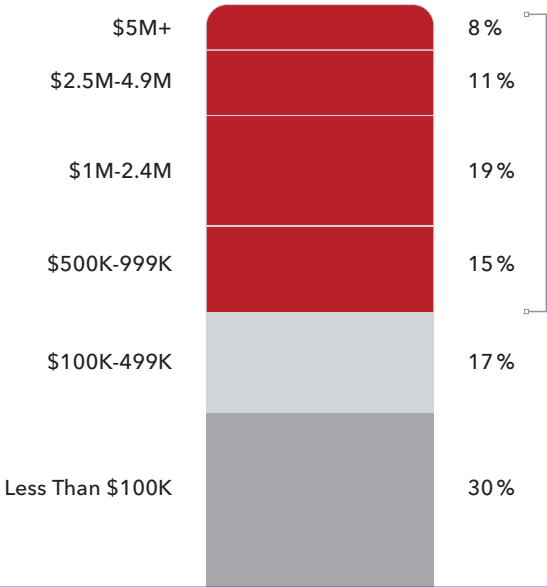
Saw Substantial Loss of Customers

Cisco 2018 annual cybersecurity report.
The research involved more than 3600 respondents across 26 countries.

The cost of attacks

The fear of being hacked is not something indefinite. Nowadays, the price of cyberattacks can be estimated in monetary values and is not hypothetical any more. Hacks can deal significant financial damage and take months, or even years, to recover from.

Respondents reported more than half of all attacks (53%) to have led to financial losses of over \$500,000, including lost opportunities, clientele loss, direct or other losses.



Fifty-three percent of attacks result in damages of \$500,000 or more

The cornerstones of Monolith Plus system

Ease of use and maintenance

IT does not require any special knowledge.
You sustain your business processes.

All-inclusive approach to data security

Monolith Plus controls and protects all communications channels and lower the impact of human factor by creating an isolated environment.

Plausible denial

You can deny the existence of any confidential data and expose only public data.

The service is owned and controlled by you only

We are not just providing you with access credentials, rather provide a fully controlled system.

Services and features we deliver

Monolith Plus is a hardware and software complex providing data confidentiality and security.

The server infrastructure with automated security features

Secure service

- Telephony
- Messaging
- Email
- Remote Desktop
- VPN

Secure hardware

- Smartphone
- Desktop PC
- Laptop PC
- Token (a hardware key)

Integration and security for 3d-party software

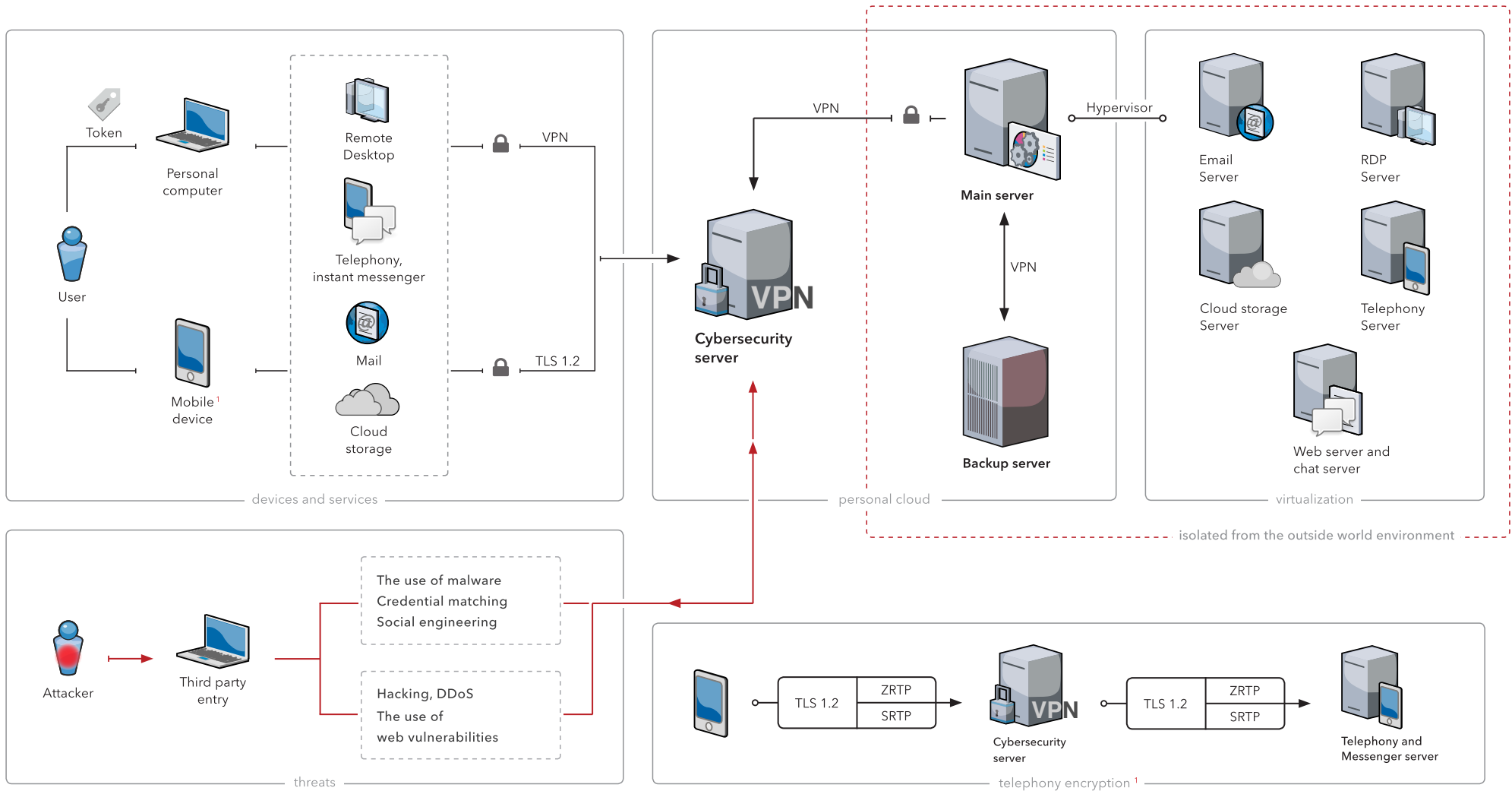
- Industrial software
- Specialized softwaree
- Databases
- CRM
- CMS etc.

Support

- User support
- Technical support

We help your business form a secure mindset

Secure and isolated environment



Infrastructure details

Hardware servers

The server infrastructure is represented by three main parts: a firewall server, a main server, and a backup server.

The firewall (cybersecurity) server performs filtering of the processed traffic according to pre-configured rules.

Its features include:

- ▶ providing secure connection (through VPN or Proxy) from personal devices;
- ▶ users and resources authentication on the system;
- ▶ Deep Packet Inspection;
- ▶ restricting unauthorized access (Intrusion Detection System);
- ▶ forwarding traffic to a guest system when special guest credentials are used.

The main server is running all your software and services. This is where you store and manage your data.

The backup server creates copies of your data in the cloud storage. These copies can be used to restore data where it used to be or at a new location, in case of damage.

The server is responsible for:

- ▶ overall system resiliency;
- ▶ data recovery in case of the main server's emergency shutdown;
- ▶ fast recovery and uninterrupted system operations.

Computer - Cybersecurity Server connection

In order to transfer data to the Firewall Server, the system uses a VPN (Virtual Private Network) method, which can establish one or multiple connections over another network.

The cybersecurity server allows for:

- ▶ highly encrypted data transfer (AES256-GCM-SHA384);
- ▶ online anonymity;
- ▶ network traffic analysis and filtering;
- ▶ data protection in transmission between two endpoints.

To establish a **Computer - Cybersecurity Server** connection users must authenticate with a Token.

Smartphone - Cybersecurity Server connection

In order to ensure data security a TLS protocol is used providing:

- ▶ asymmetric encryption for authentication;
- ▶ symmetric encryption for data confidentiality;
- ▶ message authentication codes (MAC) for data integrity.

Cybersecurity server - Main server - Backup server

All servers are interconnected with a VPN network. A reverse proxy technology is used to hide both the Main and Backup server's IP addresses.

A Token is a compact device (a USB dongle) designed to ensure its owner's security on the network.

The token is used for authentication purposes, as well as remote data access encryption.

AN AUDIT FOR YOUR IT INFRASTRUCTURE

We offer an audit of your personal or enterprise IT system.

We will check it for vulnerabilities, analyze them and provide remediation guidance, all free of charge.

Order an audit by calling +7 495 957 48 49

Anonymity and security for your personal computer

We offer an encrypted laptop with two independent work environments.

It also enables secure storage for your data on the computer itself.

Two isolated systems plus a hidden volume

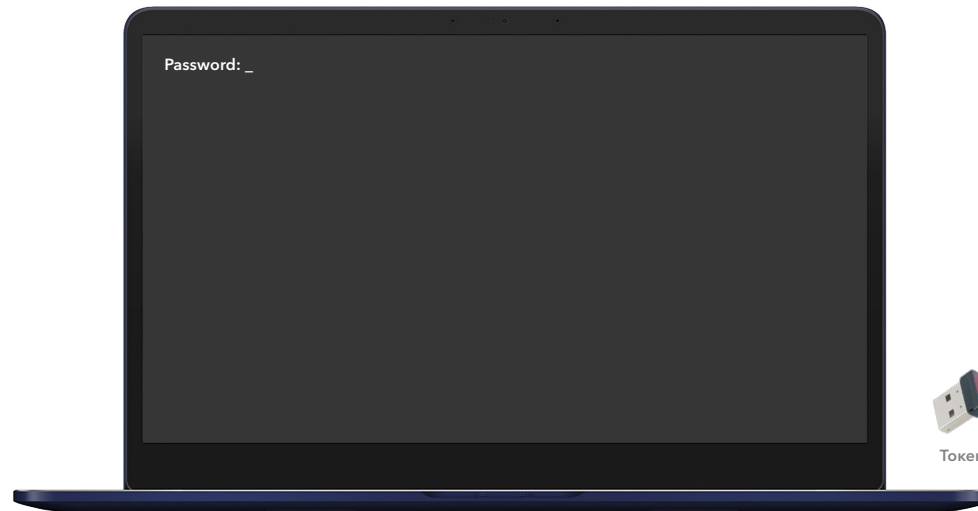
How you log in defines where you find yourself. For example, one password takes you to the main system, another password to the guest system.

Token-based authentication

You use a token to authenticate and to encrypt your data.

Remote desktop service

You work with a remote server where you authenticate with a token.



You, virtually, have you two computers rolled up in one.
All enabled for encryption and token-based authentication.

Encrypted operating systems

Per-volume encryption make data invulnerable to hacking attempts.

IC laser

It monitors the laptop's physical position. Whenever it is lifted off the desk, the system is automatically shut down.

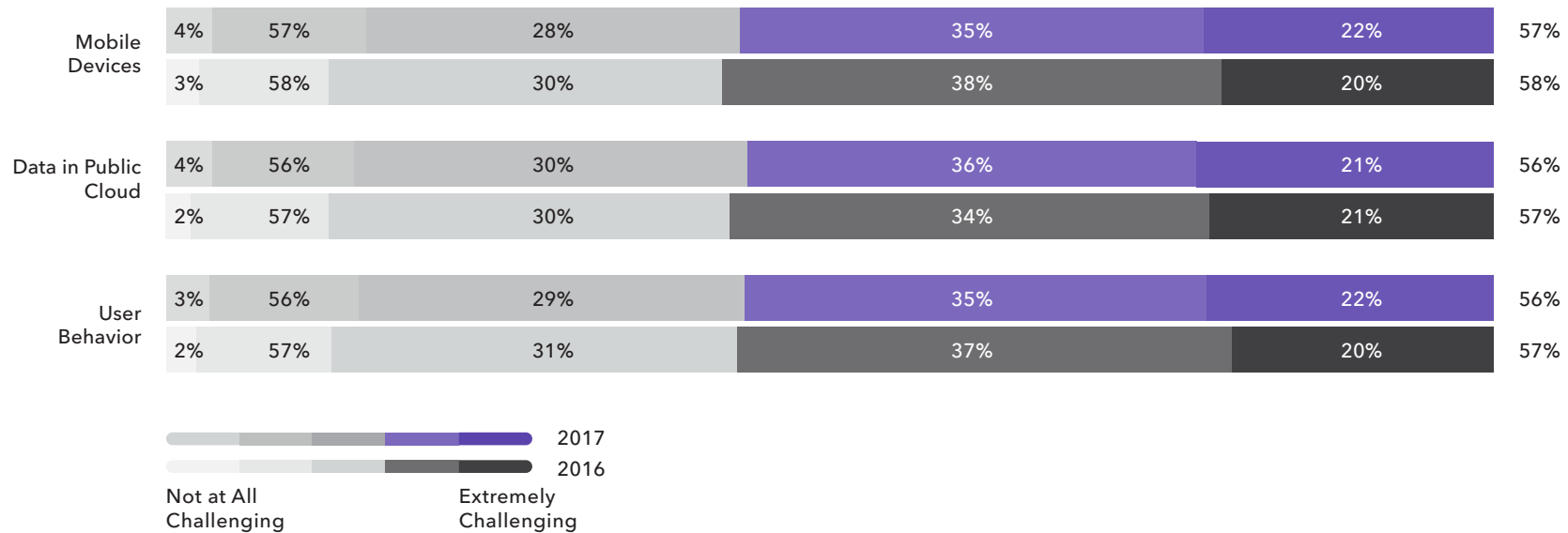
RAM and portable storages security

Both hardware and software levels.

The most complicated areas to secure: mobile devices and cloud storages.

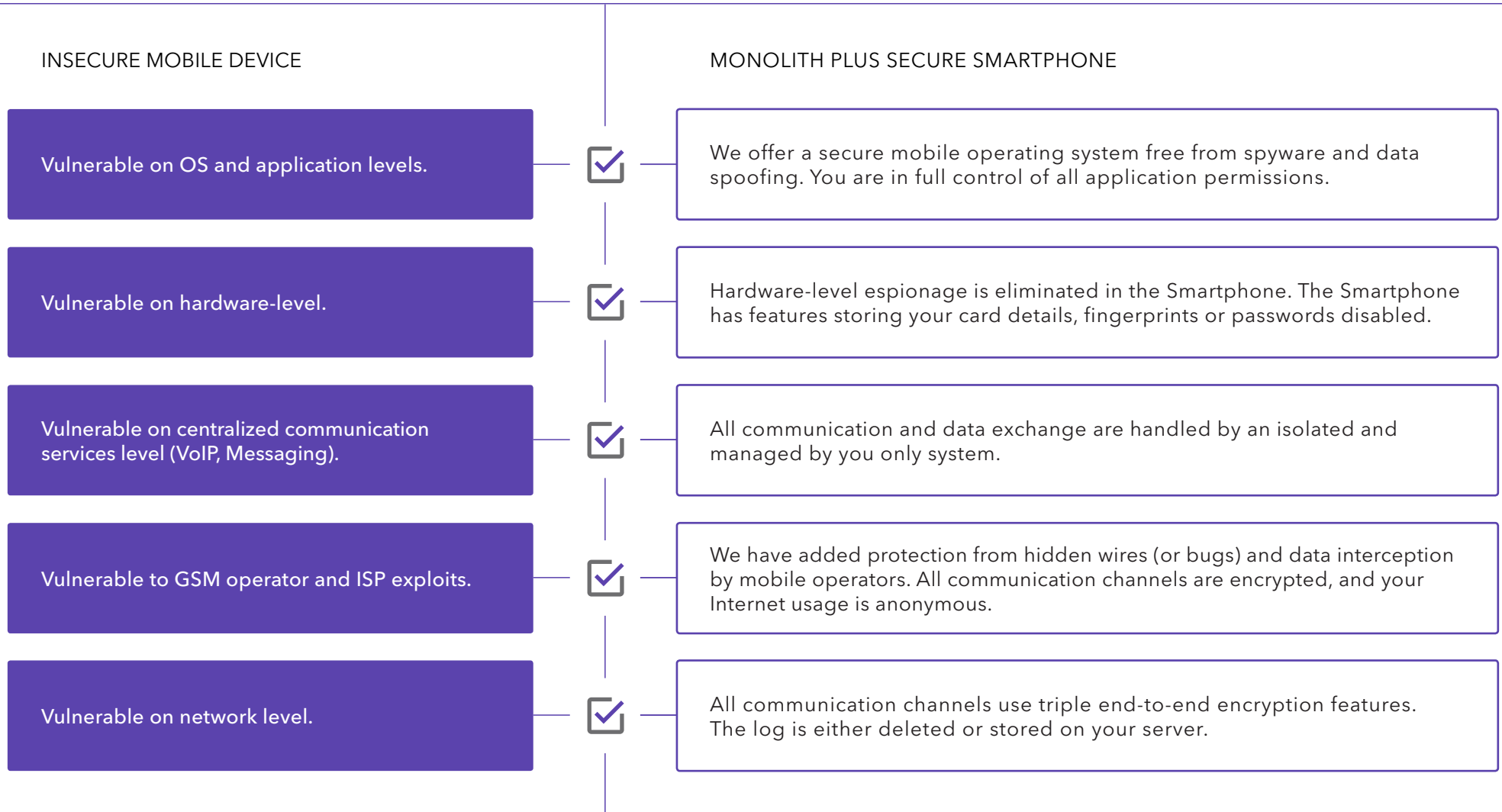
There are many problems in building an enterprise secure environment the IT professionals need to solve. Securing multiple areas of operation simultaneously stands out among those.

The hardest part is establishing secure use of mobile devices, use of data in a public cloud, as well as managing employees' behaviour.



Cisco 2018 annual cybersecurity report. The research involved more than 3600 respondents across 26 countries.

Mobile devices security: vulnerabilities in mobile devices



Anonymity and security for smartphones

We offer a secure smartphone capable of anonymous use.

A smartphone that has sustained all the features and use case scenarios you are familiar with.



Unable to re-issue SIM card.

As a result, it is not possible to access the services in which authorization takes place by phone number.

Secure use of public messengers such as Telegram or WhatsApp.

The phone has two isolated workspaces with separate files and applications.

Cell service from anywhere in the world with internet connection.

Without any restrictions.

The phone is protected from wiretap, data interception, tracking, and user identification.

All files, history and passwords are protected by triple encryption during transfer and storage.

anonymous – secure – powerful

Establishing a secure connection

Triple encryption is used for voice traffic:

- ▶ encryption is transforming data into an ineligible form;
- ▶ metadata encryption is a method for stored and transmitted files security;
- ▶ the server side is encrypted as well.

1 Using its IP address, the smartphone establishes a secure TLS 1.2/TLS 1.3 tunnel (T1) to the Firewall server.

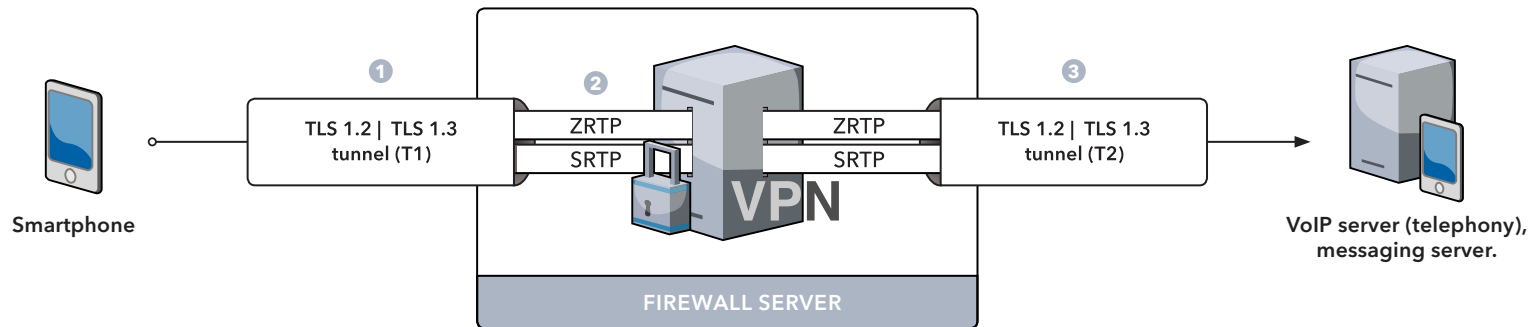
2 Encrypted data is sent to the external IP address of the Firewall server

3 The Firewall server forwards data to the VoIP server via another (T2) tunnel and that is where the data is decrypted.

The Firewall Server forwards the encrypted data from one TLS tunnel into another, while inspecting IP packets and hiding the path to the VoIP server.

The Firewall Server is transparent for the Smartphone.

The VoIP server connects to the Firewall Server as a client which enables for full anonymity.



The Smartphone communicates to the open Internet resources via the server infrastructure which results in a secure and anonymous environment.

The Firewall server ensures the connection security. You cannot establish a non-TLS connection.

ZRTP is a crypto protocol for encryption key negotiation used in Voice-over-IP networks.

SRTP is a protocol that ensures message authentication, message integrity and prevents data spoofing.

Voice and messaging services comparison

	Telegram	WhatsApp	VPole Enterprise	Signal	VoIP services	Monolith Plus
Data storage and management by 3d party	Managed by provider	Managed by provider	Managed by user	Managed by provider	Managed by provider	Managed by user
User identification	By mobile phone number	By mobile phone number	Not required	By mobile phone number	By mobile phone number or passport data	Not required
TLS (metadata protection)	Yes	Yes	Yes	Yes	No	Yes
End-to-end encryption	Encryption managed by vendor	Encryption managed by vendor	Encryption managed by vendor	Encryption managed by vendor	Encryption managed by vendor	Encryption managed by user
Open source server software	No	No	No	Partially open source	Only the protocol is open source	Fully open source
Messages encryption protocol	Proprietary MTProto protocol	Modified proprietary Signal-based protocol.	Proprietary VPole protocol.	Signal	N/A	Open source E2EE/OMEMO/OTR protocols
Voice traffic encryption protocol	Enabled, controlled by provider	Enabled, controlled by provider	Enabled, controlled by provider	Enabled, controlled by provider	No	Yes: SRTP/ZRTP
Locally store data	Partially encrypted with device key	Partially encrypted with account key	Partially encrypted with account key	Partially encrypted with device key	No	AES256 full encryption
Vendor/provider can block accounts	Yes/done regularly	Yes/done regularly	Yes	Yes	Yes/done regularly	You are in control of all ac-counts
Location tracking	If permitted by user	If permitted by user	If permitted by user	No	By IP address	No
Locally stored usage log	Stored	Stored	Not stored	Stored	Stored	Not stored, only backed up to your server
Hiding user's IP address	IP address is available to the ISP	IP address is available to the ISP	IP address is available to the ISP	IP address is available to the ISP	IP address is available to the ISP	Your IP address is hidden
Traffic anonymizing	No	No	No	No	No	Looks as regular HTTPS
Mobile device's data security level	On application level	On application level	On application level	On application level	On application level	Both on OS and application levels

MONOLITH.PLUS

Site: monolith.plus
E-mail: hello@monolith.plus
Telegram: [@monolithplus](https://t.me/monolithplus)