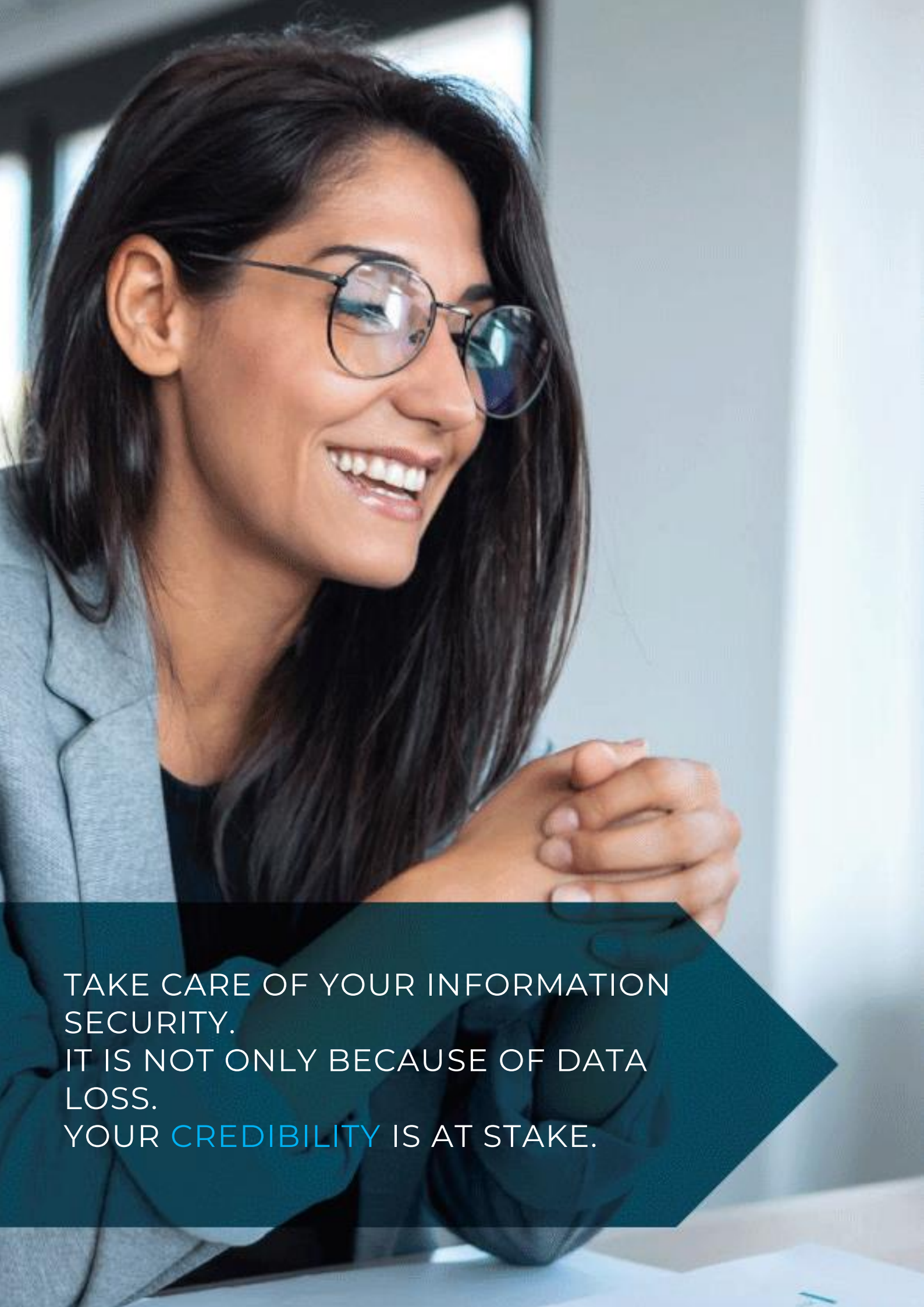
MOORE

CYBER SECURITY

BUSINESS SOLUTIONS THAT TAKE YOU FURTHER


TAKE CARE OF YOUR INFORMATION SECURITY.
IT IS NOT ONLY BECAUSE OF DATA LOSS.
YOUR CREDIBILITY IS AT STAKE.

CYBER SECURITY

Looking at the client business today and thinking ahead

Against background of long-term international and local experience, Moore renders a package of tailored services to meet every objective of clients.

The following is a list of information security solutions. Our clients may receive a full range of services thereunder. The turnkey implementation package includes: choosing an appropriate IT solution, preparation of project documentation, implementation and configuration of solutions, formation of internal documents, staff training and further local technical support on behalf of our certified experts.

Our team members will be able to meet your most demanding needs in the field of implementing integrated solutions, creating project documentation or other information security services.

PORTFOLIO OF SERVICES AND SOLUTIONS

SERVICES AND CONSULTING:

- ·Implementation of IS and IT solutions;
- ·First line technical support;
- ·Development of project documentation;
- ·Training according to proprietary and certified technologies;
- ·Penetration testing;
- ·Software development;
- ·IT and IS audit.

Our mission lies in assisting our clients in successful development of their businesses by rendering robust solutions at high quality standards.

HARDWARE:

Vendor Hardware Solutions;

Network Hardware:

- Commutators of various types and configurations;
- Routers of various types and configurations;
- Scalable multi-functional network appliances;
- Wireless access points;
- Wireless bridges;
- Wireless network controllers.

Server Hardware:

- Hardware and virtual servers;
- Mainframes.

Redundancy Systems and Data Storage;

Work Location Subsystem;

Peripheral Equipment.

ACCESS CONTROL SOLUTIONS PORTFOLIO

Frontline protection

NETWORK ACCESS CONTROL

The functional task of NAC is to collect information about any devices that connect to the network (laptop, printer, IP phone, MFP ...) from anywhere and in any way (Ethernet, Wi-Fi, VPN .. .), and in the automatic mode to grant the given device or the user access / not to grant access / grant access with restrictions.

The result of implementing this solution will be a full visibility of your network with access control and compliance with regulatory requirements. Full and permanent visibility of the network provides control over any changes.

UNIFIED ENDPOINT MANAGEMENT

Solutions of this class are a single console for managing mobile devices of the organization (laptops, tablets, smartphones ...). Among the functionalities of these solutions is a set of technologies, processes and policies for managing and ensuring the security of corporate and personal mobile devices. This is done by managing the parameters of both the devices themselves and corporate applications.

The use of such systems allows solving the problem of blurred perimeter of the organization and reduce financial and reputational risks associated with the end devices (personal or corporate ones).

MULTI-FACTOR AUTHENTICATION

The essence of implementing such solutions is the use of a combination of passwords and additional factors. The combination of this data is: 1) the factor of ownership (what I have): codes from SMS, e-mail, mobile applications, USB-keys and more; 2) property factor (what I am): fingerprints, iris.

Modern solutions offer many technologies for the implementation of multifactor authentication, including the use of artificial intelligence. This will additionally protect your organization from data hacking and theft, as well as optimize the process of authentication of your employees.

THREAT INTELLIGENCE

Threat Intelligence solutions play the role of cyber intelligence, the main task of which is to obtain and analyze data on current threats in order to predict possible attacks and prevent them. Stages of exploration: collection and accumulation of data on threats from different sources into a single system, their enrichment, analysis and application of knowledge.

Increasing the competence of employees through such sources contributes to their efficiency, as well as provides you with protection from new threats.

PORTFOLIO OF NETWORK AND APPLICATION SECURITY SOLUTIONS

Protection, optimization and analysis of terrestrial and / or virtualized infrastructures

DDOS PROTECTION

An increasing number of organizations are exposed to distributed attacks; and they steadily lead to losses. Advanced solutions that quickly and clearly identify malignant traffic provide protection against such attacks. Their algorithms will protect both from simple volumetric attacks, and complex ones as well as from those which are difficult to determine.

Ensuring service continuity is one of the top priorities for many companies. DDoS protection is one of the solutions that can provide round-the-clock access to your services.

IN-DEPTH FILE ANALYSIS (SANDBOX)

Targeted attacks can now be hidden in various types of files that are sent as e-mail attachments, or in update files. Their detection requires in-depth analysis in an isolated environment. Such analysis is performed by "sandboxes", which run suspicious files inside an isolated environment.

The need for such solutions is preconditioned by the fact that one open mail attachment by an inattentive employee or insider can lead to a complete stop of business processes.

FIREWALL POLICY MANAGER

Along with the growth of infrastructure, there is an accumulation of more firewalls. In each of their configuration there are rules that can conflict with each other and subsequently prevent access of devices and applications to each other.

The solution is to get recommendations on the configuration of network screens. As a result, you get an optimized configuration and infrastructure.

WEB APPLICATION FIREWALL

Unlike classic firewalls, a detailed analysis of application-level traffic is performed. The result of such an analysis will be the detection of abnormal or malicious requests to the application and the prevention of application-level attacks. By blocking malicious requests, the load on the server is reduced and the security of applications is ensured. The advantage of such solutions is to provide security without the need to change the application code.

NETWORK PERFORMANCE MONITORING AND DIAGNOSTICS

By using specialized solutions to identify the causes of service degradation, teams may save both time and budget. In large network environments, you can often face various problems, such as low traffic speeds between individual network nodes. The solution may be as follows: detection of bottleneck, suboptimal network channel usage and traffic anomalies. This is performed by analyzing the statistics obtained via IPFIX or xFlow of different versions.

Using such solutions, you can review the prioritization of transmitted traffic, detect, and accelerate slow applications. As a result, you can significantly optimize and speed up the architecture.

PORTFOLIO OF NETWORK AND APPLICATION SECURITY SOLUTIONS

DECEPTION

It allows speeding up the process of detecting the presence of an attacker in the infrastructure to seconds / minutes, slowing down or completely isolating the attacker and stop the attack. To this end, the baits - traps / sensors being deployed in the infrastructure in minutes are used. Externally vulnerable data entities misinform the attacker and signal illegitimate activity. At the same time, there is no unnecessary load on the infrastructure and no additional points of failure are created.

SECURE REMOTE ACCESS

Such solutions will help ensure secure access to corporate applications regardless of the location of users. Remote users are provided with secure use of resources through encrypted tunnels (VPNs). The process of establishing a secure connection can be automated. Such solutions can serve as a single sign-on and provide detailed reporting.

As a result, remote access for employees will be controlled and secured. Accordingly, the critical work is performed much faster.

NEXT-GENERATION FIREWALL

From time to time, information security vendors combine the functionality of multiple solutions into a single solution, thus creating a new class of solutions. A similar situation occurred with Firewall, IPS, Application control, which were combined into NGFW.

A brief list of functions is as follows:

- Packet filtering;
- Network address translation (NAT);
- URL blocking and virtual private networks (VPNs);
- Quality of Service (QoS);
- Intrusion prevention;
- SSL and SSH inspection;
- Deep-packet inspection;
- Reputation-based malware detection;
- Application awareness;
- Full stack visibility and granular control.

The advantage of implementing such a solution is the ability to abandon the historical heritage in the form of a group of legacy solutions, as well as the ability to optimize the staff, support and infrastructure costs.

We are always in quest of up-to-date solutions, innovative approaches and technologies to render high-grade and qualified services.

PORTFOLIO OF ENDPOINT SECURITY SOLUTIONS

Applications, workstations, servers and response security & protection

APPLICATION CONTROL

To protect and prevent intrusions on endpoints, such as desktops and servers, in addition to using dynamic whitelists and blacklists, you need to control whether different pieces of code are allowed to run. An advantage also lies in the ability to configure different degrees of control over capacities of application when it is running and when it interacts with system resources.

If such a solution had been available, the infamous Petia would not have had such an effect. All running applications are subject to pre-configured policies, and, according to them, the application receives a degree of freedom.

DEVICE CONTROL

A possibility to copy data to media devices with the further work outside the office is very convenient and speeds up many workflows. However, such convenience inevitably leads to serious risks of data loss or theft. As external media devices still occupy a leading position among vulnerable areas in information security, there is an urgent need to protect against data leakage on external media devices. To this end, solutions that apply security and encryption policies are used. Compliance with such policies is monitored by security officers from a single panel. The reporting system allows you to determine in a few clicks how effective security policies are.

PORTFOLIO OF ENDPOINT SECURITY SOLUTIONS

ANTIVIRUS

This is one of the first information security solutions. It's hard to imagine a person who hasn't encountered various vendors providing their antiviruses. Initially, there was a jet defense mode. A characteristic feature of such protection is the detection of known threats using knowledge of code areas and other unique features of malware. For correct and effective protection, the anti-virus program must have the latest database of virus signatures. Then proactive protection appeared - protection against unknown viruses, based on an understanding of the code and behavior of malware.

Many antiviruses are now a part or basis of more complex solutions.

ENCRYPTION

Another software tool to prevent the leakage of confidential data is the encryption of media. It can be run on tablets, laptops and desktops running Windows. This will prevent the leakage of confidential data, in particular in the event of equipment loss or theft. When encrypting a disk, all the data on it become incomprehensible to outsiders; this, in turn, helps to comply with regulatory requirements. This tool is compatible with traditional, solid state and self-encrypting drives.

ENDPOINT DETECTION AND RESPONSE

Detecting complex targeted attacks is not an easy task. It is even more difficult to react quickly and efficiently. For these purposes, progressive solutions are used, which are usually combined with the Center for Monitoring and Response to Information Security Incidents (SOC), being a client-server architecture. Data of events occurring at network endpoints are continuously recorded, processed and analyzed to detect threats to information security in real time mode. Bulk cloud platforms that include aggregated threat information can be used. Such platforms allow you to: detect previously unknown threats by comparing information about current and existing workstation data; to combine the services of prevention, detection, response, search of threats to information security with managed services into a single platform to simplify the information security of the organization.

PORTFOLIO OF DATA AND USER ACCOUNT PROTECTION SOLUTIONS

Protection, prevention, detection of sensitive data and user accounts leaks

PRIVILEGE ACCESS MANAGEMENT

“The keys to the IT kingdom” are often referred to the privileged accounts, which is preconditioned by their high administrative powers.

Therefore, monitoring and controlling these records, managing their authentication and authorization, auditing their actions, controlling access, and recording their sessions are critical tasks for the security department. Functionality includes: 1) centralized management of accounts with privileges; 2) auditing the actions of privileged employees; 3) password management; 3) control of employees' access to administrative resources; 4) management of the authentication and authorization process; 5) recording and monitoring sessions.

The implementation of PAM will result in protection against most targeted attacks and compliance with regulatory requirements. IS officers will have confidence in the observance of password policies and the prevention of undesirable actions. IT staff will receive an effective tool to access critical infrastructure.

DATA LEAK PREVENTION

The possibility of data leakage can be minimized through the following actions and operations performed on a regular basis:

- Detection and automated control of confidential information on all corporate resources.
- Implementation of policies, rights, and transactions block regardless of data location. It is important to record incidents, quarantine suspicious events and promptly report recorded incidents.
- Further adjustment and creation of new security policies. Further management of the solution on the basis of new and changed documents. General analysis of the situation and automated preparation of risk reduction reports.

By implementing and properly configuring such solutions, users themselves will be protected from transmitting sensitive information to attackers.

DATABASE ACTIVITY MONITORING

To optimize and protect databases, it is necessary to monitor the activity of databases, regardless of the type and vendor of the solution used in the infrastructure. Monitoring of the privileged users allows you to track all actions performed in the database and detect atypical and abnormal actions. This is complemented by software activity monitoring, while applications work with databases. As a result, the employees who perform illegitimate actions directly or using applications are detected. By performing analysis, such solutions protect against database-targeted attacks.

DATA CENTER BACKUP AND RECOVERY SOLUTIONS

The gentleman's set of any organization shall include the backup solutions. Enterprise backup solutions combine virtual and physical environment protection, simplify backup, and have the ability to create instant copies of virtual machines through integration with such technologies as Volume Shadow Copy Service and VMware vStorage API for Data Protection. All this reduces the use of CPU, memory and I / O resources on virtual hosts. Due to their specialization, these solutions can perform backups to disks, magnetic tapes and in the cloud.

PORTFOLIO OF DATA AND USER ACCOUNT PROTECTION SOLUTIONS

IDENTITY AND ACCESS MANAGEMENT

To ensure the proper level of security of the organization, you need to get a full and up-to-date picture of the accounts in the infrastructure. This can be achieved through regular auditing of accounts, collection of data on used and unused accounts, their privileges, access and management. An important aspect of work optimization and elimination of the human factor is the automation of the processes of attracting a new employee to the organization, leaving or changing the post (position). IAM can make life easier both for security professionals and employees of other departments.

SECURITY INFORMATION AND EVENT MANAGEMENT

SIEM is required to obtain and analyze information. You can get this information from a variety of sources, such as DLP, IDS, routers, firewalls, servers, etc. The motivation for buying such a solution can be a huge number of objects, the events of which must be monitored. The scenarios when seemingly harmless events, when correlated, pose a threat, are not rare. Suppose a letter with sensitive company data is sent by a person who has the right to do so, but to an address that is outside the standard range of his recipients. The DLP system may not catch this, but SIEM, using statistics, will already generate an incident.

PATCH MANAGEMENT

With a large number of regulatory requirements and third-party applications that are prone to vulnerabilities, comprehensive patch and update management are required. Any configuration changes can break the logic of the configured processes. Updates and patches should be tested to prevent such situations. Automation capabilities that reduce downtime and infrastructure load should not be overlooked. Some solutions allow you to quickly detect vulnerabilities in Windows, Mac OS, Linux and hundreds of third-party applications (Acrobat Flash / Reader, Java, web browsers, etc.), as well as centrally deploy pre-tested patches.

DARK WEB MONITORING

Solutions of this class icodeindex the web pages of the darkweb itself, Telegram channels, criminal forums, marketplaces and other sources. Therefore, the risks associated with unwanted data leakage are prevented and the organization is able to protect itself from external threats. The main advantages of such solutions are automation and the ability to detect the required information from all the variety and noise being stored on the pages of the darknet. The use of such solutions opens up opportunities to track leaks of user credentials, confidential information in the form of documents, technical data, intellectual property or data of your customers.

We use our best practices and professional background to exceed the clients' expectations irrespective of the type of service.

PORTFOLIO OF OPTIMIZATION SOLUTIONS

Exchange of experience with the leading manufacturers enables synergy ensuring a high-quality service and compliance with the highest customer demands.

APPLICATION PERFORMACE MANAGEMENT

Solutions on optimization of the application performance are intelligent platforms that are paid off quickly. Due to their versatility, they are also used for applications with modern architectures. The principle of operation is to intercept contextual data of the code level with time-bound for all transactions – end-to-end. In parallel, the monitoring is performed since the moment of the user clicks, as well as the formation of the request in the database, its delivery and vice versa through all components of the architecture. Full and in-depth detailed breakdown of 100% of transactions and infrastructure provides high-speed identification of the root causing problems. The specialization is to provide the required level of visibility, the right context and the ability to adapt - all that is needed to proactively address application performance issues as well as weaknesses affecting the user experience.

OUR TEAM

Through our expert knowledge in teamed with our long standing experience gained in cooperation with local and international companies, our team ensures an expertized approach to the customer objectives.

ALEXEY YAKOVLEV, HEAD OF INNOVATION PROJECTS DEPARTMENT

Alexey Yakovlev is the Head of Innovation Projects Department. Alexey has an extensive experience in rendering IT services to both private clients and public sector. Alexey is responsible for implementation of computer audit methods (CAAT) and IT programs that optimize business and audit processes. Over recent years, Alexey has been engaged in the blockchain field as well as legal and financial issues related to the adoption of this technology at the governmental and corporate levels.

VITALII NASONOV, HEAD OF INFORMATION SECURITY DEPARTMENT

Vitalii Nasonov is an experienced expert engaged in the cyber security field. He worked his way from information security analyst & engineer to the Head of department. He's gained experience in implementing complex projects on information security solutions in large commercial and governmental organizations.

WITH APPRECIATION FOR COOPERATION!

Our contacts:
T: +380 63 170 8884
T: +380 44 206 1030
E: info@moore.ua

8/26 Vadyma Hetmana St., Cosmopolite Multimall, 10th Floor, Kyiv, 03057
www.moore.ua

MOORE

www.moore.ua