An innovative solution by

ITrust
IT Security Services

IKare©

LEADING EUROPEAN VULNERABILITY ANALYSIS AND SECURITY MONITORING TOOL

Having a clear view of your overall security issues has always been a time consuming, costly to implement and difficult to manage process, especially when taking into account asset variety and the associated threats.

IKare automates security best practices, as well as your entire vulnerability management process. The tool provides a simple solution to network discovery, common sense security practices control and vulnerability assessment, all included in one single package. It can upgrade security up to 90%, which is already 10 times more than what a firewall or an antivirus can achieve.

IKare combines successful engines that boost team work. It allows you to cross-correlate data and to filter or to simplify results for both managers and engineers. All services are integrated into a single view and provide the same type of information, displayed differently according to a user's specific needs.

IT Security delivered as a Service

IKare's approach to IT Security enables organizations to successfully achieve both control over security best practices and vulnerability management, while automating the whole process and reducing costs.
Taking advantage of the Software as a Service (SaaS) possibilities, IKare combines powerful services with a tailored delivery model.

VULNERABILITY MANAGEMENT

IKare automates the vulnerability management process lifecycle across the organization. Regardless of the size of your organization, IKare enables you to keep an eye on and efficiently manage your network security.

IT SECURITY MONITORING

IKare is a fully automated tool dedicated to security and vulnerability management, which can toggle: *from a "photo" mode (IT flash security audit done every year at a specific date), to a "video" mode (monitoring your IT security level as well as each of its components),* and generate **automatic summary reports**, including **synthetic reports**, targeting corporate reps.
IKare is continuously evolving thanks to the experience of our security engineers.
They permanently feed the security and vulnerability test scenario database.
These new tests are then automatically pushed forward to our Customers using IKare (as done in the case of antivirus signature databases). Therefore, an optimal security level is maintained with the help of knowledge concerning past breaches or security alerts, as well as any recent intrusion scenarios known or encountered by our teams.

BEST PRACTICES

"The antivirus is no match in the face of new threats.
To maintain a good security level by avoiding default passwords and by monitoring security flaws was, and still is, the best practice for SMEs".

***Herve Schauer**,*
Security Consultant Expert

AUTOMATISEZ LES PROCESS de gestion des vulnérabilités

"To a cybercriminal, your network vulnerabilities are high-value assets (or, in other words, "open doors").
When exposed, these vulnerabilities can be targeted for exploitation, which may result in unauthorized entry into a network.
This can also lead to the exposure of confidential information, providing fuel for stolen identities, triggering theft of trade secrets, violating privacy law provisions, or even paralyzing business operations.
Every day, new vulnerabilities appear because of misconfigurations, flaws in software codes and human errors.
The more wide and complex your network is, the more you are exposed to vulnerabilities.
The issue of vulnerabilities concerns all organizations and so, we understand that vulnerability management is essential if we want to avoid risks."

Source:
"Vulnerability Management for Dummies"

AWARDS

ITrust has already won several international innovation awards:

FEATURES

TECHNOLOGY INSIGHT

The Open Vulnerability Assessment System (OpenVAS) is a framework of services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The actual security scanner is accompanied by a daily updated feed of Network Vulnerability Tests.

As Security Consultants, we decided to take advantage of our field experience, integrating the best security practices into one single easy-to-use tool.
Indeed, IKare includes a Security monitoring scanner working along with a Vulnerability Assessment scanner.
This unique technology increases drastically the accuracy of security flaws detection and reduces the chances of false positives.

A powerful scanner and monitoring tool

IKare is a light scanner that does not impact systems and that can run fast and give users a "real-time" view. Our pentesting engineers developed this technology in our lab to be able to easily target exploitation flaws.
Originally conceived to perform more efficiently internal intrusive audits, our powerful scanner automates a large number of scripts: Netbios, LDAP, SNMP, FTP, NFS, MSSQL, MySQL, Oracle… Now, the scanner is also working great for external servers with HTTP, SSL, WEBApps, DNSn SMTP, SSH… and is able to perform both internal and external scans as a fully-established vulnerability scanner.
The IKare process is different from other vulnerability scanning solutions, since it introduces the notion of "memory" between two scans and provides thereby a real time security monitoring.

IKare displays the following features:

ASSET DISCOVERY

Assets are auto-discovered and added to the IKare Mapping. Securing an infrastructure begins by knowing every device and application within your network. IKare, through the IKare scanner, can discover most devices and applications including firewalls, servers, operating systems, desktop, printers, wireless devices, as well as many other elements.

SECURITY MONITORING

Easily check compliance with security 'best practices'.
Our technology is able to neutralize even the latest threats, thanks a great vulnerability knowledge base, updated each week by a strong community.

VULNERABILITY MANAGEMENT

Simplify and automate Vulnerability Management using a trusted vulnerability scanner (OpenVas), IKare is capable of accurately detecting the vulnerabilities across your network.
Also, our Web Application Scanner (Available since the 1.8 release) automates web application security assessment.

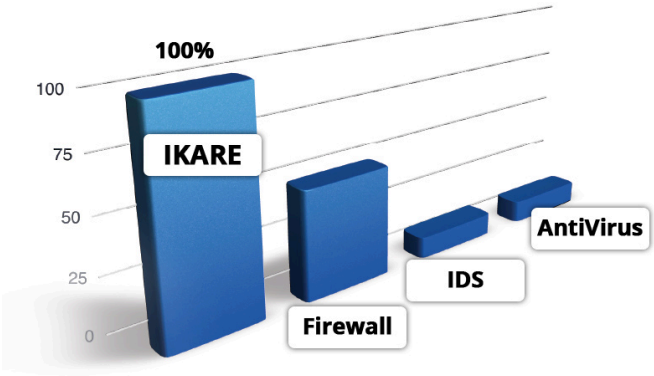
ITRUST SECURITY METRICS

The ITrust label will prove to your customers what a high security level you have in place. It is an authentic evidence of your efforts to maintain a high-level of security.

90% of problems and risk in companies are issued from only ten vulnerabilities. IKare protects you from these 10 weaknesses and easily brings security up to 90%.

Top 10 flaws in enterprises	Covered by IKare
Verbose systems	👍
Weak passwords	👍
Rights & special access	👍
Trust between domains	👍
Default database password	👍
Verbose DNS servers for internal domains	👍
Sharing confidential files	👍
Unecrypted protocols or misconfigurations	👍
Development servers, abandoned servers	👍
Uncorrected vulnerabilities	👍

Coverage rate of top 10 vulnerabilities by technology type



ANALYZE THREATS

IKare's reports provide both executive summaries and a detailed analysis including all vulnerabilities, a description, a risk factor, a CVSS score and the already practiced solutions.

The ITrust technology is the most efficient one when

ADVANTAGES

Non-intrusive

By using scanning technologies, IKare does not impact or disturb customers' resources.
IKare has no impact on information services. Indeed, its powerful algorithm is optimized to not use large bandwidth.
Agentless scanning technology – does not impact resources. There's no need to install agent, an IP device is detected and audited each time when its behavior changes.

Software as a Service

There is nothing to install for external scans. And it only requires a few minutes to install IKare virtual server within an internal environment.
SaaS also represents economic advantages with no extra expenditures:

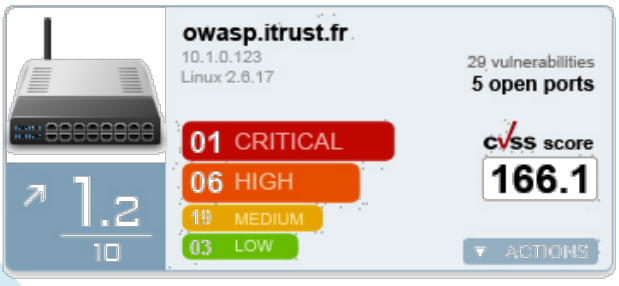
- Lowers your operational costs of deployment and operation;
- Variabilisation (opexisation) of fixed costs concerning computer security;
- Lower insurance premiums and production operations.

Global deployment

- Assesses security within geographically distributed networks;
- Detects inappropriate changes in networks, efficiently and in an up-to-date manner;
- Our engineers are always active and willing to improve all technologies used by IKare;
- Moreover, the different knowledge bases and product improvements are open and global;
- Offer a real-time vision of network assets state through short period scanning;
- One to six hours to put you in regulatory compliance:
- Package Telecom European-Union compliance;
- No production disruption during the security scan.

Tested protocols

- **Databases (MYSQL, oracle, MSSQL)**
- **SSL/TLS and certificate X509**
- **RPC (DCE and UNIX)**
- **DNS (on UDP et TCP)**
- **Finger, FTP, LDAP**
- **http (reverse proxy method and WeBapps)**
- **Netbios (datashare, users on SMB et RPC)**
- **NTP, Pop 3, telnet**
- **Small services (chargen, echo…) SMTP, SNMP, SSH**



Identify easy-to-exploit security flaws

IKare performs basic and best practices security tests to identify easily-exploitable security flaws (example: sharing with low restrictions).

- These engines reduce the number of false positives and detect abnormal behaviors such as unknown viruses "0 day";
- Consistency with CNIL E-Privacy;
- Vulnerability detection becomes much more reliable;
- Vulnerability audit in real time.

Detect malicious behavior

- Le scan détecte les changements inappropriés sur le réseau en comparant les données avec celui fait précédemment (exemple : un nouvel utilisateur devient administrateur) ;
- Identification des zones de responsabilité ;
- Alertes de sécurité ;
- Evolution du niveau de sécurité.

Analyze security flaws

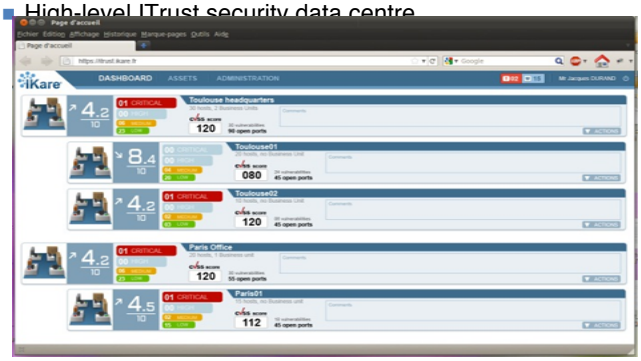
- Scan detects inappropriate changes within your network by comparing data with previous vulnerabilities (example: a new user becomes admin);
- Business Unit Management;
- Security Alerts;
- Treding, time trends of safety.

Centralized vulnerability management

- Automatic centralized reporting from distributed scans;
- Consolidated administration of both internal and external (perimeter) scanning;
- Executive Dashboard;
- Asset-based solution with an interactive asset search portal;
- Authorized user access from any location;
- Export reports.

Automation

- Scheduled scans and network discoveries;
- Automated daily updates concerning the vulnerability knowledge base;
- Automated remediation ticket generation and verification;
- ITrust delivers an easy-to-use scanning infrastructure for distributed networks that can be deployed in 10 minutes;
- High-level ITrust security data centre.



AVANTAGES

Accuracy

- Comprehensive vulnerability knowledge base incorporating thousands of unique checks;
- Trusted, third-party network security certification with tamper resistant audit trails;
- Inference-based scanning engine with non-intrusive scanning techniques;
- Both entrusted and authenticated scanning capabilities.
- Internal and external scanning provides a 360-degree view of network vulnerabilities;
- Configurable scans for customized audits;
- Unique fingerprints for over 2,000 operating systems, applications and protocols.

Reporting

- Customizable reports for on demand reporting by a business unit for executives and managers;
- Automated trending and differential report;
- Remediation reporting: ticket trending by asset group, user and vulnerability;
- Scorecard reports for enterprise stakeholders;
- Automated report generation and distribution;
- Multiple report distribution options.

Evolution

- On demand SaaS technology allows users to scan globally with no additional infrastructure;
- Fast scanning through load balancing of scanner appliances;
- User definable Business Units and Asset Groups that tie into business operations;
- End-to-end encryption of vulnerability data;
- Hierarchical role-based user access controls allowing delegation of responsibilities to reflect organizational structure;
- Policy-based remediation workflow management with automatic trouble ticket creation and assignment.

Interoperability

- Extensible API XML;
- Integration with others SIM, HelpDesk solutions;
- Industry standard support for vulnerability scoring with Common Vulnerability Scoring System (CVSS);
- Industry standard support for the addition of custom detections using Open Vulnerability Assessment Language (OVAL).

Support/Maintenance

- 24x7x365 live customer support;
- Daily signature updates and features enhancement are completed automatically: transparent to the user;
- On-going Web-based customer training;
- Technical training and certification workshop.

Pricing

Annual subscription offers an unlimited assessment of a redefined number of IP devices.
Ideal for regular security assessment of network assets.

Delivery

IKare is delivered as a SaaS (Software as a service), both internally and externally; also available in cloud mode from ITrust servers. Starting from an ISO image, IKare is instantly deployed on an existing infrastructure and comes running in minutes. IKare can next be accessed via a simple browser on any platform.

- Agentless – no agent to install,
- Automatic network and applications discovery,
- Minimalist footprint on bandwidth,
- Ready-to-connect to your IT via XML-RPC API,
- Delivered as well as virtual or physical device,

The ITrust security label

It independently establishes the security of your information system, according to objective criteria and international standards.
The display of this label reassures your clients about the reduction of their overall risk. They would prefer to contract with assessed and labeled suppliers, rather than associate t

Contact

Email: sales@itrust.fr
Tel.: +33 (0)567.346.781
Address: ITrust, 55 avenue l'Occitane
31670 Labège Cedex, France

www.itrust.fr/en
www.ikare-monitoring.com