DIGITALSKILLS
CONSULTING LDA

CYBER SECURITY SOLUTIONS

INNOTECH®

DIGITALSKILLS & INNOTECH SOLUTIONS

Cybersecurity attacks, including ransomware attacks, are a topic that comes up regularly when we talk to CISOs and information security leaders, which is understandable, as recent reports highlight two growing themes: First, Covid-19 resulted in an increase in ransomware campaigns and, in another hand, this type of campaigns has been turning against larger organizations.

There is no denying the impact that a successful ransomware attack can have on an organization, not only in terms of financial and reputation problems, but also the effects of service disruptions. If we look at some of the organizations around the world that have been victims of ransomware, it is not difficult to understand the devastating implications for our reality that a successful attack can have on businesses, customers and citizens.

We have never heard of cybersecurity issues as much as in the past few months. Every day we see news from banks, football clubs, multinationals from various areas and even government entities that are attacked by hackers on a daily basis.

So, in the last 5 years we have been working to fulfill one main objective: to visit the main international events, investigate interesting and innovative cybersecurity companies that appear around the world, and speak with professionals who, in fact, get their hands dirty and work hard and with a focus on protecting companies and their systems, to provide Portuguese entities with the most unique and recent solutions that aim to increase their cyber-resilience to cybersecurity attacks.

At a time when the theme of data protection with the imposition of new legislative standards resulting from the GDPR joins the theme of remote work motivated by COVID-19, it has never been more important to provide a range as diverse as possible of solutions that protect companies like now. And that is our goal.

If we think that the number of connected devices today has far exceeded the number of global populations, we can easily see that some problems are emerging with the increase in the use of the internet, mobile devices and, today, the IoT “devices”. On the other hand, if we think about the number of employees versus the number of devices that each one uses both at their workplace and at home, we begin to analyze the dimension of this problem from another perspective.

And this problem has two faces to protect: human resources and technology.

DIGITALSKILLS®
OFFICIAL DISTRIBUTOR IN PORTUGAL

Centro de Escritórios Campo Grande
Avenida do Brasil, 1, 6º Piso, Sala 8
1749-008 Lisboa

(+351) 217 923 841
info@digitalskills.pt
cyberteam@digitalskills.pt
www.digitalskills.pt

INNOTECH®

Avenida 5 de Outubro 124
2º Piso
1050–061 Lisboa

(+351) 211 315 849
we@innotech.pt
www.innotech.pt

DigitalSkills and InnoTech have the solutions, know-how and experience that address all these challenges, helping many decision-makers to increase their companies' cyber resilience.

Please feel free to ask for more information about our solutions.

PENTERA

AUTOMATED PENETRATION TESTING PLATFORM

A thousand pen-Testers at your service | Not on your Payroll.

THE CHALLENGE

As hackers become more and more sophisticated, corporate security officers and regulators become more aware of the need to integrate the hacker's perspective into their ongoing cyber defense strategy.
Traditionally, penetration testing has been completed manually by service firms, deploying expensive labor to uncover hidden vulnerabilities and produce lengthy reports, with little transparency along the way.
Professional services-based penetration testing, as we know it today, is time consuming, intrusive, costly, represents a point in time snapshot, and cannot comply with the need for continuous security validation within a dynamic IT environment.

THE SOLUTION

Focused on the inside threat, PenTeraTM mimics the hacker's attack - automating the discovery of vulnerabilities and performing ethical exploits, while ensuring an undisrupted network operation. Detailed reports are produced together with proposed remediations, one step ahead of tomorrow's malicious hacker.

AGENTLESS

Zero agent installations or network configurations. Penetration testing starts with physical AN access without any credentials. Just like a hacker would.

ATTACK CHECKPOINTS

For mission-critical systems, a company's security officer can assume discrete control for higher-order exploitative stages to selectively control the intrusiveness level of the attack.

HARMLESS EXPLOITS

Like a hacker, we perform ethical exploitations without disruption of service: e.g. lateral movement, remote execution, relay attacks, password cracking, ethical malware injection and privilege escalation.

PRIORIZED REMEDIATION

Get a clear packaged summary of the critical remediation steps to perform based on threat-facing priorities that are relevant to your organizational network and critical assets.

ATTACK VECTOR VISIBILITY

Every step in the attack vector is presented and reported in detail to document and explain the attack "kill chain" and select the minimal amount of vulnerabilities to stop the attack.

LATEST HACKING TECHNIQUES

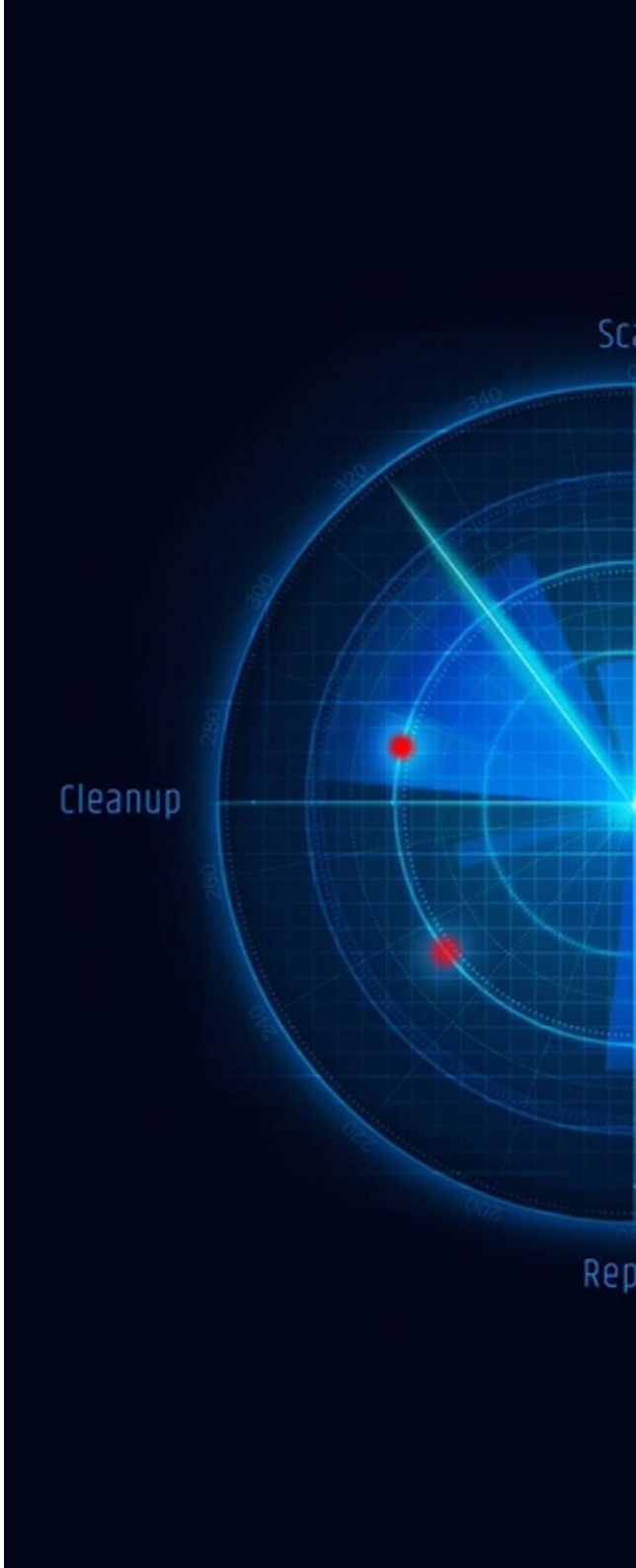
Know that your penetration testing techniques are the most up-to-date.

AUTOMATED

Press "Play" and get busy doing other things while the penetration test progresses. All you need to do is define a range of Ips and check the type of tests you want to perform.

CUSTOM BUSINESS ALERTS

You can set any starting point and penetration testing target and run a targeted attack setting for a specific weakness or for the cyber resilience of specific applications.



PenTera™
By Pcysys

AUTOMATED PENETRATION TESTING PLATFORM

BENEFITS

Continuous Protection

Hold all of your networks to the same high standard

It is critical to consistently check your security controls and defenses across your organizational networks. Pcysys' automated penetration testing platform tests your entire infrastructure with a wide array of hacking techniques ensuring that you remain resilient regardless of how the hacker is trying to break in.

Consistent Validation

Test as frequently as needed - daily, weekly or monthly

Because networks, users, devices and applications constantly change and expose vulnerabilities, it is critical to pen-test continually. Pcysys allows you to validate your cybersecurity posture as often as you need, keeping your guard up at all times.

Easy Deployment

PenTeraTM is locally installed on your network effectively securing your vulnerabilities from the internet and the outside world. The software requires standard hardware and installation only takes a few hours, at the end of which the entire functionality is accessible to you in any environment.

Criteria	Automated PT	Human Based PT
Test frequency	Continuous / On Demand.	Annual / Quarterly
Speed	Minutes-Hours per full PT run.	Days-Weeks per limited PT run.
Consistency	Highest – software runs millions of attack vectors, non-stop.	Partial and highly dependent on the individuals performing the act.
Scope	Entire network / complete coverage.	Based on the time and the number of PT consultants deployed.
Project Approach	None. It's a Plug-and-Play Solution.	Intense project team needs to be assigned & vendor's personnel involved.
Privacy	PT findings only visible to company's personnel.	External PT consultants exposed to confidential information, intrusive, unpleasant.
Most Current	Automated PT is updated monthly with latest vulnerabilities and exploits	Highly dependent on the PT company playbook that is often outdated.

FIDELIS

DETECT | HUNT | RESPOND

FIDELIS ELEVATE: ONE PLATFORM – MULTIPLE USE CASES

Fidelis Elevate provides a streamlined security stack that integrates network, endpoint and deception defenses, automates and orchestrates workflows, and correlates rich metadata across these security layers so you have continuous visibility across your environment. Now you can quickly detect, hunt and respond to threats, while keeping your sensitive data safe.

THE CHALLENGE

Increasingly advanced attacks evade preventive defenses making threat detection, hunting, and response critical as your last line of defense. Attacks make lateral movements within hours of initial compromise and learn new environments to quickly embed themselves deep within organizations' environments. Logs and events are not detecting these advanced threats, nor are existing platforms providing high-speed, interactive and iterative detection and investigation capabilities. Additionally, centralized alert monitoring infrastructure designed to address compliance issues is ill-prepared for today's detection, investigation, response, and hunting requirements.

What's missing is rich metadata with the content and context to drive threat detection and hunting from multiple sensors and endpoints in real-time and retrospectively, driven by multiple threat intelligence feeds. Metadata is also the foundation for machine-learning models and applying data science to security use cases.

THE SOLUTION

Fidelis Elevate™ empowers security analysts to know their environment better than attackers and to engage attackers prior to the point of impact. Regain the advantage with a streamlined security stack that maps your cyber terrain, including all managed and unmanaged assets, and aligns attacker TTPs to MITRE ATT&CK™ so you know their next move and what action to take.

The Fidelis Elevate platform integrates network traffic analysis with endpoint detection and response and deception defenses, automates and orchestrates workflows, correlates rich metadata across these security layers, and leverages machine-learning to gain strong indicators of APTs and potential zero-days attacks. Now you can benefit from higher confidence detections and faster response.

BENEFITS

- Map your cyber terrain of assets and services, plus software inventory and known vulnerabilities.
- Improve detection and response by adding rich metadata to your security infrastructure.
- Enable machine-learning based.
- defenses across multiple sensors, endpoints and deception layers.
- Automate core security analyst tasks for detection, investigation and response to increase efficiency.
- Validate alerts from sensors to endpoints and collect forensic evidence, including full disk images.
- Empower threat hunting across sensor metadata and endpoint files, processes and event data.
- Augment security operations with MDR and IR services

The solution contains three different components, combined in the Elevate platform that centralizes and correlates the data.

Fidelis Network®

Deep Session Inspection®: provides full session reassembly, protocol and application decoding, recursive deep content decoding, and full content analysis to detect threats and data exfiltration.

Multiple Sensors: for gateways, internal networks, cloud VMs, email, and web gateways providing full data visibility and collecting metadata of 300 plus attributes and custom tags for real-time and retrospective analysis.

Asset Profiling & Classification: network sensors map cyber terrain including enterprise IoT, shadow IT, and legacy systems, plus importing external sources including Fidelis Endpoint.

Prevention and Detection: using static, dynamic and retrospective defenses including machine learning anomalies, behavior analysis, sandboxing, multi-dimensional rules, emulation and heuristics, signatures, and threat intelligence feeds (Fidelis Insight, third party, shared, internal).

Data Theft and Loss: using pre-defined policies, data profiling, metadata attributes and custom tags for DLP on network, web and email sensors including OCR image to text analysis.

Automation: of prevention, detection, investigation and response for tier-1 security analyst tasks in a single UI of seam-less workflows for network, endpoint, and deception defenses.

Fidelis Endpoint®

Detection and Response: robust EDR for Windows, macOS and Linux systems including behavior monitoring and detection by indicators (IOCs, YARA rules), on/off grid protection, system isolation, and proven forensic integrity with full disk imaging, files and folders, and memory capture.

Executable/Script Collection and Metadata: for endpoint process and event data for 30, 60, or 90 days enabling automated and manual threat detection, hunting, and custom searches, plus first time seen executable files and scripts for analysis.

Installed Software and Known Vulnerabilities: provides endpoint security hygiene for installed software with links to MITRE CVE and Microsoft KB vulnerability reports, plus OS state and applying patches, report and change FW and AV state, and alerts on USB insertion.

Live Console: provides incident responders with direct, remote access into an endpoint's disk, files and processes, to more quickly mitigate threats found on an asset.

Script Library: with hundreds of ready to use scripts for automated gathering of artifacts, response, or restoring endpoints, plus customization for ad hoc or unique customer requirements.

Threat Intelligence: includes Fidelis Insight cloud-hosted sandboxing, machine learning analysis, behavioral indicator rules, and threat research. Also, custom behavior rules, open feeds for IOCs, YARA rules, and third-party TI feeds.

Prevention: provides anti-malware for Windows powered by BitDefender or AV of customer choice. Process behavior blocking and process blocking by IOC or YARA rules run independently of AV engines.

Fidelis Deception®

High Fidelity Alerts: for cyber security research to learn TTPs and analyze files with real OS decoys, or as a smart alarm system using emulation decoys for no risk, plus supporting enterprise IoT and non-standard devices as decoys.

Automation and Scale: provides discovery of environments to auto-generate decoys, distribute, test access and advertise decoys, plus auto-generate breadcrumbs for distribution to real systems to lure attacks.

Wide Choice of Decoys: Real OS VM decoys, golden image OS decoys, emulated IT assets and services decoys, cloud VM decoys, enterprise IoT decoys, plus loading web pages to HTTP decoys and supporting file uploads into cloud-based sandbox analysis.

Traffic Analysis: scales to enterprise performance levels to determine human traffic from automated malware traffic, detect anomalies and C2, plus provide profiling and classification of assets and services to continuously map environments for changes.

Adaptation and Freshness: deception layers automatically adapt to environment changes, plus provide frequent logins to decoys, publish existence in ARP tables, query DNS servers, and fake accounts with frequent activity in Active Directory.

The joint use of the **Network**, **Endpoint** and **Deception** products provides a complete and in-depth view of the infrastructure, including the vulnerable attack surface. Fidelis integrates, automates and orchestrates capabilities such as asset discovery and classification, network traffic analysis, data loss prevention, endpoint detection and response, and honeypots / breadcrumbs to deflect the attention of potential attackers.

NELYSIS

Detection, warning and prevention of cyber threats on Physical Security and Control System networks.

Real time detection of cyber-attacks.

Protect: Automatic network discovery, interactive network visualization, device profiling, understanding of the normal network behavior.
Detect: Constant monitoring of malicious activities within the network and real time alerting.
Sterilize: Communication with the malicious devices may be disconnected and quarantined, minimizing the risks and damage.

Nelysis protects organizations from new cyber-threats, 0-day exploits and targeted attacks on Physical Security elements and Control Systems networks:

Video Surveillance | Access Control | Intrusion Alarm and Sensors | Fire Alarm | Radars | I/O controllers

REALTIME DETECTION
of cyber security attacks

INTEGRATION
With popular edge security devices

NOT HACKABLE
isolated from the network

FORENSIC
capability with historical traffic analysis

DETAILED ALERTS
to understand root cause and incident analysis

CONSTANT MONITORING
of network edge devices

DEEP PACKET INSPECTION
to monitor all the traffic at the deepest level

DEVICE PROFILING
to detect immediately changes in behavior

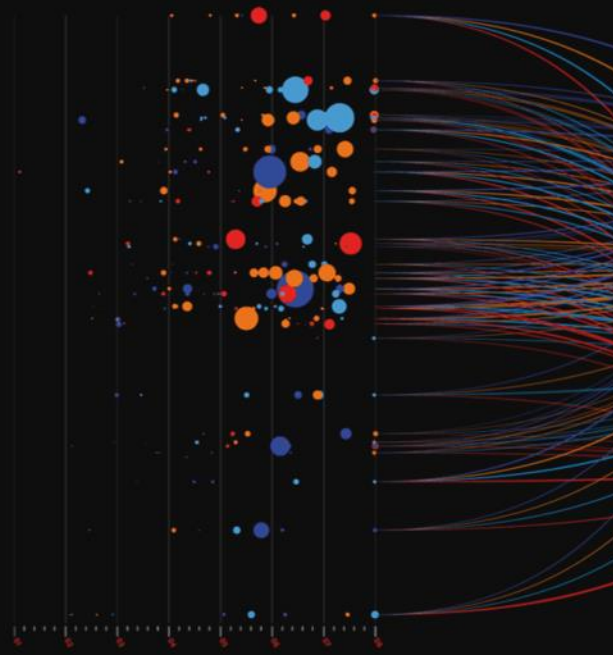
VISUAL NETWORK MAPPING

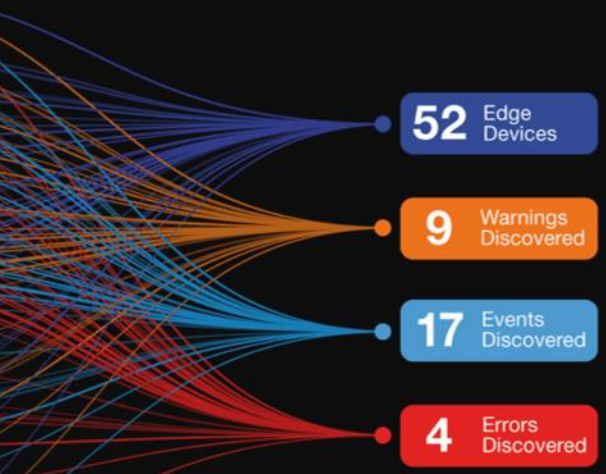
MACHINE LEARNING ALGORITHMS
to automatically identify network elements

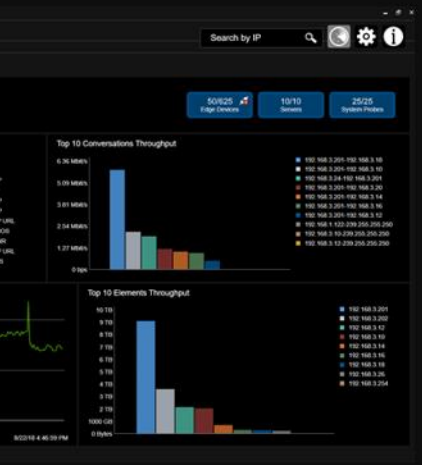
NETWORK INVENTORY
and statistics

PROPRIETARY DATABASE
of vendor vulnerabilities

NEXT GENERATION CYBER SECURITY







VANGUARD ALL-IN-ONE: CYBER SECURITY AND NETWORK TRAFFIC ANALYZER

Vanguard ALL-IN-ONE automatic algorithms allow early detection of cyber threats on Physical Security and Control Systems networks.
Vanguard ALL-IN-ONE is the best and cost effective integrated cyber security and network TCP/IP traffic analyzer for small networks. It's supplied as a standalone unit, for easy and fast deployment at customer's site, no need for other equipment.
Vanguard ALL-IN-ONE it's also a unique tool for network analysis, allowing System Integrators to perform real time and offline traffic analysis, reducing time and costs for onsite interventions

VANGUARD NCM: NETWORK CYBER MANAGEMENT SYSTEM

Early detection, warning and prevention against cyber threats on Physical Security and Control Systems networks.

The Vanguard NCM system, is a unique system enabling e early detection, warning and prevention of cyber threats on Physical Security and Control Systems networks.
The Vanguard NCM visualizes the network and its various elements, detects and identifies a wide range of cyber threats.
The Vanguard NCM extracts network metadata through DPI, detects mismatches with established behavior profiles and issues alerts. The metadata are stored in a Big Data Repository for forensic analysis.

VANGUARD NTC: NETWORK TRAFFIC COLLECTOR

The Vanguard Network Traffic Collector (NTC) is a network analyzer that collects, consolidates and send traffic information to the Vanguard Network Central Management software (NCM).
The Vanguard Network Traffic Collector designed by Nelysis is part of Vanguard System, a unique solution enabling early detection, warning and prevention of cyber threats on Physical Security elements and Control Systems networks.

VANGUARD USB PROTECTOR

Protection, data loss prevention and USB drive control of cyber threats on Physical Security and Control Systems networks.

The increased mobility of storage devices and easiness of data transfer across multiple computers is posing significant risks to network systems. Nelysis, following its mission of full cyber protection, has developed a specific system to prevent cyber-attacks from USB ports.
Vanguard USB Protector provides control and data protection on USB ports, helping the IT administrators and Data Protection Teams to prevent unauthorized content from being introduced in the network as well as restricts sensitive data from leaving the domain.
Vanguard USB Protector is fully compatible with Vanguard NCM and its events and alerts management capabilities

Vanguard USB Protector allows the user to:
Restricts flash-drives usage to the organization's network | Reduces security Vulnerabilities | Prevents leaks and illegal infiltrations | Monitors the outgoing data | Controls the volume and format of outgoing data | Groups USB thumb drives under the same label with specific assigned permissions | Backups/shadows outgoing files | Send Alerts when specific selected data are accessed | Keeps your mobile data confidential at all times | Immediately responds in case of data leaks.

HARMONY IOT

Because things are not as innocent as they seem

Phones, TVs, watches, coffee makers, air conditioners and lightbulbs are all getting smarter and connected. Your enterprise is likely blind to what all these things are doing, which can be a lot!

- The number of Internet-connected things (IoT) is expected to reach 50 Billion by 2020.
- Most of these things communicate via hotspots, unmanaged or public wireless networks, and peer-to-peer wireless connections, making them invisible to traditional management and security systems.
- Most are built with convenience, not security in mind, making them easy targets for attackers.
- As a result, these seemingly innocent things are being used to pierce enterprise defenses to eavesdrop, steal, data, and completely compromise digital assets.

IT IS TIME TO SHINE A LIGHT ON ALL THESE THINGS AND **PROTECT YOUR ENTERPRISE'S SENSITIVE INFORMATION AND ONGOING OPERATIONS FROM IOT THREATS**.
IT IS TIME FOR HARMONY IoT.

HARMONY IOT – KEEPTING YOUR ENTERPRISE SAFE IN TODAY'S SMART CONNECTED WORLD.

HARMONY IoT delivers an enterprise-grade defense for your airspace that protects valuable digital assets from IoT-born attacks.

TOTAL VISIBILITY

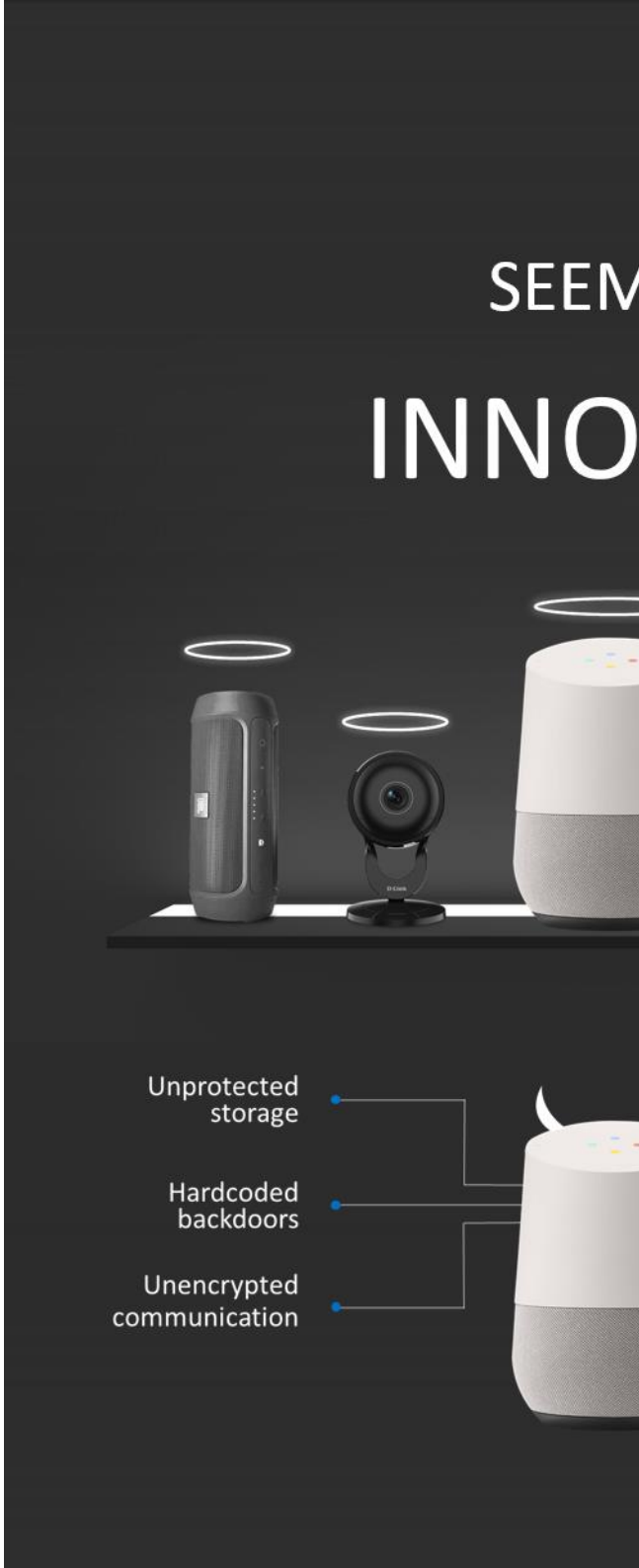
Harmony IoT analyzes your airspace 24x7 to identify and profile all smart connected devices in and around your environment. With HARMONY IoT, you get continuous insights into what each device IS doing and what SHOULD BE doing.

PROACTIVE THREAT DETECTION

HARMONY IoT produces high fidelity alerts, with its unique data science approach that combines positive and negative security models, that accurately identify all the threats and vulnerabilities created by them smart connected devices active in your environment.

REALTIME ATTACK MITIGATION

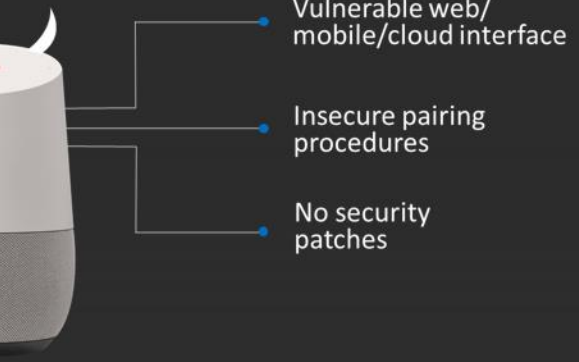
HARMONY IoT takes precise actions to neutralize malicious IoT activity, in real-time, to protect the integrity and privacy of your sensitive information and ongoing operations.



HARMONY IoT

IS SO

CENT



HOW HARMONY IOT WORKS

The HARMONY IoT defense is comprised of:

SMALL, NON-INTRUSIVE HARMONY IoT SMART PROTECTS

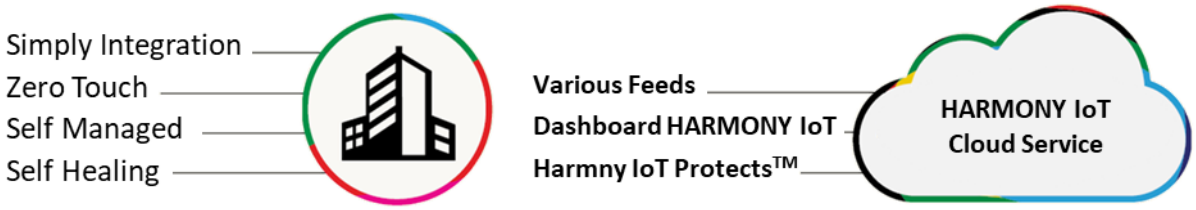
Continuously monitor the activity of all smart connected devices in your airspace and mitigates threats when identified. The Smart Protects are quick and seamless to deploy, requiring no access to your networks or assets and are completely independent, agentless, and out-of-band.

HARMONY IoT CLOUD SERVICE

Applies proprietary techniques, which combine distributed machine learning, algorithms and big data science, to identify and profile all the smart connected devices in your airspace, then pinpoint and mitigate malicious activities and threats.

INSIGHTFUL HARMONY IOT DASHBOARD

Allows you to control what goes on in your organization's airspace, with the ability to monitor activities, set policies, and react to threats.



FILL THE CYBERSECUTIY GAP

HARMONY IoT expands your defenses, allowing you to continuously monitor, control and protect against attacks from smart connected devices in your airspace to support your cybersecurity and compliance objectives.

ACHIEVE GREATER SECURITY WITH THE SAME TEAM

HARMONY IoT delivers the zero-touch, self-managed solution you need to add to your security, without having to add to your resources.

FREEDOM TO EMBRACE IOT AND WIRELESS

HARMONY IoT accelerates your digital transformation, allowing you to benefit from the use of IoT in your enterprise, with the confidence your business remains safe.

GYTPOL VALIDATOR

Validator is an endpoint threat & compliance analysis suite.

Our initial scan, finds in **90% of already secured endpoints**.
Within 2 months, our customers **reduced threats in endpoints by 45%**.

MAIN COMPONENTS

Endpoint Threat Analysis

- Discovers critical configuration vulnerabilities in endpoints;
- Identifies unprotected credentials & clear text passwords;
- Alerts local admins, unauthorized open ports, inactive anti-virus, etc., in endpoints.

Compliance & Audit

- Accurate compliance & audit status at the endpoints;
- Supports: GDPR, SOX, ISO 27001, PCI DSS, CIS, NIST, HIPAA.

Policy Validation

- Identifies Azure & OnPrem Active Directory threats;
- Intune & Group Policy discrepancies & vulnerabilities;
- Verifies Security Updates are in place;
- Enterprise wide unified Security Baseline.

Policy Validation

- Improves Start up and Login times. Correlates delays with hardware types

CROSS PLATFORM	ENVIRONMENT	OPERATIONAL
Microsoft	Group Policy	Unified Dashboard
Apple	Active Directory	Remediation
Android	Intune	SIEM Integration
Linux	Azure &OnPrem	Guides & Solutions
	Domain & Non-domain Endpoints	

Endpoint Configuration Risks | Policy Validation | Compliance & Audit | Remote Workforce Analytics | Remediation | Performance Optimization

gytpol
eyes on policy

DATOR
guration Security
y & Compliance

Validator is an Endpoint Configuration Security (ECS) analysis suite used for IT Security and Compliance. It detects security issues and vulnerabilities caused through policy configuration flaws or missing best practices. Once detected, Validator remediates the issue, keeping your Endpoints safe and compliant.

VALIDATOR MODULES

Endpoint Configuration Risks

Discovers critical configuration risks in endpoints. Identifies unprotected credentials & clear text passwords. Alerts local admins, unauthorized open ports, inactive anti-virus etc. in endpoints.

Policy Validation

Identifies Active Directory threats. Intune & Group Policy discrepancies & vulnerabilities. Verifies OS Security Updates.

Remediation

Remediation actions allowing issues to be fixed quickly and accurately without risk. Trusted knowledge you can rely on.

Endpoint Performance Optimization

Improves Start-up and Login times. Correlates delays with hardware types.

Remote Workfoce Analytics

Maintain visibility on employees working from home even if they are not connected to the network by VPN.

Compliance & Audit

Major compliance standards supported including GDPR, ISO 27001, NIST, CIS, SOX, PCI DSS, HIPAA. Create and customize your own internal audit rules for validation.

REMOTE WORKFORCE CYBER ATTACK?
IT'S NOT "IF", BUT "WHEN".

Employees working from home are more vulnerable and exposed to hackers compared to those working in the office.

IT & SecOps in organizations feel exposed due to the lack of visibility of remote endpoints and hence successful cyber-attacks are inevitable.
Validator delivers the visibility required by IT & SecOps. Provides continuous identification and self-remediation.
Does not require a VPN Connection.

BITDAM

The only solution stopping unknown content-borne threats at first sight.

Protects enterprise email, cloud drives and instant messaging from malicious files and links.
Ransomware | Malware | Phishing | Data Breach

>20% of unknown content-borne attacks go undetected.

Leading security products such as Office 365 ATP and G Suite Enterprise miss 20-40% of the unknown content-borne threats during the first 24-48 hours. Secure Email Gateway, Sandboxing, and other cyber security solutions turn ineffective as attackers use automation to constantly create unknown variants of malware.
Despite the significant investments made by organizations to protect their Email, Cloud Drives, and Instant Messaging against malicious files and links, they are still exposed to unknown cyber threats delivered on a daily basis.
Traditional protection is no longer sufficient. A new approach is needed to meet the full range of cyber threats contained in any type of file or URL.

STOP UNKNOWN THREATS.

BitDam stops known and unknown content-borne threats contained in any type of file or URL at their source, pre-delivery, blocking malware without hurting end users' experience.

UNMATCHED DETECTION RATES.

BitDam's detection rates of advanced threats are 10X higher than current solutions, covering malware of all types, including hardware and logical exploits, N-Day and Zero-Day attacks.

FOREVER PROTECTED APPLICATIONS.

Exposure to malware, even while waiting for the next security update, may be devastating. BitDam stops content-borne threats for both known and unknown vulnerabilities from the first sight, making response time irrelevant. No more security updates and patches. No more exposure to malware.

MAKE ALL CHANNELS SAFE TO CLICK.

BitDam secures content across all enterprise collaboration channels - email services by any vendor, cloud storage and file sharing services, instant messaging and more - all in one place.

EMAIL

Secure Microsoft Office 365, G-Suite or any other e-mail service to protect your employees from malicious emails.

CLOUD STORAGE AND FILE SHARING

Protect Microsoft OneDrive, SharePoint, Google Drive, Dropbox, Box or any other cloud drive, to ensure that end users access only legit files.

CHAT AND INSTANT MESSAGING

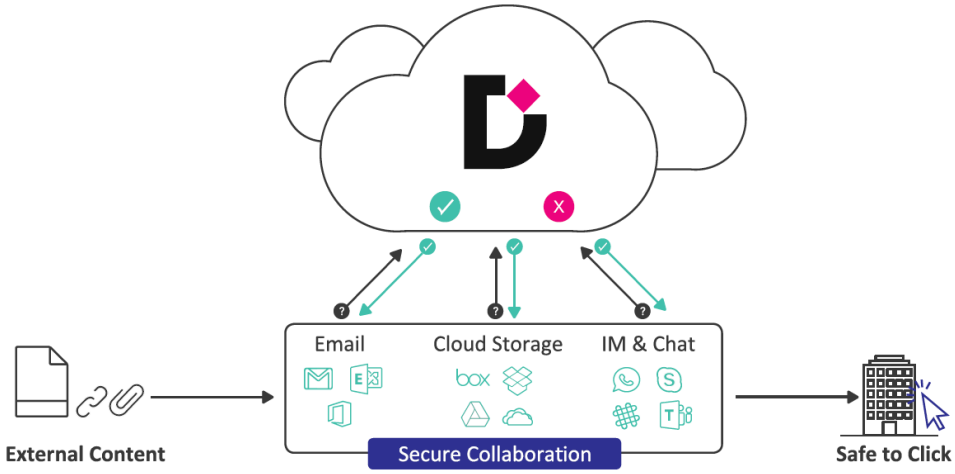
Make your enterprise Instant Messaging a safe zone using BitDam for Slack, Skype, Teams, Zoom and other chat platforms.

BitDam

alware and
missed by all

and instant messaging from

BITDAM PROTECTS ALL YOUR COLLABORATION CHANNELS IN ONE PLACE.



DEPLOYED WITHIN MINUTES.

BitDam solutions are cloud ready and easily integrate with any security solution, collaboration channel, email and chat provider, through a simple set of APIs.
Deployed outside of your network, it requires no changes to existing security infrastructure, policies, or processes, allowing rapid and smooth rollout.
Set-up takes just a few minutes thanks to built-in integration with Office 365, G-Suite, DropBox, OneDrive, Slack and others.
The BitDam Dashboard makes day-to-day operations fluent and intuitive, helping SOC teams to view, monitor and investigate malware with a click.

FOCUS ON LEGIT APPLICATIONS.

Instead of chasing previous and ever-evolving cyber threats, BitDam focuses on how your business applications should behave, thereby detecting when they are being exploited.

All enterprise applications protected

BitDam covers all standard business applications. It protects against advanced attacks aimed at MS office files, pdf, ics, zip, and rar files, as well as website links.

CPU-level application learning, alien code detection

BitDam knowledge base maps application code paths and legitimate run time operations. Full visibility of CPU level data enables detection and blocking of alien code flows, evasive techniques and threats, at their source.

100% attack-agnostic

Independent of past knowledge, BitDam is attack-agnostic by nature.
As such, it blocks malicious files and links regardless of the specific attack or manipulation they may contain.

MINEREYE DATA TRACKER

Govern your information anywhere

With MinerEye Data Tracker™, you can automatically discover and monitor your precious company and customer data wherever it is, whether it's within the organization or out in the cloud.

ILLUMINATE YOUR FILES WITH MINEREYE DATA TRACKERTM

The MinerEye Data Tracker™ is based on Interpretive AI™ technology and uses a three-step automated process to identify sensitive data by its essence: identification, classification and tracking.

BUILT FOR COMPLIANCE

Nothing escapes MinerEye

The MinerEye Data Tracker™ was designed specifically to support compliance scenarios – it allows you a single interface for tracking data usage violations wherever they occur, keeping you covered at all times.

POWERED BY INTERPRETIVE AI™

MinerEye's Interpretive AI™ Technology uses computer vision and machine learning to crawl, identify, and classify all company data. Going down to the pixel level, it generates "fingerprints" of the data, creating a learning process for content optimization.

Granular Classification.

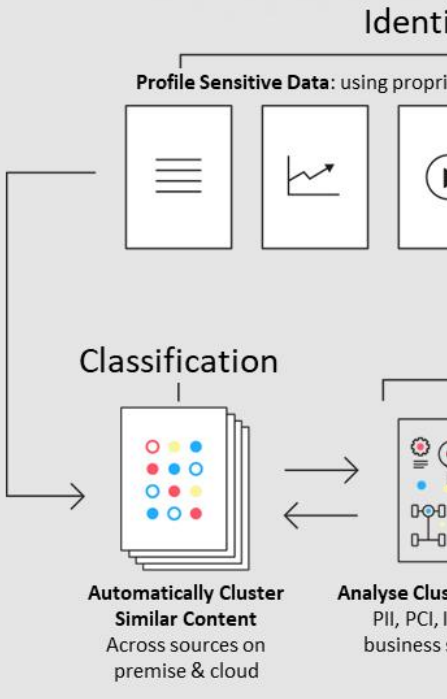
MinerEye's Interpretive AI™ Technology goes deep into any file at the pixel and byte level for the most accurate classification, ensuring nothing is missed.

Artificial Intelligence

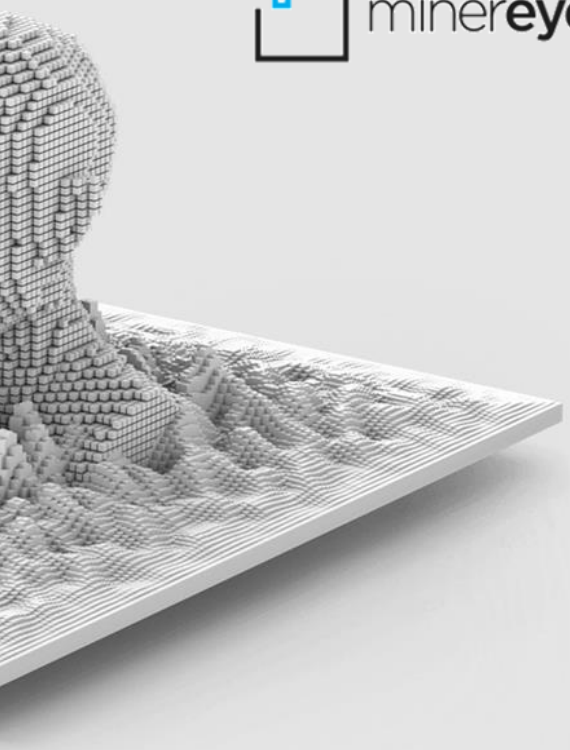
Information security teams only need to train the system once with example files and strings to continuously track data. Say goodbye to tedious dictionary regex, creating rules, and maintenance.

Any Data in Any Form

Locate and identify data within most file formats and file types. MinerEye illuminates "dark data" for a comprehensive coverage that supports the full protection of intellectual property.



minereye



ification

etary computer vision technology

Tracking

DLP DAM IRM SIEM PIM

sters Essence
P, ROT &
sensitivity

Trigger Security System & Compliance
Azure information protection, O365

Automated Process

MinerEye uses AI to automatically learn, discover, map, track, and trigger sensitive data protection.

Built for Scale

MinerEye scans enormous amounts of data, in minimal time - up to 1TB per hour.

Seamless Integration

MinerEye is designed for fast integration with existing tools and ecosystems, such as Office365, DLP, Access control, and SIEM systems.

Index Data

MinerEye's Interpretive AI™ Technology accelerates the search, discovery, and analysis of unstructured data.

Data Minimization

Data retention policies can be easily established and enforced to limit data.

PRODUCT BENEFITS:

- Profiles and matches data patterns using only the bytes of a file
- Auto Classify and track all unstructured sensitive data anywhere
- Detect outlier and abnormal data behavior
- Ability to scan large amounts of data
- Lower OPEX by leveraging machine learning to eliminate the need of implementing rules and regular expressions
- Helps limit personal data collection, storage, and usage to data that is relevant
- Reports on sharing violation without compromising personal information
- Trigger Data Protection system with similar data locations report

MINEREYE APPLIES ARTIFICIAL INTELLIGENCE AND RESHAPES INFORMATION GOVERNANCE & DATA PRIVACY COMPLIANCE OVER BIG DATA REPOSITORIES & SCATTERED SOURCES

Technologically Neutral

Categorizes data at 1 TB/ Does not depend on human actions or definitions, but leverages Artificial Intelligence to learn, discover, continuously map, track, and triggers personal data protection hr.

Right of Access

Continuously tracks and reports on personal data based on multiple identifiers that enable quick and easy access by category/data subject.

Genetic Data

Uses byte-level analysis to find and match genetic data to natural persons.

Time Limits

Identifies all data and tracks its origin and lifecycle for rectification of inaccuracies and timely deletion, and periodic review.

Resilience

Continuously scans vast volumes of data for PII, restoring classifications and protections even after incidents.

PII Categories

Rapidly identifies and automatically enforces established categories of personal data.

Impact Assessment

Enables fast and simple impact assessment over large volumes of data without necessitating subject matter expertise.

Protection & Rectification

Continuously scans and finds where data resides and has changed, enabling erasure of extraneous data minimization and pseudonymization.

Data Transfers

Data segregation capabilities enable automatic data tracking across geographic boundaries.

FIRSTPOINT MOBILE GUARD

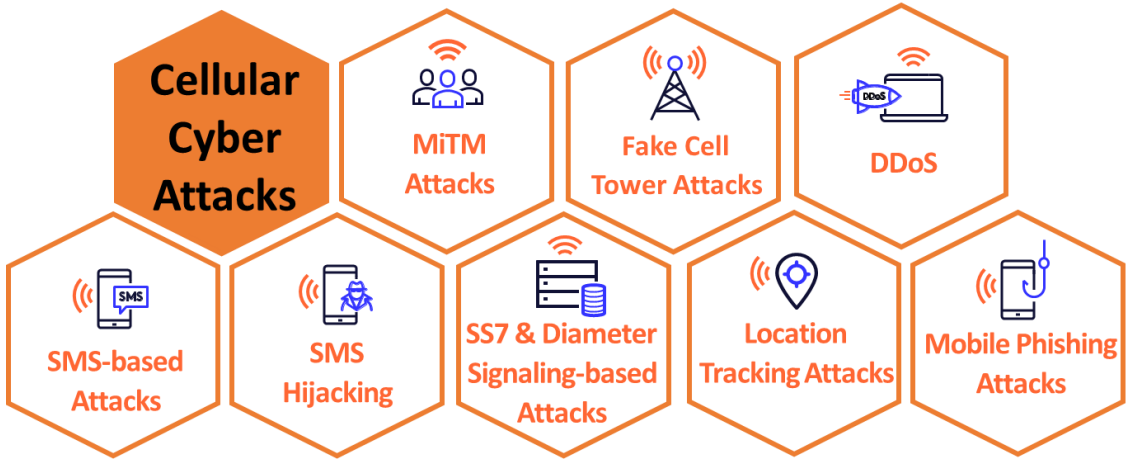
Deceive hidden attackers by keeping cellular identities private, on any device, anywhere

Cellular devices now outnumber the world population by **about 19%.**
The overwhelming popularity of cellular devices demonstrates that cellular devices are probably the most important cog in the digital transformation machine taking over the world.

However, even though cellular devices deliver technology to even the most remote corner of the world, they also introduce new cyber security risks and vulnerabilities. In fact, the speed of mobile connectivity growth **and adoption of cellular connectivity for crucial communication** has been nearly matched by the speed of new mobile cyber security vulnerabilities.

Mobile network operators (MNOs), as well as enterprises concerned with data safety, are discovering that they must hurry to catch up with the pace of technology and the cyber-attacks that follow. We can expect to see a direct correlation between the growing popularity and increased reliance on connected devices, and an increase in the number and quality of mobile cyber-attacks.
To stay ahead of present and future attacks, there is a growing need for a solution that continuously protects against network-based cyber-attacks on the almost infinite number of cellular devices. I expect to see network based cyber security solutions, like FirstPoint, adopted by every MNO and cellular IoT network in the coming years.

Cybercriminals are now taking a mobile-first approach to hacking the enterprise



Mitigat
cellular cyber
on connected d

Targeted solution for telec

With 3G, 4G and 5G networks still vulnerable to such damaging attacks as fake cell towers (IMSI catchers), MiTM and location tracking, organizations are challenged to protect their cellular networks. Other solutions mainly provide protection against data leakage and do not have any visibility into cellular attack vectors.

The most effective way to protect cellular network and data leakage protection is a full, proven, network-based solution that is agnostic to the device type, future generation technologies and hacker tactics.

	IMSI catchers	Network loopholes	Malicious SMS	Malware	Device Types
FirstPoint	✓	✓	✓	✓	ALL
Secured hardware on device	✗	✗	✗	✓	Limited
Cloud-based solutions	✗	✗	✗	✓	ALL
Security SW on-device	✗	✗	✗	✓	Limited
SS7/SMS firewalls	✗	✓	✓	✗	ALL
Network-based data protection	✗	✗	✗	✓	ALL

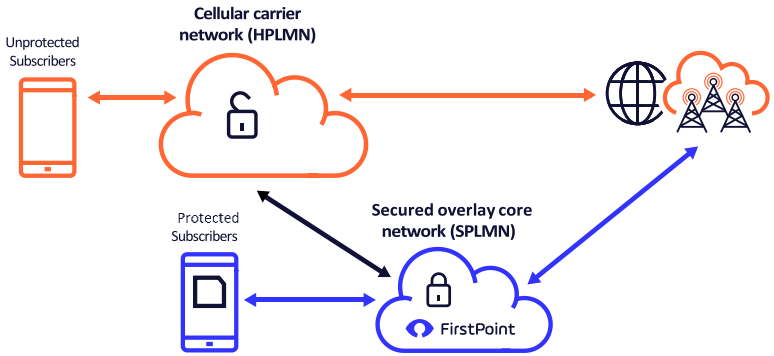
FirstPoint offers a seamless platform that covers all cellular device threats on any SIM/eSIM-based device. This mobile network solution identifies, alerts and protects against any hidden cellular network risks to connected devices; e.g., IMSI catcher detectors, network loopholes, malicious SMS, malware, SMS hijacking and location tracking. The platform delivers continuous, updated, network-based security anywhere, on any device – even when users roam.

Management can specify security by policy, scenario, location or custom grouping and can monitor all devices from one dashboard.

Users enjoy a consistent, secure experience: no hardware, software or updates to install, no slowdowns and no battery/performance impact.

The platform comprises:

- A secured overlay core network, which is operated side-by-side with the MNO's original core network;
- A dedicated applet, installed on the protected device's SIM;
- Communication routing through the secure environment;
- Novel security measures;



DIGITAL ID PROTECTION

Europe based certificate authority

THE CHALLENGE

The protection of digital identity and data must be protected from a European datacenter (GDPR). It is vital to strengthen the idea of European sovereignty in information technology, so it is necessary to be able to offer strong solutions as an alternative to Japanese, Chinese and American Certificate Authorities (CA).

THE SOLUTION

This unique platform brings together world-class, exclusively European CAs.
With our SSL / TLS certificate offerings, including the 100% European QWAC, our eIDAS certified e-signature and eIDAS server signature solutions, our e-mail protection services with the S/MIME protocol, our integrated MPKI certificate management tool and our packages for small and medium-sized companies. BlueCerts brings you a clear answer concerning the protection of your digital ID and your dematerialized data.

BLUE SSL CERTIFICATES

BLUE QWAC PSD2

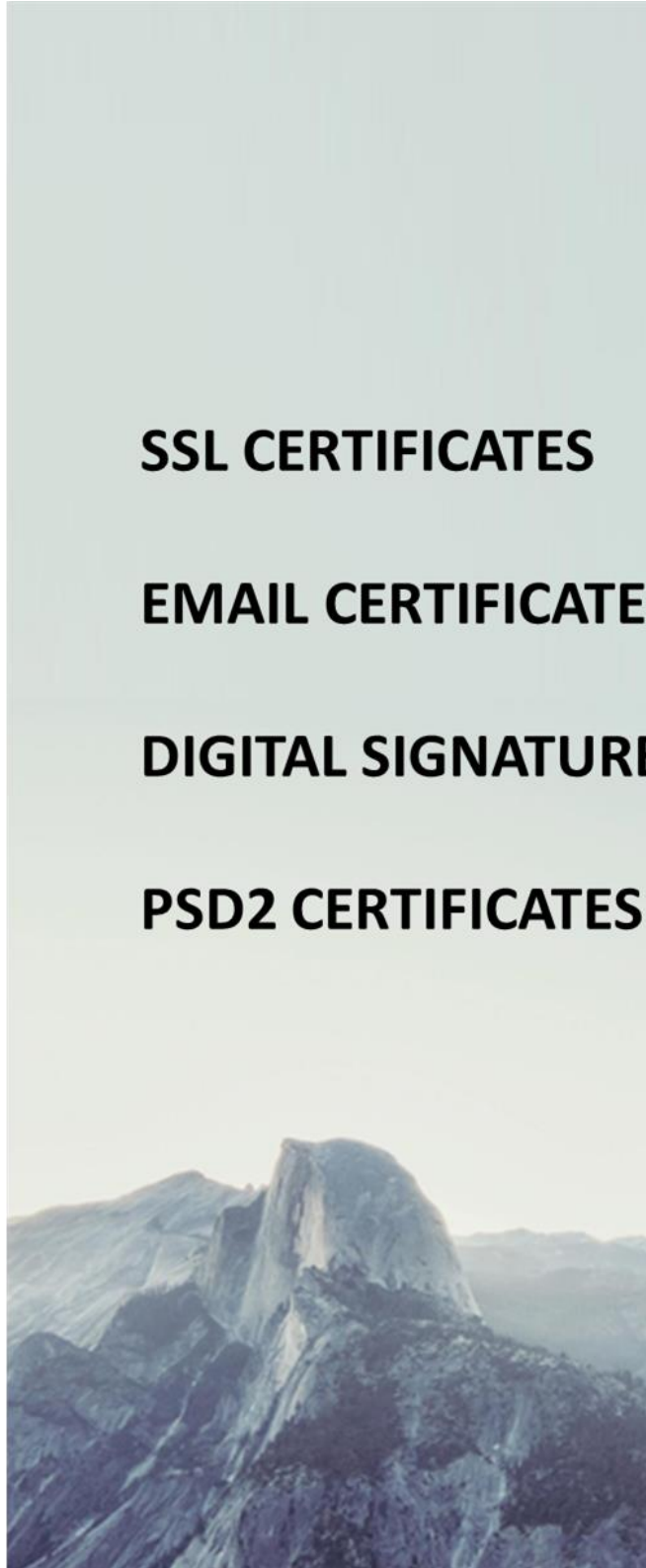
BLUE DIGITAL SIGNATURE

BLUE eIDAS SIGNATURE

BLUE eIDAS SIGNATURE

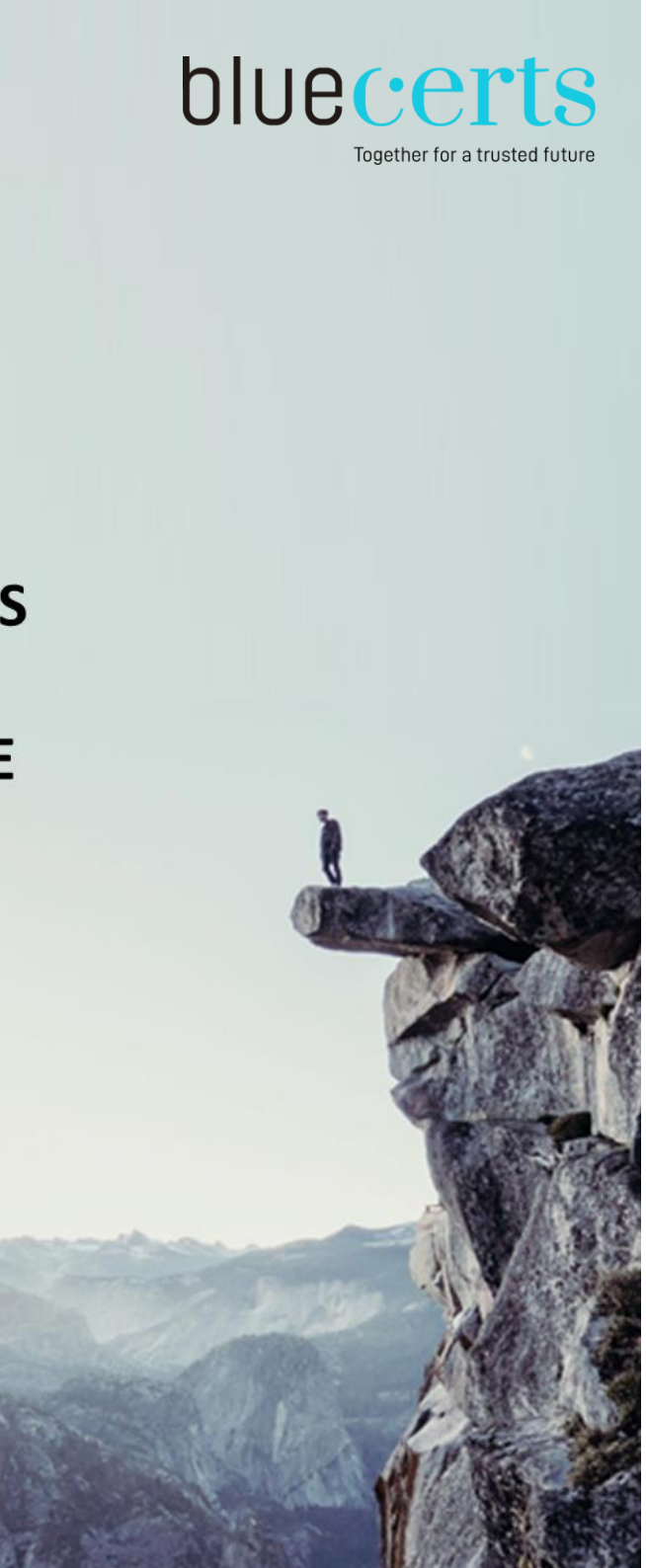
BLUE PKI MANAGEMENT

DOMAIN REGISTRATION



bluecerts

Together for a trusted future



SLL CERTIFICATES

SSL certificates protect your servers and your websites due to confidential data being encrypted during transmission over TLS. These certificates also contain trusted information about the certificate owner and thus confirm the identity of the website or server operator thus, guaranteeing the trust of your customer. They also increase the visibility of your website because Google's ranking assigns websites with SSL / TLS encryption a much higher level than websites without SSL.

Depending on the type of certificate (DV, OV, EV), different characteristics of the owner of the certificate are verified SSL certificates provide protection against phishing and man-in-the-middle attacks.

All Certificates are encrypted with RSA 2048 bits keys and are using SHA-2 256 bits hash algorithms.

EV Certificates – This certificate is the right solution for critical web applications or e-commerce.

OV Certificates – This certificate is appropriate for standard corporate websites in order to validate the organization.

DV Certificates – This certificate with domain validation is the right choice wherever internal communication needs to be encrypted.

WildCard Certificates – This certificate is used if you want to secure an unlimited number of subdomains on a single certificate.

QWAC PSD2 – represents a mix between an EV SSL certificate conforming to the CA / B Forum and fields specific to PSPs (Payment Service Provider) according to the Payment Services Directive (PSD2).

ELECTRONIC SIGNATURES

With the electronic signatures you can authenticate the signer of the document, time stamp the document (guarantee the time and date of the signature), guarantee the integrity of the document (cannot be physically modified) or simply sign the documents and give them legal value.

BLUE EIDAS SIGNATURE - is a signature certificate for a natural person in accordance with European regulations which define the rules of trust for international digital exchanges between member states of the European Union. It has the same value as a signature on your behalf or the organization. With smartcard support.

BLUE TIME STAMPING - Companies can ensure, through the use of time stamps, the legal validity and compliance of their electronic documents. It provides a mechanism to prove that the digital certificate was valid at the time of its use.

BLUE STAMP EIDAS SERVER – A signature certificate for a legal person (company or organization) in accordance with European regulations which define the rules of trust for international digital exchanges between EU state members.

PKI MANAGEMENT

Issue your own certificates, approve, manage and withdraw certificate requests yourself for your employees, customers and partners within a matter of minutes whatever the time of day.