DIGITALSKILLS®
CYBERSECURITY SOLUTIONS
OFFICIAL DISTRIBUTOR IN PORTUGAL

2022

CYBER SECURITY SOLUTIONS

INNOTECH®

DIGITALSKILLS & INNOTECH SOLUTIONS | 2022

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 other 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 a 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 cyber security 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 in our company 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 and InnoTech have the solutions, skills 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.

INNOTECH®

Avenida 5 de Outubro, 124, 2º Piso
1050-061 Lisboa

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

DIGITALSKILLS®
OFFICIAL DISTRIBUTOR IN PORTUGAL

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

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

DATTO (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.

DATTO 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.

Datto'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. Datto 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.

Datto 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, Share-Point, 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 Datto for Slack, Skype, Teams, Zoom and other chat platforms.

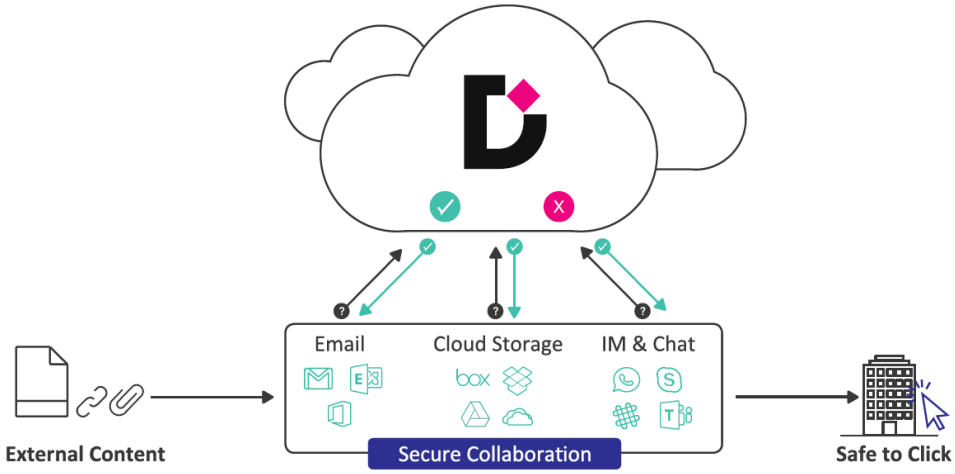
E-MAIL & COLLABORATIVE PLATFORMS PROTECTION

datto
(formerly BitDam)

ops malware and
ttacks missed by all

cloud drives and instant messaging from

DATTO PROTECTS ALL YOUR COLLABORATION CHANNELS IN ONE PLACE.



DEPLOYED WITHIN MINUTES.

DATTO 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 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, Datto focuses on how your business applications should behave, thereby detecting when they are being exploited.

All enterprise applications protected

Datto 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

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

DEVICE TOTAL

DeviceTotal by ArcusTeam is a complete attack surface management platform for connected devices that evolves faster than the everchanging cyber risks that threaten your network.

PROTECT YOUR ENTERPRISE FROM THREATS BY AUTOMATICALLY MONITORING YOUR ATTACK SURFACE FOR CONNECTED DEVICES.

Enterprises like yours are becoming increasingly reliant on connected devices. All of these connected devices and their firmware and software act as open doors for cyber-attacks – leading to an ever-evolving attack surface that's difficult to manage and control.

As a result, your CISOs and security teams are dealing with multiple challenges as they try to manage an ever-evolving attack surface and protect your organization from cyber-attacks.

SECURE YOUR ENTERPRISE FROM THREATS YOU DIDN'T EVEN KNOW IT'S EXPOSED TO:

CENTRALIZES
Manage one single unbiased platform and monitor your whole attack surface from anywhere in the world.

AGENTLESS
Benefit from zero-intrusion, with no need for hardware or software installation and no network scanning.

TRANSPARENT
Benefit from zero-intrusion, with no need for hardware or software installation and no network scanning.

PROACTIVE
Gain insight into new device vulnerabilities, including brand-new threats and attack patterns.

CONTINUOUS
Continuously identify exploitable vulnerabilities on each device with no false positives.

CONTEXTUAL
Analyze cyber-threats in relation to your business operations, with an accurate risk-level down to a single device.

COST-EFFECTIVE
Reduce your attack surface management workload by 70%, and stop worrying about the skills gap.

ATTACK AND RISK SURFACE MANAGEMENT IN IOT DEVICES

ATTACK SURFACE M
CONNECTE

Ready to get proactiv
of your conne

ArcusTeam

MANAGEMENT FOR ED DEVICES

ve about the security cted devices?

BENEFIT FROM AUTOMATED ENTERPRISE DEVICE SECURITY IN 4 SIMPLE STEPS

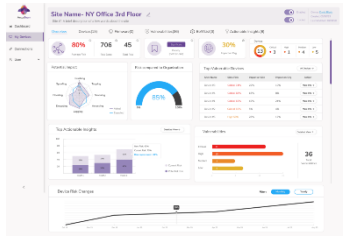
1. **DISCOVER**
Identify all connected devices in your network, together with their location, hardware, firmware, software, and BOM list of components.

2. **ANALYZE**
Discover all known and unknown vulnerabilities for every connected device and its components, including risk score, and status.

3. **MITIGATE**
Discover all known and unknown vulnerabilities for every connected device and its components, including risk score, and status.

4. **CONTROL**
Prioritize response based on business context, risk level, impact, and more, and monitor the effect of your actions continuously.

MANAGE YOUR ATTACK SURFACE ON 3 DIFFERENT LEVELS



DEVICE LEVEL - Dive into each individual device's most pressing vulnerabilities and actionable insights you can use to remediate them, and see how each device impacts the site it is located in and your organization as a whole.

SITE LEVEL - Get full control over the security of your organization's sites. Manage your attack surface by gaining security insights into each individual site; including the breakdown of vulnerabilities in that site, the site's contribution to the organization's overall risk level, and actionable insights for remediation.

ORGANIZATION LEVEL - In one clear view, you can get complete control over the security of your organization. Using consistently updated charts of top vulnerable sites and devices in your enterprise, your security teams can get to work on the most pressing matters and protect your organization from attack.

THE TECHNOLOGY BEHIND DEVICETOTAL

NUCLEON DETECTION & RESPONSE

Endpoint Detection, Response and Remediation Platform.

COMPREHENSIVE CYBER THREAT PROTECTION APPROACH

Nucleon Detection & Response platform ensures the protection of workstations and servers by implementing successive layers of protection to protect you during all phases of an attacks. Nucleon Detection & Response allows the identification of weak points on your infrastructures, blocks attacks and provides you with all the tools to investigate.

A REAL TAILORED PROTECTION OF BUSINESS DATA

Nucleon Detection & Response absorbs your organization's specific business uses, identifies your critical data, then automatically creates specific protection rules. These rules will protect your critical data against illegitimate access, leakage or blockage.

IDENTIFICATION AND BLOCKAGE OF MALICIOUS BEHAVIOR

Multi-Layer Zero-Trust policies block attacks techniques used by hackers on different levels:
At a system level, the protection rules will focus for example on the protection of sensitive administration scripts and tools in order to prevent complex infection like "fileless" attacks.
At a network level, the protection rules will restrict internet access to avoid data exfiltration. For example, the Microsoft Office suite only has access to the servers and domains it needs to function normally.
Many attack processes are based on malicious macros by abusing users, which is why Office Suite files are scanned before being opened.

THE EASIEST WAY TO INVESTIGATE

All the tools needed to identify the root cause of an attack or to follow a suspicious behavior are made available at the centralized management console. It is simpler now to understand the execution flow of malware or your own software.

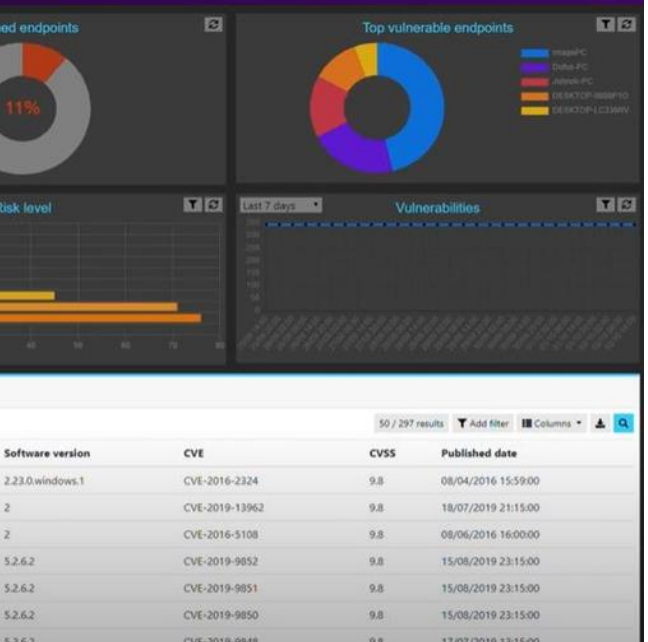
REMEDIATION, ISOLATION AND ROLLBACK

If the data is altered or compromised by malicious software, or simply by a user's inadvertence, it can be restored from the administration console. This functionality will always provide a solution in case of a cybersecurity incident and it is natively available with no need to install any additional components.
In case of suspicious behavior, the machine(s) can be remotely isolated from the network to prevent any additional damage. The remediation features allows a complete cleaning of the system that delete all the files created by the attack vector.

REMOTE ACTIONS

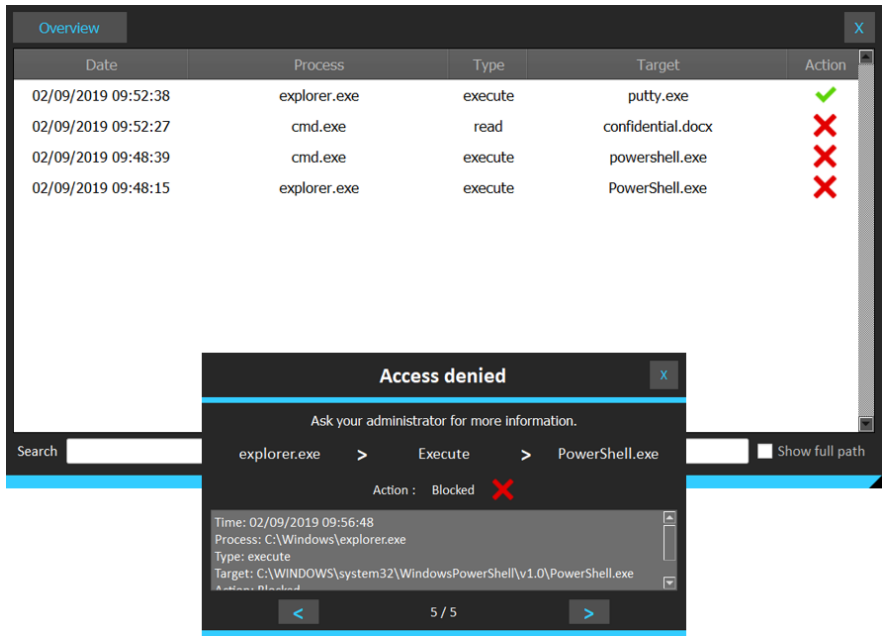
The administration console allows remote commands to be launched on one or more machines. These features facilitate investigation and incident response.

EPP ZERO TRUST WITH ROLLBACK FEATURES



GLOBAL COVERAGE AGAINST CYBER THREATS

✓Vulnerability management
✓Workstations and servers hardening
✓Protection against known and unknown Malware/Ransomware
✓Investigation tools
✓Removable devices control
✓Protection against malicious Word / Excel
✓Smart Scan
✓Protection against network attacks
✓Resources management
✓Cloud Storage Control (One drive, Box, Google Drive, etc.)
✓Remediation tools
✓Rollback of altered or compromised files
✓Remote actions (distant shell)



BENEFITS

- Complete and simplified protection using Zero-Trust policies
- Real-time visibility of system and network activities
- A purified and light agent which does not affect the production and the daily life of the users
- Centralized console
- Easy deployment
- Cloud or On-premise deployment
- Personal data compliance

PERFORMANCES

- Extremely lightweight agent:
  1% < CPU
  100Mo < RAM

GDPR COMPLIANCE

Records of processing activities; Native pseudonymization and anonymization; Stored data Encryption

SKURIO

A different approach to Cybersecurity.

It is no longer necessary for bad actors and criminals to attack your network in order to get hold of your critical business data. Whether it's a carefully constructed Magecart exploit or simply a disgruntled employee posing an insider threat - your data can end up being shared or sold on the shady parts of the Internet which are invisible to your internal security systems. Looking for your data outside your firewall in a safe and automated way is the next step on your journey to Cybersecurity maturity.

Digital protection of your data no longer resides purely inside your firewall. Your business faces risk from cyber-attack, insider threat, human error, 3rd party breaches and more. To understand this, you need to look outside your perimeter.
Skurio solutions continuously monitor the surface, deep and Dark Web to provide the illumination you need to see this Digital Risk and respond.

PLATFORM FEATURES

BreachAlert

- Eliminate false positives and reduce noise by searching for your specific content.
- Create simple or complex targeted alerts to search for your business and customer data using keywords, email domains, login credentials, IP Addresses, email addresses and account numbers.
- Access years of breach information and data in our unique, compiled, historical database.
- Monitor surface, deep and Dark Web sources for your data 24x7; including Social Media, IRC chatrooms and text repository sites like Pastebin.
- Be notified of threats or breaches appearing outside your perimeter by SMS, email, Slack or API, within minutes of your data appearing anywhere it shouldn't.
- Reduce impact and cost with faster breach detection through automation; saving time and effort.
- Collaborate and improve productivity by setting up custom folders, managing response statuses and collating comments.

BreachResponse

- Use powerful BreachAlert API connectivity to integrate breach alert details into SIEM systems, ITSM and other IT applications.
- Customize workflows and automate your response to data breaches efficiently.
- Remove false positives and identify high-risk user credential breaches to active accounts quickly by understanding the types of users affected.
- Gain insights into employee sign-ups to breached 3rd party services and password hygiene.
- Improve cyber policies and target educational opportunities pro-actively.
- Improve your SOC productivity through intelligent automation and give your threat analysts space and time to focus on high-risk threats.

PROTECTION AGAINST INFORMATION LEAKS & ATTACKS VIA DARK AND DEEP WEB

SKURIO

Protection Platform

Threat Intelligence

BreachMarker

Easily watermark your data to detect breaches across your data supply chain

Cyber Threat Intelligence

Identify intelligence sources, investigate threats, process incidents and disseminate results

ns, with high levels of automation

deploy and easy to integrate

y Skurio's Threat Analysts

BreachMarker

- Watermark your data to detect breaches across your data supply chain by easily creating synthetic identities with automated set up of monitored mailboxes.
- Detect breaches from 3rd party or partner systems and identify where they took place using your synthetic identities.
- Use simple keyword configuration to remove false positives and approve trusted sources.
- Prevent data breaches from becoming full-scale cyber-attacks; reducing risk and cost.

Cyber Threat Intelligence

- Skurio features Cyber Threat Intelligence tools to broaden your threat detection surface with social and surface web feeds.
- 'Scraped' social sources collects useful information from sites including Reddit and Telegram.
- This provides a valuable historic database for use in investigations as well as alerts of data or mentions of the company's brand, products, senior executives and more.
- 'Queried' social sources extends coverage even wider into a range of popular social media platforms to bring back items which are relevant to the company.
- The Insights feature helps you analyze and filter thousands of messages in a single screen, quickly identify threats and eliminate noise from your investigation.

KEY FEATURES

Configurable alerts

Configure alerts quickly and simply for any data important to your business; from domains and email addresses, through to customer data or network infrastructure details. Set up pattern matching searches to find proprietary information like contract numbers or SKUs. BreachAlert scans the surface, deep and Dark Web for any of your data that shouldn't be there; around the clock. Get instant alerts when something is found and use contextual information to respond and reduce your Digital Risk.

Collaboration

Define your own folders so you can manage alerts and keep track of threats. Assign messages to colleagues and track their status. Add your own notes and comments so that your team are up to date with any useful information you have uncovered. Use our range of API features to pass alerts into your security operations center applications so they can be acted on sooner. Integrations can enable you to define your own response processes and automate further notifications and actions.

Clear insights

Search through results to find similarities or patterns using details like author, date ranges, URL etc.
Use advanced search filters to easily cut through the noise to get to the information that's most important to you.
Use CTI features to filter high volume channels on social and surface apps and sites; then investigate threats with greater precision.

Keep customers safe

Use BreachMarker synthetic identities to mark the data sets you share with your partners and channels. Get instant notifications if your data is found where it shouldn't be and early warnings from attempts to email BreachMarkers.
Pinpoint the source of 3rd party breaches quickly and efficiently. Automatically compare hashed customer data with data dumps to check for correlation and identify breaches of your data.

DEEP INSTINCT

Deep learning. The most advanced form of AI.

By using deep learning, we are able to predict and prevent any kind of threat – known and unknown – anywhere in zero-time. Every endpoint, server, mobile device, network and operating system is protected against any type of attack, be it fileless or file-based. This advanced approach to threat prevention ensures that attacks are identified and blocked before any damage can be caused.

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose-built, deep learning cybersecurity framework.

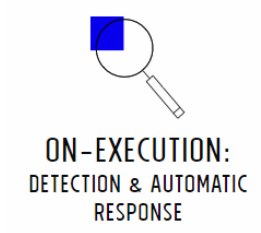
Deep learning is the most advanced form of AI-based threat protection available today—allowing Deep Instinct to predict and prevent cyber-attacks before they happen and protecting well beyond traditional AV or machine learning-based solutions.

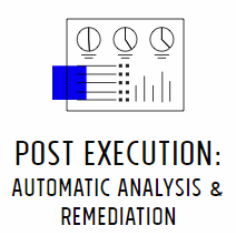
Powered by a deep neural network brain that mimics the logic and learning of the human brain, the Deep Instinct Prevention Platform anticipates and prevents attacks with unmatched speed and accuracy. We stop malware before it executes, identifying malicious files in <20ms with 99% accuracy to prevent attacks pre-execution.

To stay ahead of the latest threats and to prevent unknown threats, the predictive power of a deep learning-based solution is a necessity.

Deep Instinct provides full protection, based on a prediction and prevention-first approach, followed by detection and response. The solution offers unmatched efficacy in predicting zero-day threats and can identify unusual, suspicious, and malicious malware on the endpoint, preventing threats as they happen.

It uses the following multiple layers:





Deep Static Analysis

D-Client predicts and prevents any malicious file upon the file's initial access on the device, and can also perform a full file scan during the initial installation or on-demand. It can be configured to prevent or detect malicious files, using different thresholds adapted to the organization's needs.

D-Cloud File Reputation

Additional layer of endpoint protection based on file reputation, both for known malicious and benign files.

XDR THAT BLOCKS RANSOMWARE DURING ITS PRE-EXECUTION PHASE

Script Control
A compliance and policy infrastructure to eliminate the script-based attack surface, including PowerShell, JavaScript, VBScript, Macros, HTML applications, rundll32, and many more.

Blacklisting
Files can be blacklisted based on hashes, based on IoC's, and based on import IoC lists.

Deep Behavioral Analysis
Behavioral analysis capabilities can detect and stop malicious business logic malware, including ransomware, remote code injection, and known payloads for system endpoint protection.

Deep Classification
Rapid classification of malware (known and unknown) in real-time, with no human involvement, into seven different malware types, using our unique deep learning malware classification module for endpoint security.

Attach Chain
Root-Cause Analysis to describe the process chain that led to the event.

Advanced Threat Analysis
A set of tools that perform advanced analysis on threats found within the organization. This includes static analysis, sandboxing analysis, screenshots and network dumps of the threats. Integration with MITRE ATT&CK identifiers in support of threat hunting.

REMEDIATION
Quarantine files: Quarantine malicious files during their prevention.
Whitelist: Whitelist files detected falsely as malicious based on hash, certificate and/or path. The ability to import a list of IoCs based on hashes is also available.
Delete files remotely: Detected files that were not prevented and quarantined can be deleted remotely from the endpoint.
Terminate running process: Files thar were detected as malicious and processes that were detected behaving maliciously can be terminated remotely.
Isolate device from the network: Devices that pose a risk to the organization can be isolated remotely.

CYNET 360

The world's first autonomous breach protection platform.

Consolidates and automates Monitoring & Control, Attack Prevention & Detection, and Response Orchestration across the entire environment. Cynet 360 delivers these capabilities by pioneering the use of Cynet Sensor Fusion™ to continuously collect and analyze all endpoint, user, file, and network activities across the protected environment, making it the only platform capable of seeing the actual context of each activity and radically different from any siloed endpoint or network solution that monitors small parts of the overall activity, resulting in reduced accuracy and protection scope.

Through its complete threat coverage, Cynet 360 eliminates the need for complex multi-product security stacks, making robust breach protection within reach for any organization, regardless of its size and security skills.

Cynet360 is comprised of multiple layers and capabilities that allow our solution to detect and remediate advanced threats across all attack vectors.

All detected threats can be automatically remediated with no user interaction required.

Monitoring & Control

Attack Prevention & Detection

Response Orchestration

CYNET SENSOR FUSION

CONSOLIDATED COLLECTION

Continuous and active collection of activity signals from the entire environment: endpoint, network and users.

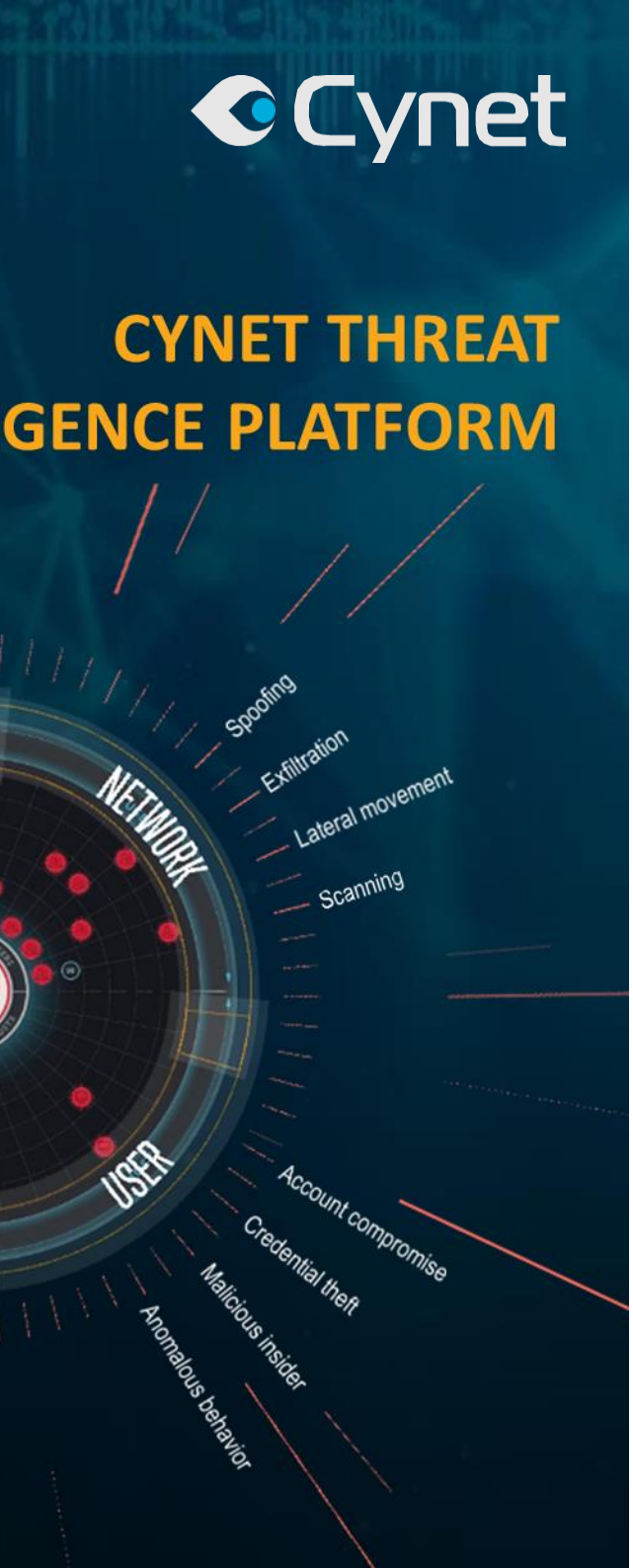
CYNET SENSOR FUSION ANALYSIS

Adaptive and integrated analysis of all signals, yielding context verdicts of unprecedented coverage and accuracy.

HIGH-PRECISION ENFORCEMENT

Leverage Cynet Sensor Fusion verdicts to automate breach protection operations: monitor, prevent, detect and respond.

XDR WITH 24/7 MDR TEAM



KEY BENEFITS

IMMEDIATE TIME TO VALUE
Cynet smart agent is fully operable within two clicks and auto-deploys itself on newly added hosts with no human intervention.

UNPARALLELED ACCURACY
Cynet Sensor Fusion collects all core activity signals gaining clear insight into the unique context of each event, reducing false positives to a minimum.

COMPLETE ATTACK-SURFACE COVERAGE
Airtight protection against all attack vectors that involve users, network files and hosts.

FULLY AUTOMATED RESPONSE
The widest set of automated response workflows to any type of attack.

INCLUDED CYOPS SOC SERVICES
Elite team of 24/7 threat analysts and security researchers.

CAPABILITIES

MONITORING & CONTROL
All the required capabilities to effectively discover and reduce exposed attack surfaces.
Cynet 360 automated collection and correlation of all activities across the environment results in deep visibility that introduces unmatched ease and agility into operations such as vulnerability management, file integrity monitoring and inventory management.

PREVENTION & DETECTION
Complete coverage of all attack vectors that involve users, network, files and hosts.
Cynet Sensor Fusion leverages its visibility into all endpoint, network and user activities in the environment to prevent and detect the widest range of attack vectors, natively achieving the core capabilities of NGAV, EDR, UBA, Network Analytics and Deception to deliver unparalleled threat coverage and accuracy.

RESPONSE ORCHESTRATION
Full automation of response workflows across the entire environment.
Cynet 360 provides the widest set of remediation actions for infected endpoints, network-controlled traffic, malicious files and compromised user accounts, as well as cross-environment operations that involve core components such as firewall, AD and others.

HARMONY PURPLE

Automated Purple team makes Operation Much Simple than it Seems

Harmony Purple is an automated blue team and red team combination to ensure that your cybersecurity controls are the most effective. Harmony Purple layers its patented attack path scenario engine on top of your existing cyber capabilities. Harmony Purple continuously analyzes your security posture to prioritize the most effective ways to minimize your cyber risks. Harmony Purple provides any size company with next-generation security tools that were previously only available to the largest companies.

RED TEAM

The automated red team feature gives you powerful discovery capabilities, plus a full view into the potential impact of each vulnerability. It includes simulated attacker activity, as well as, prioritizing how important each vulnerability is to your business.

BLUE TEAM

Utilizing data science and cyber intelligence, Harmony Purple prioritizes each threat to the organization and translates its content into an actionable security intelligence, control or compensating control.

HARMONY PURPLE

Harmony Purple sees a world where enterprises can efficiently manage current and future cyber risks across the global attack surface. Its cybersecurity risk validation platform reduces your risk by prioritizing the vulnerabilities that matter most.

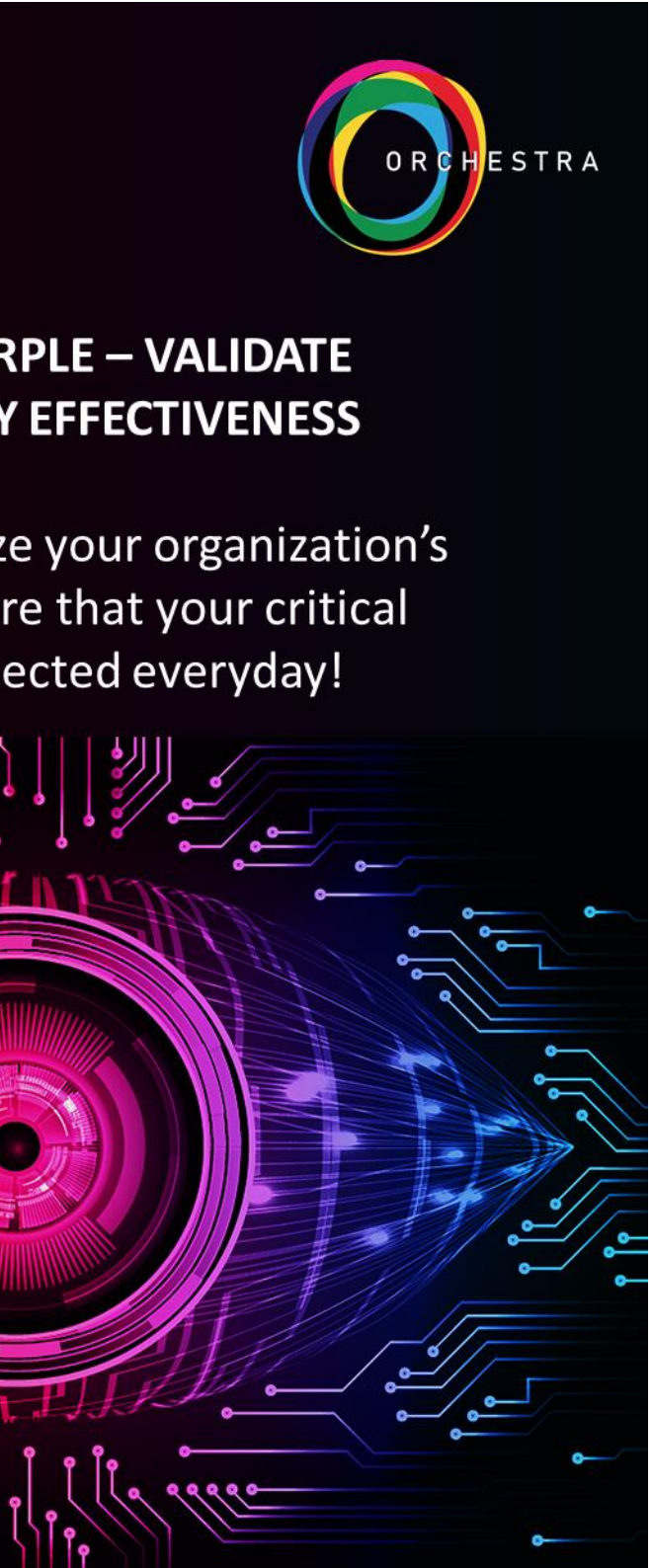
For **red teams**, they are presented with a significantly smaller list of high-risk issues to track, as compared to the number of issues that traditional vulnerability assessment tools produce.

For **blue teams**, the benefit is that they are given the most cost- and resource-effective strategy to remediate the threats presented to them by the security teams.

Harmony-Purple's automated **purple team** tool, which combines red and blue team best of breed capabilities, provides a level of continuous cyber defense previously available only to the most advanced companies. Automated purple teams put the next generation of risk-based cyber defense within everyone's reach.

HARMONY PURPLE IS LEADING THE FIELD OF RISK-BASED VULNERABILITY MANAGEMENT, ENABLING ORGANIZATIONS TO MEASURE, PRIORITIZE, AND CONTINUOUSLY PREVENT CYBER RISK.

GREY-BOX PENTESTING WITH RISK ANALYSIS



Harmony-Purple's solution is a Vulnerability Prioritization Technology (VPT) that enables organizations to assess their cyber risks based on asset criticality and advanced analytics.
The technology also allows organizations to invest its time and resources on those vulnerabilities that threaten its critical assets and business processes. Powered by Harmony-Purple's patented Attack Patch Scenario (APSTM) technology, the system creates a prioritized list of vulnerabilities.

In **comparison to traditional vulnerability assessment tools**, Harmony-Purple's uniqueness derives from its innovative combination of threat intelligence and understanding business processes. This understanding of the internal asset exposure and criticality provides a better view of the true risks within the organization. It assists blue teams by offering recommendations to prevent potential breaches using an effective patching strategy that can be deployed on a minimum number of hosts. With its effective remediation strategy, Harmony Purple also effectively fulfils the needs of the blue teams.

The technology approach used by most **Breach and Attack Simulation (BAS)** vendors involves the deployment of agents that actively test the environment against attack simulation methods used by attackers. While the main focus of those tools is to provide a picture of the organization's environment from the attacker's perspective, they provide information geared mainly to the organization's advanced security researchers and highly-trained staff. They do not focus on the needs of the blue teams. With its unique, patented AI technology that creates Attach Path Scenarios (APS™), Harmony-Purple also provides an effective tool to fulfil the needs of the red teams.

AUTOMATED PURPLE TEAMS ENSURE CONTROL EFFECTIVENESS

Continuous Scanning
Continuous scanning of all the company assets' vulnerabilities including critical servers, web servers, endpoints, applications, network configuration weaknesses, and data connectivity flows. With patented advanced lean scanning technology, Harmony Purple is designed for critical systems and production environments thanks to its high speed and minimal network-traffic load.

Recommended Remediation
Reports on all critical assets at risk and recommends the best mitigation options that fit your critical asset risk, significance, and operational needs. It offers several remediation options, and validates vulnerability remediations over time.

Visibility into Attack Path Scenarios
Harmony Purple's patented algorithm analyzes the network scanning results to identify high-probability attack patterns that can be exploited by hackers to penetrate the organization's most critical assets, and demonstrates the attack paths to the organization's crown jewels and the vulnerabilities to be exploited from a hacker's point of view.

Prioritization by Business Risk
Continuously analyzes your critical assets, business processes, and network context to identify vulnerabilities that put the critical business assets at risk. It reduces the cost and effort to patch thousands of vulnerabilities. In addition, it finds the vulnerabilities that are most critical to your business based on your unique network topology.

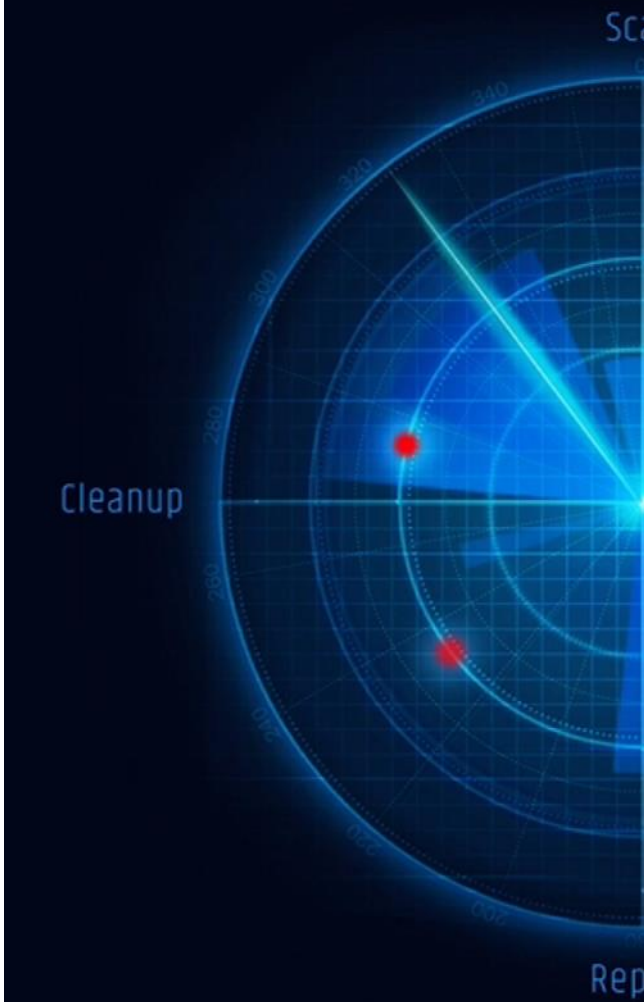
Harmony Purple allows organizations to substantially reduce its attack surface with the least amount of time and effort and with the most efficient use of staff resources, helping organizations invest their time wisely on those vulnerabilities that threaten its mission-critical assets and business processes.

PENTERA

AUTOMATED PENETRATION TESTING PLATFORM

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

AUTOMATED BLACK-BOX PENTESTING



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.

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.

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.

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.

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.

PRIORITIZED 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.

LATEST HACKING TECHNIQUES

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

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

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.

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 – KEEPING 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

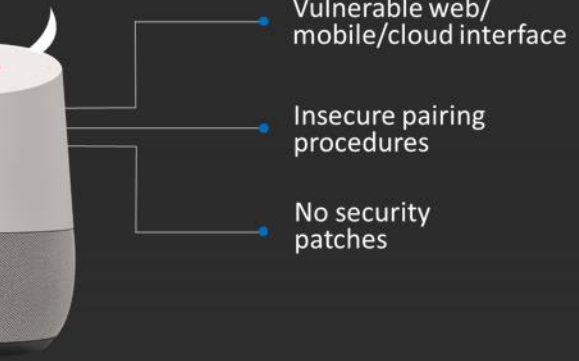
HARMONY IoT takes precise actions to neutralize malicious IoT activity, in real-time, to protect the integrity and privacy of your sensitive information and ongoing operations.

THREAT PROTECTION FOR WI-FI AND BLUETOOTH FREQUENCIES

HARMONY IoT

IS SO

CENT



HOW HARMONY IOT WORKS

The HARMONY IoT defense is comprised of:

SMALL, NON-INTRUSIVE HARMONY IoT SMART PROTECTS

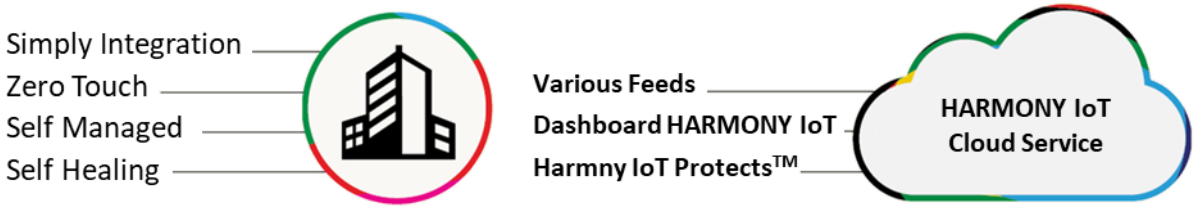
Continuously monitor the activity of all smart connected devices in your airspace and mitigates threats when identified. The Smart Protects are quick and seamless to deploy, requiring no access to your networks or assets and are completely independent, agentless, and out-of-band.

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 CYBERSECURITY 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.

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

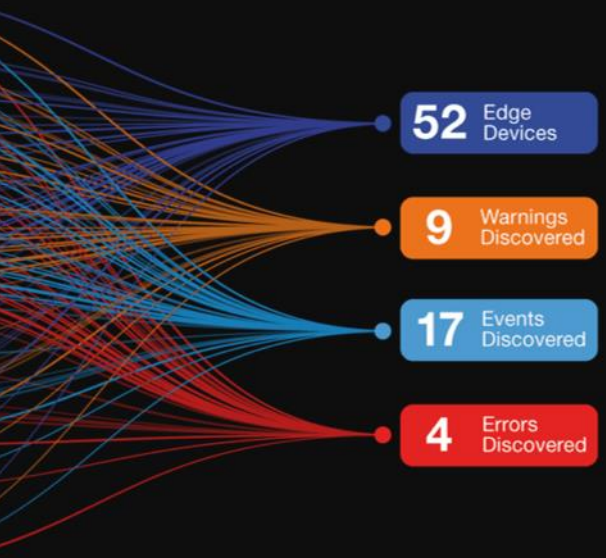
MACHINE LEARNING ALGORITHMS
to automatically identify network elements

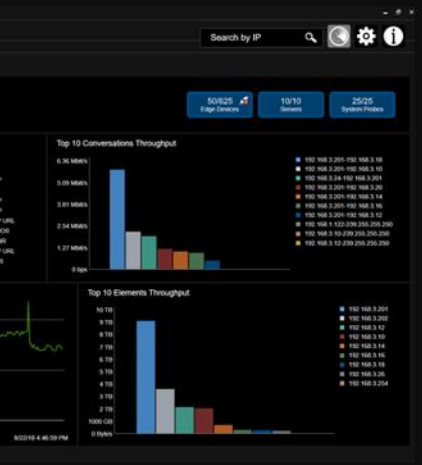
NETWORK INVENTORY
and statistics

PROPRIETARY DATABASE
of vendor vulnerabilities

CYBER-PROTECTION FOR PHYSICAL SECURITY NETWORKS

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.

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

CYBERSECURITY THREAT ANALYSIS AND AUTOMATIC REMEDIATION ACROSS ALL OS'S

VALI
Endpoint Config
For IT Security

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.

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

360 PROTECTION WITH DECEPTION CAPABILITIES

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.

MINEREYE DATA TRACKER

Govern your information anywhere

SEARCH AND PROTECT THE ORGANIZATION'S CONFIDENTIAL DATA – PERFECT FOR DPO'S

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 TRACKER™

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.

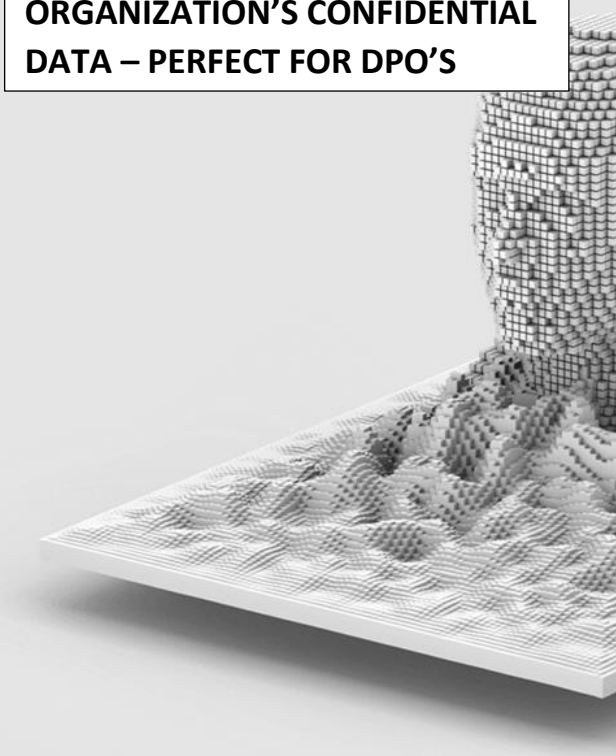
MinerEye's Interpretive AI™ Technology goes deep into any file at the pixel and byte level for the most accurate classification, ensuring nothing is missed.

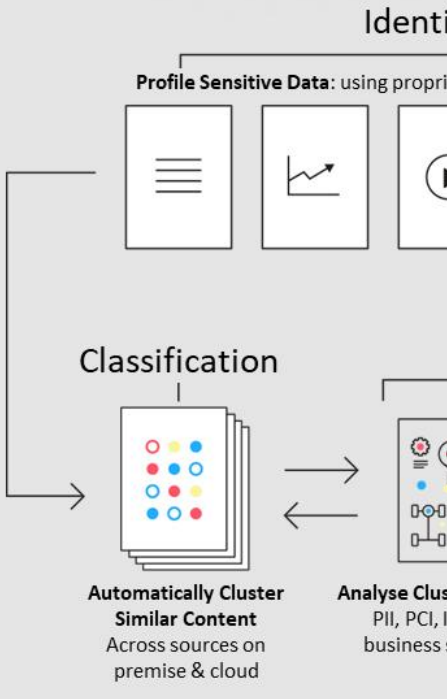
Artificial Intelligence

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.

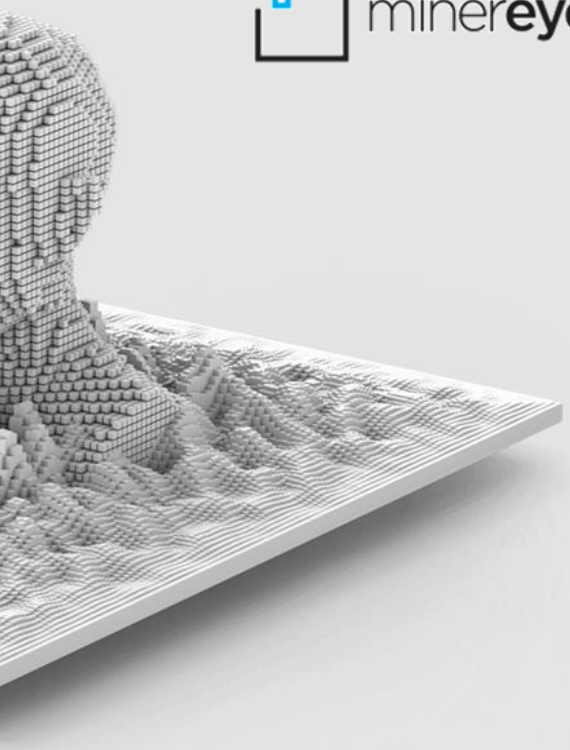
Any Data in Any Form

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.

MOBILE PROTECTION

Multiple options, one goal: Protect all your mobile phone communications!

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 SECURITY – FOR OPERATORS

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. We expect to see network based cyber security solutions, adopted by every MNO and cellular IoT network in the coming years.

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

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.

We offer 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.

	IMSI catchers	Network loopholes	Malicious SMS	Malware	Device Types
Our Solution for Operators	✓	✓	✓	✓	ALL
Secured hardware on device	×	×	×	✓	Limited
Cloud-Based solution	×	×	×	✓	ALL
Securiy SW on-device	×	×	×	✓	Limited
SS7/S;S firewalls	×	✓	✓	×	ALL
Network-based data protection	×	×	×	✓	ALL

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

PROTECT ALL YOUR MOBILE DEVICES & COMMUNICATIONS

MOBILE P
FOR EV

TELECOM OPERATORS

MULTI BRANDS

ROTECTION
ERYONE

& END USERS

MOBILE SECURITY FOR END USERS

For the end users level, we provide two different solutions: MTD (Mobile Threat Defense) & Encrypted Mobile Device and Communications. These solutions can be purchased separately or together to ensure the highest possible level of protection.

Protect your trade secrets, business assets, and digital privacy to enjoy freedom of mobility - minus the risk.

MTD (Mobile Threat Defense) – with protected SIM cads

This solution uses machine learning machine learning to detect device, network, phishing and application mobile attacks on-device and in real time. This engine was designed specifically for mobile, deviating from traditional endpoint security, being like next-generation EPP solutions to guard against the unique threats (known and unknown) targeting iOS, Android and Chromebook devices.

Encrypted Mobile Device and Communications

This solution provides enterprises with military grade encryption on the OS (from layer 1 to 7) to protect their most private information and via an encrypted communication application that allows users to perform calls, share files and messages with the utmost privacy.

Option A) Hardware with specific OS (Currently supported models: Google Pixel/Pixel XL)
The first fully encrypted smartphone
This solution is based on hardened, off the shelf smartphone devices, installed with a proprietary secured version of the Android OS and backed by a secured communication and content management infrastructure with the ability to effectively protect against a wide range of mobile threats while providing maximum usability and standard smartphone functionality.

The device is protected from all known attack capabilities, including:

- **Network Interception**: All voice, SMS and internet communications are protected.
- **WiFi**: protected from interception, data manipulation and infection.
- **Data extraction**: protected from physical extraction means.
- **Trojan horses and Malware attacks**: full permission control policy over hardened OS.

Option B) Google Play / App Store Application – For Android & iOS
Voice calls & chats that stay private
Encrypted chats and voice call for safe communications and data exchange.

- Secure calls & messages
- Metadata encryption
- Available for iOS & Android
- PBX/Telephony Integration
- Group chats (up to 12 contacts)
- No access of the company to private messages
- Available for whitelabeling
- Self-destructing messages
- Hashing personal data

DIGITALSKILLS CYBERSECURITY SERVICE PACKS

VALIDATE YOUR SECURITY POSTURE AND ELEVATE YOUR RESILIENCE

CYBERSECURITY PROFESSIONAL SERVICES

CYBERSECURITY ASSESSMENTS

Our multi-disciplinary technical team is experienced in conducting several types of in-depth assessments for your organization, ranging from your technological areas to your processes, people and also compliances. With our assessments it's possible to validate your current cybersecurity posture as well as improve your cyber-resilience in order to mature the organizations controls, responses and plans to reduce your attack surface.

Our assessments are adapted to each partner's needs to help them structure their internal plans (DRP, BCP, ISCP, governance and others). Our team can perform QNRC/QACC/NIS assessments, CIS assessments, NIST CSF assessments, SWIFT and many more depending on the compliances and frameworks that the client is currently implementing – during these assessments we validate the controls based not only based on industry standards but also based on the current reality of the client were we elaborate on improvements to be made.

PENETRATION TESTING

Professionals allocating to projects related to the provision of penetration testing services specialize in cybersecurity governance, infrastructure security and compliance with existing methodologies and legislation, cybersecurity regulations and standards. In Portugal, our team has extensive experience in performing this type of services, we can perform tests ranging from the internal, external, web applications, wireless, mobile, code analysis and many others including SCADA and IoT'S.

DigitalSkills believes that its specialized technical team, together with the innovative solutions it distributes in the area of cybersecurity and its recognized methodologies that will be described in this proposal, they will be a starting point for the beginning of the partnership relationship between clients and our company, with solid foundations that will allow our partner client to truly increase its level of cyber-resilience and maturity positioning it in the lead as a precursor to the best security practices of its sector of activity. We have already pre-made packs that you can verify bellow, being that we also provide custom made services.

ZERO TRUST ASSESSMENTS

We are proud to announce that DigitalSkills brings to our cybersecurity solutions catalogue the performance of Zero Trust Architecture and eXtended maturity assessments based on the existing compliances. With this assessment we can help partners and clients to start their journey into implementing a Zero-Trust model in the organization or understand the current phase of Zero-Trust in which they are.

Previously, the focus was on creating a security perimeter of the organizations' infrastructure and existing assets internally. With digital transformation, the organization's perimeter no longer exists, as cloud and collaborative environments have migrated and many employees have moved to doing their jobs remotely, with this, the security landscape has to change to a Zero-Trust approach.

Our assessment will cover the analysis of the organization's current architecture and assess it for maturity and compliance to Zero-Trust Architecture (ZTA) based security controls architecture - i.e. advanced analysis of strategies and planning for risk management and incident response processes, identity and Cloud edge device management and security, governance and a network security architecture including existing controls and micro segmentation. Our team will also review the strategies of Zero Trust eXtended (ZTX)-based security controls, and we will check the security maturity of information management, processes, network infrastructure, employees, devices, incident response automation, and continuous monitoring.
Our reports include STANDARD, DREAD or STRIDE risk analyses. We also include gap analysis and as-is/to-be.

Network

Devices

Applications

Processes

Information Management

Identity

Least privilege accesses

Monitoring

Incident response automation

DIGITALSKILLS IS PIONEER IN ZERO TRUST ASSESSMENTS

CONTACT US FOR MORE INFORMATION AT INFO@DIGITASKILLS.PT