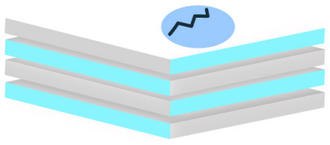
IT Security Solutions and Services Brochure



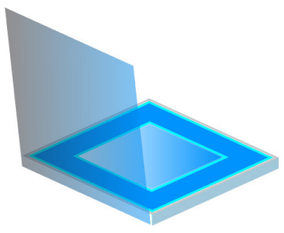


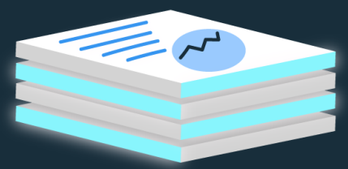
Table of Contents

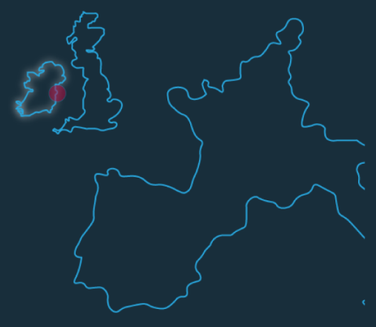
Application Performance Management

Advanced dashboarding and alerting

INCA Networks APM Solution is scalable, extendible, and easily automated to reduce your companies overheads and ensure the right data is accessible to everyone who needs it.

Our APM solution uses machine-learning based alert systems to auto-detect and surface anomalies with zero configuration.
It can also help reduce dozens of dashboards to just one more convenient dashboard.
Easily identify user-end network problems and monitor information transcation speeds efficiently.





Navigate applications seamlessly with the Service

INCA Networks APM Management is built to support live root-cause analysis to reduce resolution time and help teams release features more quickly.

- Automatically map data flows and cluster services based on their interdependencies in real-time

- Investigate service disruptions by isolating the services that interact with the application of interest

- One-click navigation from global alerts to relevant traces, logs, and infrastructure metrics

Search + APM

Finding and fixing roadblocks in your code boils down to search. Our dedicated UI lets you identify bottlenecks and zero in on problematic changes at the code level. As a result, you get better, more efficient code that leads to a speedier develop-test-deploy loop, faster applications, and better customer experiences.

String it all together with distributed tracing

Wondering how requests are flowing through your entire infrastructure? String transactions together with a distributed trace and get a clear view of how your services are interacting. See which messaging frameworks (like Kafka) were utilized and visualize service calls across them, find where latency issues are arising in the path, and pinpoint the components that need optimizing.

Detect anomalous response times with machine learning

Create a job directly from the APM app in Kibana. Find the abnormal behavior and the problematic pieces with machine learning features that automatically model your data.

Get alerted, then react

The dashboards that we implement from Elasticsearch are pretty, but you'll probably have to look away at some point. Stay up-to-date on how your code is performing with our alerting features. Get an email notification when something goes awry or a Slack notification when something goes really right.

It's developer-friendly and language friendly

Elastic APM ships with support for Java, Go, Node.js, Python, Ruby, .NET, and Real User Monitoring (JavaScript) for multiple-page and single-page applications — and more programming languages are on the way. If you've already instrumented your apps with Jaeger, you can stream those traces directly to Elastic APM with our free and open source agents. Don't see what you need? Don't see what you need? Build it or leverage the open source community.

Wifi Optimisation

Find The Right Wifi Solution For Your Business.

When it comes to a wifi solution that fits, INCA Networks has the solution for you. We offer a range of business-grade WIFI solutions. Our expert team help you to understand your requirments, and help you to identify what is best solution for your business.

The majority of how a business operates today is online. With daily application use, communication methods and cloud solutions all requiring online connectivity, companies cannot afford for their network to be less than excellent.

Through our links to many of Ireland's leading business broadband providers, we can offer you a wide range of competitively-priced product and service options, tailored. to meet your company's specific needs.

Professional Grade Wireless

The most constant complaint about consumer grade wireless networks is that they're slow and unreliable.Slow loading times can be harmful to a businesses efficiency. Which is why INCA Networks uses fast and reliable business-class wireless networks instead.

At INCA Networks, our managed IT service team sell and install professional wireless network solutions. With the skilled expertise of our wireless networking consultants, INCA Networks can support organisations of all sizes with their wireless needs.

So let INCA Networks be your go-to technical resource, keeping your office connected and running smoothly.

Wi-Fi 6 (802.11ax) with Multigigabit Ethernet

INCA Networks offers a host of different cloud management features. These include:

Cloud management

-Network-wide visibility and control
-Self-provisioning for rapid deployment
-Automatic reporting
-Seamless firmware updates

Enterprise security

-802.1X and native Active Directory integration
-Air Marshal: Real-time WIPS with forensics
-Stateful Layer 3-7 firewall
-Identity-based group policies
-Built-in antivirus scan (NAC)
-Built-in Umbrella DNS Security*
-Adaptive Policy automated segmentation**

Guest Access

-1-click secure guest access
-Guest isolation firewall
-Customizable splash pages
-Integrated Facebook login

RF optimization

-Dual-concurrent radios with MU-MIMO support
-Radios optimized for rate-vs-range performance
-Third radio dedicated to security and RF management
-Built-in real-time RF spectrum view
-Cloud-based automatic RF optimization

Layer 7 Traffic shaping

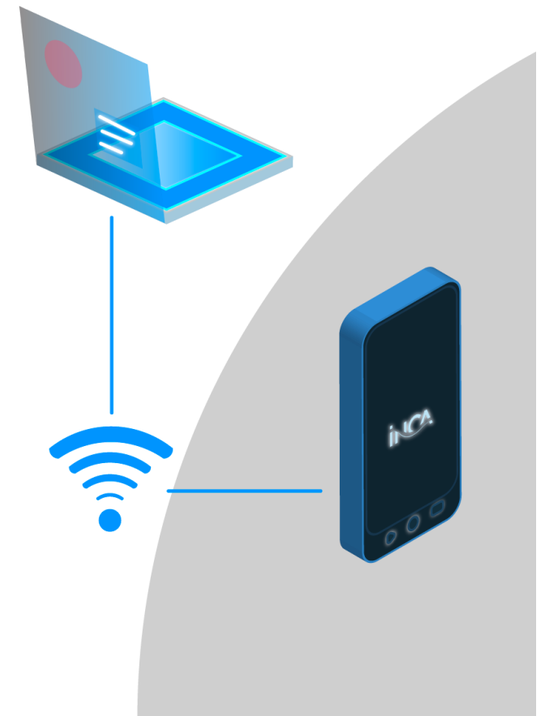
-Classifies hundreds of applications
-Create per-application bandwidth limits
-Prioritize productivity apps
-Restrict or block recreational traffic

Presence location analytics

-Measure visitor capture rate, visit length, and repeat visit rate
-Measure visitor trends over time and compare performance across locations

Device management

-Create device-specific firewall rules
-Monitor and track device inventory
-Deploy applications and enforce security settings.

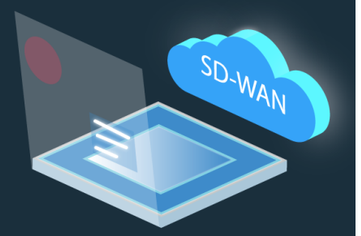


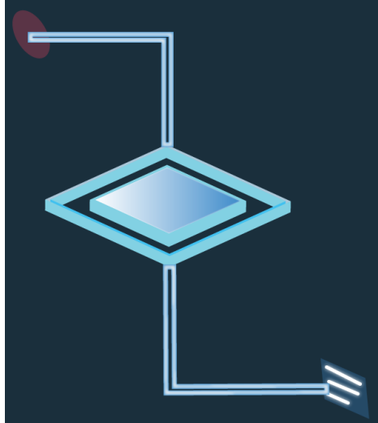
SD-WAN

SD-WAN From INCA

A Software-defined Wide Area Network (SD-WAN) is a virtual WAN architecture that allows enterprises to leverage any combination of transport services – including MPLS, LTE and broadband internet services – to securely connect users to applications.

An SD-WAN uses a centralized control function to securely and intelligently direct traffic across the WAN. This increases application performance and delivers a high quality user experience, resulting in increased business productivity, agility and reduced costs for IT.





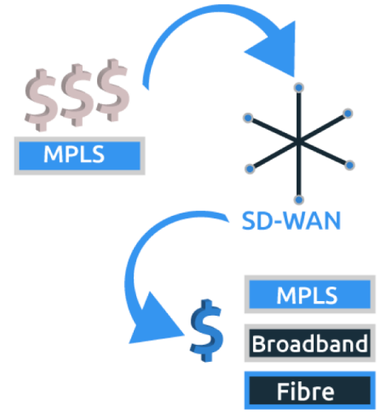
Why SD-WAN?

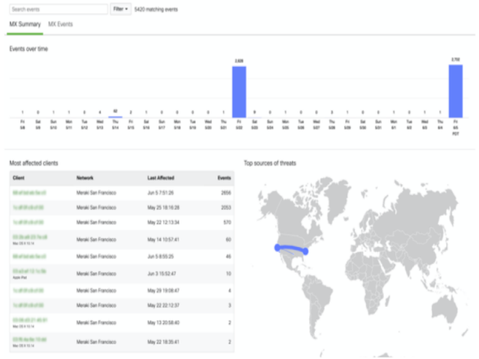
An SD-WAN enables cloud-first enterprises to deliver a superior application quality of experience (QoEX) for users. Using intelligence and by identifying applications, an SD-WAN provides application-aware routing across the WAN. Each class of applications receives the appropriate QoS and security policy enforcement, all in accordance with business needs.

Secure local internet breakout of IaaS and SaaS application traffic from the branch provides the highest levels of cloud performance while protecting the enterprise from threats. Unlike SD-WAN, the conventional router-centric model distributes the control function across all devices in the network and simply routes traffic based on TCP/IP addresses and ACLs. This model tends to be rigid, inefficient and not cloud-friendly, resulting in a poor user experience.

Reduce dependence on MPLS

Take advantage of low-cost WAN links such as broadband and fiber to significantly reduce your WAN costs with the Meraki MX appliances that can be quickly deployed at scale with true zero-touch provisioning.

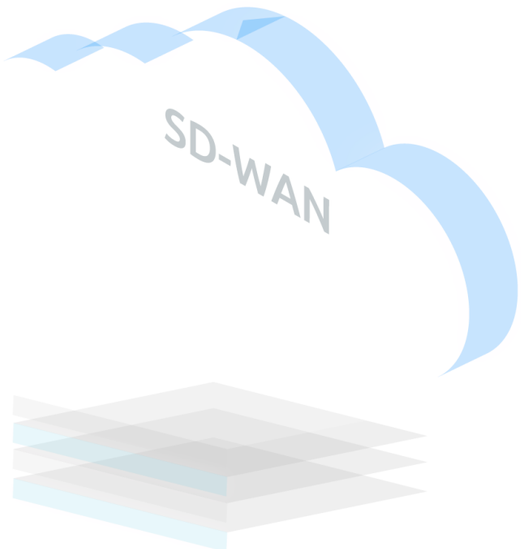




Natively secure

SD-WAN powered by Meraki is natively integrated with advanced security informed by the world-renowned security research team, Cisco Talos. MX appliances also receive zero-touch security updates so you can be confident you are protected from the latest threats and that WAN traffic is secure especially for applications with direct Internet access.

- Next-generation layer-7 firewall
- File protection with Cisco Advanced Malware Protection (AMP)
- Intrusion detection and protection (IDS/IPS) with Cisco SNORT
- Content filtering
- Cloud security integration with Umbrella SIG



Firewall Integration

INCA Networks seamlessly integrates with all leading brands of traditional and next generation firewalls and cloud security controls, as well as routers, load balancers and web proxies, to deliver unified security policy management through a single pane of glass. AlgoSec abstracts vendor-specific technologies so you can focus on what drives your business. From auto-discovering application connectivity requirements, through “zero-touch” change execution, and unified risk and compliance reports, AlgoSec simplifies and automates firewall management across your heterogeneous environment.

Firewall Policy

With INCA Networks you can get an intelligent, live topology map of your entire network security estate.
It’s also possible to automate the entire firewall change management process, including hands-free policy push directly to the devices.
- Manage next-generation firewall policies and cloud security groups alongside traditional firewalls
- Pinpoint and troubleshoot network connectivity issues
- Proactively assess risk and optimize firewall rulesets
Instantly generate audit-ready reports for all the major regulations (PCI-DSS, SOX, HIPAA, and many more).

Reduce Complexity

Consolidate products and services to reduce complexity. With industry-leading threat protection and FortiGuard Labs services, you can reduce costs and maximize your return on investment (ROI).

Encrypted Cloud Access

Achieve comprehensive visibility and policy controls by inspecting all types of traffic, from clear-text to encrypted, and implement intrusion prevention system (IPS) protection.

Visibility and Automation

Gain access to network and security events for contextual visibility, and simplify operations with automated processes.

Reduce Attack Surface

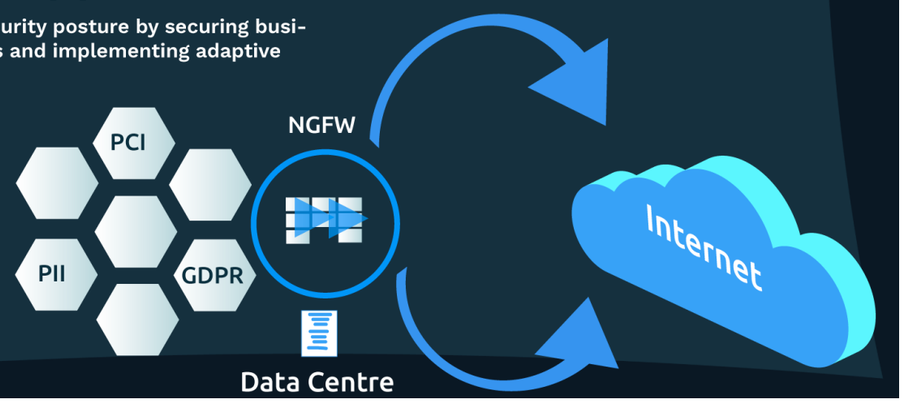
Effectively manage attack vectors with microsegments, industry-leading threat protection, and FortiGuard Labs services.

Regulatory Compliance

Meet compliance and regulatory requirements, such as PCI DSS, PII, HIPPA, and GDPR.

Trusted Application Access

Improve your security posture by securing business applications and implementing adaptive access control.

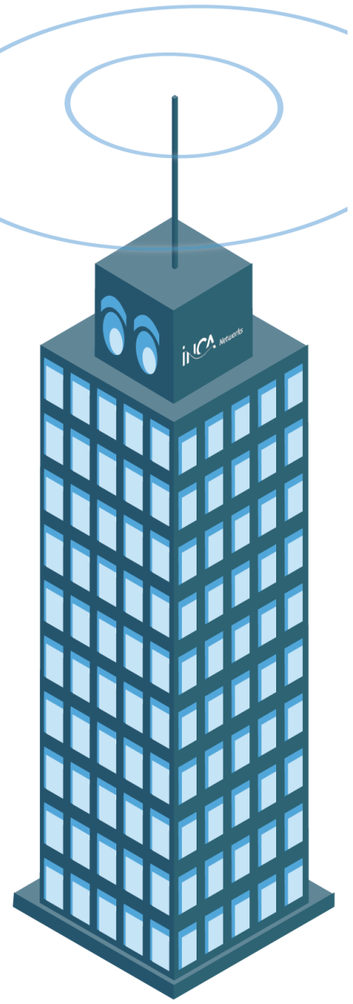


Logz.ly

IoT Monitoring

Companies managing large fleets of distributed IoT devices must contend with a torrent of telemetry data from individual devices, which are often globally dispersed and built on multiple software and hardware platforms. In these environments, interruptions in the flow of data from any one source may indicate a device failure, an application-level performance problem, or a regional network issue.

To reliably operate their IoT fleets, companies need a comprehensive view of the health of their devices in aggregate, as well as the ability to drill down to troubleshoot a particular region, device type, software version, or individual device. INCA Networks provides top-to-bottom IoT monitoring for device fleets, with the ability to aggregate performance metrics by any dimension and at any level of granularity. Companies can monitor IoT software performance, device hardware metrics, application logs, network performance data, and more, all in a single pane of glass.



Alerting For IoT Devices

The sheer volume of telemetry data from IoT devices, coupled with the intermittent connectivity issues of a distributed fleet, pose a challenge for traditional alerting tools. INCA Networks alerting capabilities for IoT monitoring are sophisticated and customizable enough for even the most dynamic, decentralized networks of devices. IoT fleet operators can build alerts that trigger only on sustained or widespread device failures, so that responders are not overwhelmed by meaningless alerts for transient issues. Machine learning algorithms such as anomaly detection and outlier detection automatically determine normal ranges and alert only on unusual occurrences, such as latency slowdowns affecting a particular software version.

Let's talk about how Logz.ly can work **for you**

More about IoT Monitoring

IoT monitoring for any device, anywhere

To bring visibility to diverse IoT fleets, Logz.ly (An INCA Networks Logstash Tool) can be installed on nearly any hardware platform and operating system, including Linux, Windows, Android, and ARM devices. On every device, the lightweight Logz.ly™ Agent collects metrics, distributed traces, logs, and more for centralized monitoring and analytics. Logz.ly™ enables companies with large device fleets to manage and monitor their logs cost-effectively. Companies can send all their logs to Logz.ly™ for real-time visibility, then generate metrics that summarize log contents and dynamically retain high-value logs for long-term analytics.

Organizations that run IoT devices using a managed cloud service can visualize all their data using Logz.ly™ fully supported integrations for IoT monitoring, including Amazon IoT, Google Cloud IoT, and Azure IoT Hub. Regardless of the source, Logz.ly™ brings together all the operational data required for monitoring IoT devices in an intuitive platform for visualization, analytics, correlation, and alerting.

Logz.ly

Monitor business-level IoT metrics alongside device health

IoT devices rarely run off-the-shelf software but instead perform functions that are unique and vital to the business. Whether they serve as point-of-sale terminals, distributed sensors, or industrial machinery, IoT devices often collect mission-critical operational data or handle custom business logic. Logz.ly™ enables companies to collect, analyze, and visualize this business-level data from IoT devices alongside health and performance metrics from the devices themselves. With robust APIs and telemetry libraries for virtually every language and framework, Logz.ly™ makes instrumentation simple and efficient. By adding just a few lines of code, developers can start collecting and analyzing custom business metrics in the same platform that they use to monitor IoT devices, distributed applications, and the rest of their IT infrastructure.

3G Network Backup

Diversify your connection

Most international businesses are dependent on wired connections to run their day to day communications. If a wired connection fails, it can be a difficult process to switch your connection to a 3G network. Without a well prepared 3G network backup plan a firm can go days without access to company E-mail and internet and in some cases, company records. This can be disasterious to a companies quarter or even year.

At INCA Networks we advocate optimising a company's WAN so as to make a potential switch to 3G during a network disruption, easier and far less traumatic.

3G wireless networks are essentially designed to attach a single device like a phone to an IP network (in most cases either the Internet or a private IP network). As such they are made for the 3G terminal device to get a single IP address. This means by default you don't get to treat the 3G terminal as a router because the 3G network only routes IP packets destined to that one address to the terminal. To make the 3G network actually route to subnets behind the 3G terminal, it can take some serious mapping.

WAN Optimisation

At INCA Networks we don't shy away from some of the hard work it takes in terms of connection mapping and WAN optimisation that goes into making a 3g network backup solution reliable. Our goal is for your company to have a reliable 3G Network that can support your unique communciations setup, should needs be.

3G And APN Solutions

Safely enable mobile working

An APN is an access point name that's set up on a mobile device. It determines which network path the device will use for data connectivity. The beauty of this solution lies in its APN settings on your mobile device: they are used to make a connection between the device's cellular network and another network, such as the Internet or a corporate intranet.

You can think of an APN as an access code the cellular network uses to direct you to either the corporate network or a shared network, depending on where the APN allows you to go. This lets you to unlock the value of a mobile workforce without compromising on network security.

Keep data secure and browsing in check

With APN Solutions your connectivity is secure – authentication is in line with your governance and risk controls. It also allows you to control which sites or networks employees may access using the company's mobile data. From an online self-service portal, you'll be able to download reports on connectivity usage and control costs by managing usage better (for example, billing different departments separately).

Make your mobile workforce more efficient

APN solutions offer fast, secure and reliable access for your mobile workforce.

Thank you for your time

Got a question?

Please don't hesitate to E-mail us at **hello@inca.ie** or call us on **01-9604021.**

Would you like to know more about INCA Networks?

Visit our inca.ie today to learn more about our IT Security services and Products.