LN INFOSEC PVT LTD

Products & Services Brochure

LN INFOSEC PVT LTD

LN InfoSec Pvt Ltd - Products & Services Brochure

At LN InfoSec, we offer a comprehensive cybersecurity ecosystem that covers every aspect of protection. Our services include everything from Governance, Risk & Compliance (GRC) and Identity Security to cutting-edge Threat Intelligence, AI Security, and Industrial OT defence. We bring together strong Endpoint, Network, and Cloud Security solutions with proactive Managed Services (MSS) and Cyber Insurance support to help you stay resilient against today's threats. Our advantage is built on strategic partnerships with leading global tech companies, along with a dedicated promise of expert installation, configuration, and ongoing technical support.

Governance, Risk & Compliance (GRC)

Security without structure is strategy without direction. Governance, Risk & Compliance (GRC) provides organizations with a structured framework to align cybersecurity practices with business objectives, regulatory requirements, and risk appetite. It streamlines policy management, audit readiness, and compliance tracking — enabling organizations to meet global mandates such as ISO 27001, SOC 2, and GDPR with greater efficiency and confidence. In the Indian regulatory context, GRC plays a pivotal role in ensuring adherence to CERT-In directives, the Digital Personal Data Protection (DPDP) Act, SEBI Cyber Security & Cyber Resilience Framework, and RBI's guidelines for BFSI sector cybersecurity among other sector-specific mandates. A strong GRC posture reduces exposure to regulatory penalties, strengthens organizational accountability, and builds lasting trust with customers, regulators, and stakeholders across both domestic and global markets.

Threat Detection & Security Monitoring

Threats don't wait and neither should your defences. Threat Detection & Security Monitoring is the practice of continuously identifying, analysing, and responding to security threats across an organization's IT environment. It combines network traffic analysis, SIEM platforms, and XDR capabilities to provide real-time visibility into potential attacks and anomalous activity. By correlating data from multiple sources, security teams can detect threats early and neutralize incidents before they cause irreversible damage. This domain forms the operational backbone of a mature and effective Security Operations Centre.

LN INFOSEC PVT LTD

Identity Security

In today's threat landscape, identity is the new perimeter and securing it is non-negotiable. Identity Security ensures that only the right individuals have access to the right resources at the right time, across every environment. It encompasses identity governance, privileged access management, and identity threat defence providing robust protection against credential-based attacks, account compromise, and insider threats. As attackers increasingly target identities over infrastructure, this domain has become one of the most critical pillars of a modern cybersecurity strategy.

Endpoint Security

Every device connected to your network is a potential gateway for attackers. Endpoint Security is the practice of protecting laptops, desktops, servers, and mobile devices against malware, ransomware, and advanced persistent threats. Leveraging Endpoint Detection & Response (EDR) and Extended Detection & Response (XDR) capabilities, it delivers deep behavioural visibility and rapid threat containment at the device level. In an era of remote work and expanding device ecosystems, endpoint security remains one of the most critical layers of defence in any cybersecurity architecture.

Security

Your applications are the face of your business and a prime target for attackers. Application Security focuses on identifying and remediating vulnerabilities across web applications, APIs, Mobile Applications and cloud-native software throughout the entire development lifecycle. It encompasses web application scanning, runtime protection, software composition analysis, and cloud-native application protection ensuring security is embedded from code to deployment. A robust application security practice is essential for safeguarding customer data, protecting business continuity, and maintaining compliance in an increasingly application-driven world.

Network Security

A compromised network is a compromised business the stakes have never been higher. Network Security encompasses the technologies and practices designed to protect the integrity, confidentiality, and availability of an organization's network infrastructure. It spans next-generation firewalls, secure SD-WAN, network access control, intrusion detection, and traffic management ensuring secure connectivity across on-premises, remote, and cloud environments. As networks grow more complex and distributed, a well-architected network security strategy is the cornerstone of any comprehensive

cybersecurity posture.

Cloud & Container Security

The cloud moves fast; your security posture must move faster. Cloud & Container Security protects workloads, data, and applications hosted in cloud environments and containerized infrastructures from misconfigurations, vulnerabilities, and unauthorized access. It delivers comprehensive coverage through Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWPP), and Kubernetes Security Posture Management (KSPM) providing real-time visibility and automated remediation at scale. As cloud adoption accelerates, this domain is indispensable for organizations looking to innovate and scale with security at the forefront.

Data Loss Prevention (DLP)

Your data is one of your most valuable assets and losing control of it can be irreversible. Data Loss Prevention (DLP) is the practice of monitoring, detecting, and preventing the unauthorized transmission or exposure of sensitive organizational data across endpoints, networks, and cloud environments. It safeguards intellectual property, personally identifiable information (PII), and confidential business records while ensuring adherence to regulatory frameworks and data protection laws. DLP is an essential control for any organization that handles sensitive or regulated information and cannot afford the reputational or financial cost of a data breach.

Identity & Access Management (IAM)

Access is a privilege, not a right — and managing it with precision is what keeps organizations secure. Identity & Access Management (IAM) governs how users are authenticated and authorized to access systems, applications, and data across an organization. It establishes a centralized framework for enforcing least-privilege access, managing digital identities, and detecting identity-based threats in real time. By ensuring that access rights are continuously reviewed and aligned with organizational roles, IAM significantly reduces the attack surface and strengthens security accountability at every level.

Third-Party Risk Management (TPRM)

Your security is only as strong as the weakest link in your supply chain. Third-Party Risk Management (TPRM) is the practice of systematically identifying, assessing, and mitigating the cybersecurity risks introduced by vendors, suppliers, and partners within an organization's ecosystem. It provides continuous oversight of third-party relationships,

ensuring that external entities consistently meet defined security and compliance standards. As supply chain attacks grow in scale and sophistication, TPRM has become an essential discipline for any organization committed to protecting its extended enterprise and maintaining the trust of its clients.

Mobile Device Management (MDM)

The modern workforce is mobile — and so are the risks that come with it. Mobile Device Management (MDM) enables organizations to centrally manage, monitor, and secure every mobile device within their ecosystem — whether corporate-owned or personal (BYOD). It enforces security policies, manages application deployments, and enables remote wipe capabilities to prevent unauthorized access and data leakage. As mobile devices become deeply embedded in enterprise operations, MDM is a fundamental control for maintaining security standards across a distributed and dynamic workforce.

Threat Intelligence

Knowing your adversary before they strike is the most powerful advantage in cybersecurity. Threat Intelligence is the practice of collecting, analysing, and operationalizing data about current and emerging cyber threats including the tactics, techniques, and procedures (TTPs) used by threat actors targeting specific industries and environments. It enables organizations to move from reactive incident response to proactive threat prevention informing decisions across vulnerability management, detection engineering, and security strategy. In an increasingly hostile digital environment, threat intelligence is the foundation of informed and resilient cyber defence.

Malware & Attack Analysis

Understanding how an attack works is the first step to ensuring it never happens again. Malware & Attack Analysis involves the deep forensic examination of malicious code, suspicious files, and attack artifacts to understand their behaviour, origin, and intended impact. Through controlled sandbox environments and multi-scanner analysis, security teams can safely investigate threats without risk to production systems. The intelligence derived directly strengthens detection capabilities, informs incident response playbooks, and enables organizations to build defences tailored to the specific threats targeting their environment.

AI Security & Governance

As artificial intelligence transforms business operations, it simultaneously introduces a new class of security and ethical risks that organizations cannot afford to ignore. AI

Security & Governance addresses two critical imperatives — protecting AI systems from threats such as model vulnerabilities, data poisoning, prompt injection, and adversarial manipulation, while ensuring that AI is developed, deployed, and used in a responsible, transparent, and compliant manner. On the security front, it safeguards AI models, pipelines, and infrastructure across the entire AI lifecycle. On the governance front, it establishes the policies, controls, and accountability frameworks needed to ensure AI systems operate within ethical boundaries, regulatory expectations, and organizational risk tolerance. Together, AI Security & Governance empowers organizations to harness the full potential of artificial intelligence — with confidence, accountability, and resilience.

Industrial & OT Security

When operational technology is compromised, the consequences extend far beyond the digital world. Industrial & OT Security addresses the distinct cybersecurity challenges faced by critical infrastructure sectors — including manufacturing, energy, utilities, and transportation — where a successful cyberattack can directly disrupt physical operations and endanger lives. It provides asset visibility, threat detection, and protection across Industrial Control Systems (ICS), SCADA environments, and connected OT devices without compromising operational continuity. As IT and OT networks increasingly converge, securing industrial environments has become both a national and organizational imperative.

Managed Security Services (MSS)

Cyber threats operate around the clock — your security posture must too. Managed Security Services (MSS) deliver continuous security monitoring, threat management, and incident response through a dedicated team of cybersecurity experts. Designed for organizations that require enterprise-grade protection without the complexity of operating an in-house Security Operations Centre, MSS ensures round-the-clock vigilance, faster threat response, and a consistently strong security posture — enabling businesses to stay focused on growth while staying protected.

Cyber Insurance

When a breach occurs, financial resilience is just as critical as technical recovery. Cyber Insurance provides organizations with financial protection against the economic impact of cyber incidents including data breaches, ransomware attacks, legal liabilities, regulatory penalties, and business interruptions. As cyber threats grow in sophistication and frequency, cyber insurance has evolved into an integral component of a comprehensive enterprise risk management strategy. It ensures that organizations can respond, recover,

and resume operations without bearing the full financial burden of a cyberattack.

Digital Forensics

Every cyberattack leaves a trail — and uncovering it is what turns an incident into an insight. Digital Forensics is the disciplined practice of collecting, preserving, and analyzing digital evidence following a cybersecurity incident or suspected breach. It enables organizations to reconstruct the full timeline of an attack, attribute it to specific threat actors, and gather evidence suitable for legal and regulatory proceedings. The findings from forensic investigations are instrumental in driving effective remediation, closing security gaps, and preventing the recurrence of similar attacks — making this domain a cornerstone of organizational accountability.

Staffing

Our Strategic Staff Augmentation services are designed to bridge the gap between your complex cybersecurity requirements and the scarcity of specialized talent. We provide a curated pool of vetted professionals who integrate seamlessly into your existing workflows, offering immediate technical proficiency and deep domain expertise. Whether you need to scale up for a specific compliance project or require niche skills for infrastructure hardening, our resourcing model ensures you have the right experts in place to maintain operational momentum without the overhead of traditional hiring.

The "Unified Ecosystem" Approach

"Beyond specialized security, LN InfoSec Pvt Ltd serves as your strategic procurement partner for a global suite of world-class software. As authorized dealers for industry leaders like Microsoft, AWS, and Google, we provide seamless access to O365 productivity suites, AI-driven workflow tools, and scalable cloud subscriptions. By sourcing your core business infrastructure through our SME-led framework, you ensure that every license—from office tools to firewalls—is backed by the same technical rigor and quality standards that define our cybersecurity practice."

LN INFOSEC PVT LTD

Contact Us

Website: https://www.lninfosec.com
Email: lnarayanr@lninfosec.com
Phone: +918939902233
Address: LN InfoSec Pvt Ltd, B4-Sri Krishna Apartments, #5, III Crescent Part Street, Gandhi Nagar, Adyar, Chennai – 600020, INDIA