JNR MANAGEMENT RESOURCES PVT. LTD.

DELIVERING HIGH ASSURANCE-PKI & CYBER SECURITY SOLUTIONS

ABOUT JNR

21+
Years Of Excellence

Platinum Elite
Certified Partner of DigiCert

5000+
Customers

100+
Channel Partners

95%+
Customer satisfaction
& Retention

End to End
Technical Support

SOLUTION **PARTNERS**

digicert Certified Partner Platinum Elite

Thales Accelerate Partner Network

appviewx

ProDMARC™

ENTRUST

CHECK POINT

CloudSEK

ProPHISH™

mimecast

accops

Google Workspace

Office 365

FIREMON

SECRITE

xorkee sign

And many more.....

100+ AWARD & **ACCOLADES**

AWARD WINNING

PARTIAL LIST OF **CLIENTS**

Reliance Industries Limited
Growth is Life

adani

mygov
मेरी सरकार

SAMSUNG

Vi

NIC National Informatics Centre

RESERVE BANK OF INDIA

pnb

PayU

Payments Bank

paytm payments bank

TATA MOTORS

MARUTI SUZUKI

HONDA

HONDA

Startek

Hero

wipro

tcs TATA CONSULTANCY SERVICES

HCL

TECH mahindra

cognizant

Mahindra

ICICI PRUDENTIAL LIFE INSURANCE

MAX LIFE INSURANCE

Canara HSBC LIFE INSURANCE

BAJAJ FINSERV

goibibo

5000+
Happy Client

CYBER SECURITY THROUGH US

PKI SOLUTIONS

- SSL/TLS
- S/MIME
- Software Trust Manager/Code Signing
- Private CA
- Managed PKI

HARDWARE SECURITY MODULES

- HSM-Payment & General Purpose
- Database Encryption-At Rest/In Motion
- Key Management
- Tokenization & Masking
- Automated Signing

CYBER SECURITY AWARENESS

- Identity Protection
- Gamified Simulation Attacks
- Learning Management

AUTOMATION MANAGEMENT

- Certificate Lifecycle Management
- DNS Protection
- Firewall Management
- ADC Management
- Consulting & Managed Services

BRAND PROTECTION

- DMARC,SPF,DKIM
- BIMI/VMC

CYBER THREATS

- Threat Protection
- Email Security
- Gateway Security
- Anti–Phishing/Spoofing

Authentication

- 2FA/MFA
- SSO
- Password less
- PKI based Authentication
- Zero trust

DIGITAL RISK PROTECTION

- SOAR/SIEM
- Cyber Intelligence
- Brand Monitoring
- Dark web monitoring
- Attack Surface Monitoring
- Infrastructure Monitoring
- Supply Chain Monitoring

PKI SOLUTIONS

SSL/TLS

SSL (Secure Sockets Layer) is a protocol that ensures secure communication over the internet by encrypting data transmission between a user's browser and a website server, safeguarding sensitive information

S/MIME

S/MIME or Secure / Multi purpose Internet Mail Extension - is the leading standard for email signing and encryption. It enables users to encrypt and decrypt messages to each other preventing unauthorized access while signing messages with a validated identity preventing impersonation.

Software Trust Manager/Code Signing

Code signing is a security practice that entails digitally signing software or code with a cryptographic signature, ensuring its integrity and authenticity. This process enables users to verify the source before executing the code.

PRIVATE CA

Code signing is a security practice that entails digitally signing software or code with a cryptographic signature, ensuring its integrity and authenticity. This process enables users to verify the source before executing the code.

Managed PKI

PKI is a framework that manages digital keys and certificates, facilitating secure communication, authentication, and data integrity in electronic transactions and communications over networks.

HARDWARE SECURITY MODULE

HSM-Payment & General Purpose

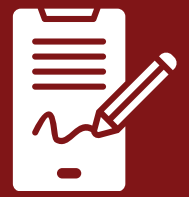
Hardware security modules (HSMs) are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates.

Key Management

Key management refers to management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Tokenization & Masking

Tokenization involves replacing sensitive data, such as credit card numbers or personal identification information, with a unique identifier or token. This token retains no inherent meaning and is meaningless to anyone who may access it without the proper authorization.



Digital Signing

A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature on a message gives a recipient confidence that the message came from a sender known to the recipient.

Automated Signing

Automation signing refers to the automated process of utilizing an HSM to digitally sign code or documents. This implies that the HSM performs signing operations without manual intervention, usually triggered by an application or system

CYBER SECURITY AWARENESS

Identity Protection

Identity protection refers to the practice of safeguarding your personal information and online identity from unauthorized access, misuse, or theft. It involves various measures aimed at minimizing the risk of becoming a victim of identity theft, where someone steals your personal information to commit fraud or other crimes.

Gamified Simulation Attacks

Gamification is the process through which we empower learners to educate themselves. In cybersecurity, gamification is often achieved by simulating phishing attacks, assigning short, bite-sized training, and fostering friendly competition among colleagues. In this article, we'll outline how any organization can implement these techniques to offer a fully gamified learning experience.

Learning Management

A learning management system is a software application designed for the administration, documentation, tracking, reporting, automation, and delivery of educational courses, training programs, materials, or learning and development programs. The concept of a learning management system emerged directly from e-Learning.

AUTOMATION MANAGEMENT

Certificate Lifecycle Management

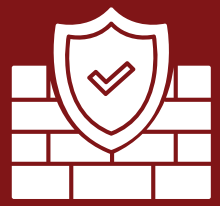
Certificate lifecycle management refers to the process of managing machine identities, such as TLS certificates, throughout their entire lifecycle, from certificate issuance to provisioning, deployment, discovery, inventory, securing, monitoring, renewal, and revocation.

DNS Protection

Domain Name System (DNS) protection adds another layer of security between your employees and the internet. It filters out unwanted traffic and adds suspicious Uniform Resource Locators (URLs) to a blacklist.

ADC Management

ADC Management typically refers to the administration and control of Application Delivery Controllers (ADCs). ADCs are networking devices that optimize the delivery of applications by efficiently distributing network traffic, ensuring high availability, and enhancing performance. These controllers play a crucial role in managing the delivery of web applications and services.



Firewall Management

Firewall management is the process of configuring and monitoring a firewall to maintain a secure network. Firewalls are an integral part of protecting private networks in both a personal and business setting. An organization may have many different firewalls protecting its devices and network as standard.

Consulting & Managed Services

Consulting involves offering expert advice, analysis, and recommendations to individuals or organizations to help them solve specific problems, make strategic decisions, or improve their overall performance.

Managed Services, on the other hand, refer to the outsourcing of specific business functions or processes to a third-party service provider.

BRAND PROTECTION

DMARC, SPF, DKIM

DMARC stands for Domain-based Message Authentication, Reporting & Conformance. It's an email authentication protocol designed to combat email spoofing, a tactic used by attackers to send emails that appear to be from legitimate senders. Spoofing is a common method for phishing attacks, where attackers try to trick recipients into revealing personal information or clicking on malicious links.

BIMI / VMC

VMC is a digital certificate that verifies the ownership and authenticity of a brand logo displayed in emails through BIMI (Brand Indicators for Message Identification). It acts as an extra layer of security, ensuring that only authorized brands can showcase their logos and preventing attackers from spoofing them for phishing purposes.

CYBER THREATS

Threat Protection

Threat protection encompasses a wide range of strategies and tools used to safeguard individuals, organizations, and systems from various cyber threats. Its ultimate goal is to detect, prevent, and mitigate potential harm caused by these malicious activities.

Email Security

Email security refers to the practices and technologies used to protect email accounts and communications from unauthorized access, loss, and compromise. It's crucial for individuals and organizations alike, considering the high dependence on email for communication and often sensitive information exchange.

Gateway Security

Gateway security refers to the protection measures implemented at the entry points (gateways) of a network to safeguard against various cyber threats and unauthorized access. These entry points could include internet gateways, email gateways, and other network access points where data enters or exits a network.

Anti-Phishing/Spoofing

Antispoofing is a technique for identifying and dropping packets that have a false source address. In a spoofing attack, the source address of an incoming packet is changed to make it appear as if it is coming from a known, trusted source.

AUTHENTICATION

2FA/MFA

2FA (Two-Factor Authentication) or MFA (Multi-Factor Authentication) is a security measure that requires users to provide at least two different types of identification before gaining access, adding an extra layer of protection beyond traditional passwords.

SSO

Single Sign-On (SSO) is an authentication process that enables users to access multiple applications and services with a single set of login credentials, streamlining access and enhancing user experience across various platforms.

Password less

Password less authentication is an authentication method in which a user can log in to a computer system without the entering a password or any other knowledge-based secret.

PKI-based Authentication

PKI-based authentication refers to a security process that uses a Public Key Infrastructure (PKI) to verify the identity of users or systems. PKI relies on the use of digital certificates to authenticate the identity of parties involved in a communication and to encrypt and decrypt data exchanged between them.

Zero Trust

Zero Trust is a cybersecurity approach that assumes no implicit trust within the network, requiring verification from anyone trying to access resources regardless of their location or network connection, in order to enhance overall security posture.

DIGITAL RISK PROTECTION

SOAR/SIEM

SIEM technologies focus on correlating and analyzing data to identify potential threats. They use advanced algorithms to detect anomalies and generate alerts when they find unusual patterns. SOAR identifies specific events or threats and carries out automated responses based on predefined workflows.

Cyber Intelligence

Cyber threat intelligence is knowledge, skills and experience-based information concerning the occurrence and assessment of both cyber and physical threats and threat actors that is intended to help mitigate potential attacks and harmful events occurring in cyberspace.

Attack Surface Monitoring

Attack Surface Monitoring involves the continuous surveillance of an organization's digital assets and potential entry points to identify vulnerabilities and proactively strengthen security measures, reducing the risk of cyber attacks.

Dark web monitoring

Brand monitoring is the act of collecting and measuring mentions of your company or brand across as many channels and touchpoints as possible – with a view to turn them into useful data.

Supply Chain Monitoring

Supply Chain Monitoring involves the systematic oversight and evaluation of the production, distribution, and logistics processes within a supply chain, aiming to ensure efficiency, traceability, and risk mitigation.

Brand Monitoring

Brand monitoring is the act of collecting and measuring mentions of your company or brand across as many channels and touchpoints as possible – with a view to turn them into useful data.

OUR REACH

Connect With Us!

https://www.jnrmr.com

+91-11-26187385, 26187635

info@jnrmanagement.com

Our Presence On Social Media...