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

imperva a Thales company

appviewx

TCPWave

infoblox

FIREMON

emudhra Trust Delivered

PROGIST

threatcop Security Starts with People

CloudSEK

Cymulate

SOCRadar

SECLORE

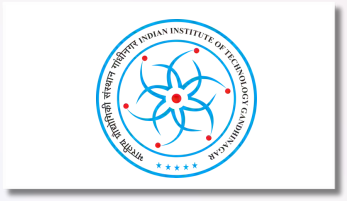
mimecast

And many more.....

100+ AWARD & **ACCOLADES**

AWARD WINNING

PARTIAL LIST OF **CLIENTS**



CYBER SECURITY THROUGH US

PKI SOLUTIONS

- SSL/TLS
- S/MIME
- Code Signing via Cloud
- Private CA
- Managed PKI
- DSC/eSign

HARDWARE SECURITY MODULES

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

APPLICATION SECURITY

- DDoS Protection
- Web Application Firewall
- API Security
- Client-Side Protection
- Attack Analytics
- DAM

AUTOMATION MANAGEMENT

- Certificate Lifecycle Management
- DDI (DNS | DHCP | IPAM)
- ADC Management
- Firewall Management
- Consulting & Managed Services

BRAND PROTECTION

- DMARC,SPF,DKIM
- BIMI/VMC/GMC/CMC

CYBER SECURITY AWARENESS

- Identity Protection
- Gamified Simulation Attacks
- Learning Management

CYBER THREATS

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

AUTHENTICATION

- 2FA/MFA
- SSO
- Password less
- PKI based Authentication
- ZTNA

DIGITAL RISK PROTECTION

- Cyber Intelligence
- Dark web monitoring
- Supply Chain Monitoring
- Brand Monitoring
- BAS / Red Teaming
- Continuous External Threat Management
- Infrastructure 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.

Code Signing via Cloud

Code Signing via Cloud enables developers to securely sign software and manage code signing certificates through a cloud-based platform, ensuring enhanced security and control over private keys without relying on local storage.

PRIVATE CA

A private CA is an enterprise-specific certificate authority that functions like a publicly trusted CA. With a private CA, an enterprise creates its own internal root certificate that can issue other private certificates for internal servers and users.

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.

DSC/eSign

DSC (Digital Signature Certificate) and eSign, are electronic signature solutions that provide secure, legally binding ways to sign documents digitally, ensuring authentication, integrity, and non-repudiation in digital transactions.

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.

Database Encryption -at Rest/In Motion

Database encryption at rest secures stored data using encryption algorithms, protecting it from unauthorized access, while encryption in motion safeguards data as it is transmitted between systems or networks, ensuring confidentiality and integrity.

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.

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.

APPLICATION SECURITY

DDoS Protection

DDoS Protection is a cybersecurity solution designed to detect and mitigate Distributed Denial-of-Service (DDoS) attacks, ensuring the availability and performance of websites, applications, and networks by blocking malicious traffic while allowing legitimate requests.

Web Application Firewall

A Web Application Firewall (WAF) is a security solution that protects web applications by filtering, monitoring, and blocking malicious traffic, shielding against threats like SQL injection, cross-site scripting (XSS), and other vulnerabilities.

API Security

API Security ensures the protection of Application Programming Interfaces (APIs) from threats and vulnerabilities by monitoring, authenticating, and controlling API interactions, safeguarding sensitive data and maintaining application integrity.

Client-Side Protection

Client-Side Protection secures user interactions on websites by detecting and mitigating threats such as JavaScript-based attacks, data skimming, and formjacking, ensuring sensitive information is not compromised during client-side processing.

Attack Analytics

Attack Analytics is a tool that accelerates security investigations by providing a comprehensive view of WAF alerts, aggregating and analyzing security data to identify common characteristics and group related incidents for efficient response.

DAM

Database Activity Monitoring (DAM) is a security solution that provides real-time visibility into database activities, ensuring data security and compliance by monitoring access, detecting threats, and automating compliance reporting across diverse IT environments.

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.

DDI (DNS | DHCP | IPAM)

DDI (DNS, DHCP, and IP Address Management) is an integrated solution that automates and centralizes the management of domain name resolution, dynamic IP address assignment, and IP address tracking, ensuring efficient and secure network operations.

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 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.

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.

ZTNA

ZTNA (Zero Trust Network Access) is a security model that provides secure, conditional access to applications and data based on strict identity verification and continuous trust assessments, minimizing risks associated with traditional perimeter-based security.

DIGITAL RISK PROTECTION

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.

Dark web monitoring

Dark Web Monitoring involves actively monitoring hidden online forums and marketplaces on the dark web to identify and mitigate potential cybersecurity threats, including the sale or exposure of sensitive information.

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.

DIGITAL RISK PROTECTION

BAS / Red Teaming

BAS (Breach and Attack Simulation) and Red Teaming are cybersecurity practices that simulate real-world attacks on systems to identify vulnerabilities, assess defense mechanisms, and improve an organization's security posture through controlled penetration testing.

Continuous External Threat Management

Continuous External Threat Management involves the ongoing monitoring and assessment of external threats targeting an organization's digital assets, ensuring proactive identification and mitigation of potential security risks from external sources.

Infrastructure Monitoring

Infrastructure Monitoring involves continuously tracking the performance and health of IT systems, servers, networks, and hardware to ensure optimal functionality, detect issues, and prevent downtime or disruptions.

OUR REACH

Connect With Us!

https://www.jnrmr.com

+91-11-40513852

info@jnrmanagement.com

Our Presence On Social Media...