Information Technology Security:

In the current digital arena, where desired information is available at one's fingertips and accessible from anywhere at any time, data privacy and protection stand at great risk. Next-gen cybersecurity encompassing a holistic approach—right from detection to protection, prevention and remediation—is the need of the hour.

We, at Connect Enterprises, help our clients strengthen their Cybersecurity round the clock via our state-of-the-art Security Operations Center (SOC). We also enable enterprises to set up their own next-gen SOCs to effectively identify potential cybersecurity incidents, facilitating preventive action right in time. The SOCs help us counter Cyber threats with a cohesive and integrated approach—one that leverages powerful technologies such as Analytics, Machine learning and Automation.

The Connect Enterprises Cyber Risk Protection Platform (CRPP) integrates automation, deep analytics and correlation across multiple domains of security with the core objective of security orchestration and automation response (SOAR). While the world is striving to bolster security operations, our focus on automation powered by SOAR helps us offer next-gen cyber security for our clients. CRPP provides enhanced visibility and situational awareness across the network, endpoints and the Cloud with a single-pane view of management and reporting data.

Connect Enterprises' cybersecurity services offer a host of benefits, including:

- Integrated threat detection and response
- An analytics-driven framework to contextualize
- Tighter integration between data, processes and products with real-time visibility
- Cost reduction in incident response and compliance

Managed Detection Response (MDR) Services:

We pre-empt cyberattacks by leveraging the power of artificial intelligence (AI) and machine learning techniques to collects, analyzes and correlates threat data, helping us to successfully offer the following MDR services:

- Constantly collecting data to identify potential threats and provide an insight of any attack risk or vulnerability
- Utilizing specialized threat hunting expertise to discover security flaws in end points, user behavior, network and application
- 24/7 security monitoring and IR to detect threats, including system policy changes and compliance violations

- Triaging alerts with a data-driven approach and countering threat incidents right in time based on priority
- Investigating and managing breaches, eliminating the root cause of the attack and allowing users to quickly get back to business-as-usual

Cloud Security:

Our cyber security offering provides a holistic approach to cloud security, effectively protecting data applications and cloud system apps while ensuring regulatory requirements are met and business goals are not compromised on. Our services in the area include:

- End-to-end visualization of cloud assets and network topology
- Real-time rectification of misconfigurations
- Access provisioning to network ports on a time-limited basis according to client requirements, ensuring a closed-by-default posture
- Detecting security risks and threats through quick analysis of the network attack surface
- Advanced identity and access management (IAM) protection against both internal and external threats
- Round-the-clock tracking and automatic reversion of unauthorized changes, ensuring world-class security standards
- Security assessment and risk tolerance to evaluate our clients' security needs and develop a strong roadmap and architecture that supports their cloud ambitions
- Access management through robust processes and technologies that streamline access to the Cloud
- Application and infrastructure security services that enable design, development and implementation of secure cloud applications
- Cloud data protection and active defense mechanism
- We provide 24*7 security monitoring and IR services using cloud native tool

Endpoint Threat Detection and Response (EDR):

We actively look for unknown endpoint threats and respond immediately. We analyze the threats and once a threat is validated, we contain the compromised endpoints and take prompt action to protect against similar attacks in future. We offer the following services:

- Threat Detection: We actively track and scrutinize our clients' endpoints, users and their network activity to identify suspicious behavior, patterns and signatures that may be indicative of cyber threats

- Expert Investigation: Our team of experts determines the level of priority of alerts and investigates every probable security risk in order to identify true threats, while eliminating false positives
- Empowered Response: After detailed investigation, we notify our clients of confirmed threat detections along with elaborate and actionable context that helps them take immediate action irrespective of the location of affected systems

Cyber Analytics:

Our analytics-driven framework enables better contextualization to customize cyber analytics services for our clients. We integrate user and entity behavior analytics (UEBA) with third-party security information and event management (SIEM) to successfully manage investigations, automate tasks and remediate breaches. Our services in the area include:

- User/entity behavior profiling, segmentation, visualization and high-risk user/entity outlier detection
- Machine-learning based anomaly detection in internal and external connections, analyzing why an outlier led to an alert, and assigning a risk score to detected threats
- Advanced threat hunting powered by an exhaustive and fast search capability
- Data analytics with extended user/entity intelligence covering logon/log off events, AD events, remote login patterns and network usage
- Network analytics with reports on network bandwidth usage, connection count, DNS resolutions, etc.
- Dynamic entity link analysis with user mapping, detection and highlighting of hidden relationships between users, IP addresses and domain demonstration

Advanced Threat Protection:

We go beyond traditional point-in-time detection and offer innovative advanced threat protection services that promptly identify attacks and alert client organizations, enabling quick mitigation. Our offerings encompass:

- Cloud-based Big Data and machine learning practices for constant detection, assessment and management of vulnerabilities and advanced malware
- Red teaming services that help simulate cyber-attacks and test their ability to effectively counter them in a safe way
- Application, device, mobile and network penetration testing and remediation to evaluate and consciously attack IT infrastructure vulnerabilities
- Security code review to identify security flaws in an application's source code and initiate an overall risk mitigation exercise that will lead to lesser vulnerabilities in future

- Indicator of compromise (IOC) analysis to detect and counter potentially harmful activity on the client network by automatically co-relating the activity to greater attacks
- Retrospective security analysis, helping enterprises to investigate the full extent of a cyber-attack and evaluate appropriate remediation measures

Advanced Network Security Managed Services:

Experts at our SOC help clients leverage the latest technologies to ensure robust network security. Our services encompass:

- Readiness Assessment: Analyzing the current infrastructure landscape to gauge readiness to deploy and derive value from network security management, aligning requirements with business performance
- Technology Selection: Choosing the right technologies and strategic planning on the basis of security, compliance and business performance goals
- Solution Deployment: Leveraging our proven implementation and integration strategies to enable greater returns on network security investments
- Security Optimization: Relooking into technology decisions; configuring and fine-tuning solutions to enhance efficiency and network security
- Managed Network Security Management: Remote tracking of network health and security

IoT Security:

We offer complete end to end security services for IoT platform to protect IoT devices from cyber-attacks, reducing endpoint complexity and securing its integration with CRPP:

- IoT Security assessment and testing
- IoT threat detection: Network traffic analysis, IoT device profiling and pattern detection to identify any deviation from normal behavior
- Security solution Implementation and Management services

Certifications

- Red Hat Certified Architects (RHCA)
- Red Hat Certified Engineers (RHCE)
- VMware Certified Professionals (VCP)
- Puppet Certified Professionals
- MapR Certified Professionals
- Cisco Certified Network Administrators (CCNA)
- 8 AWS Business Accredited Professionals

- 9 AWS Technical Accredited Professionals
- 2 AWS Certified Solutions Architects
- 5 Architecting with AWS Certifications
- Oracle Platinum Partner: Oracle Enterprise Linux Specialized
- Amazon Advanced Consulting Partner
- Microsoft Silver Cloud Competency