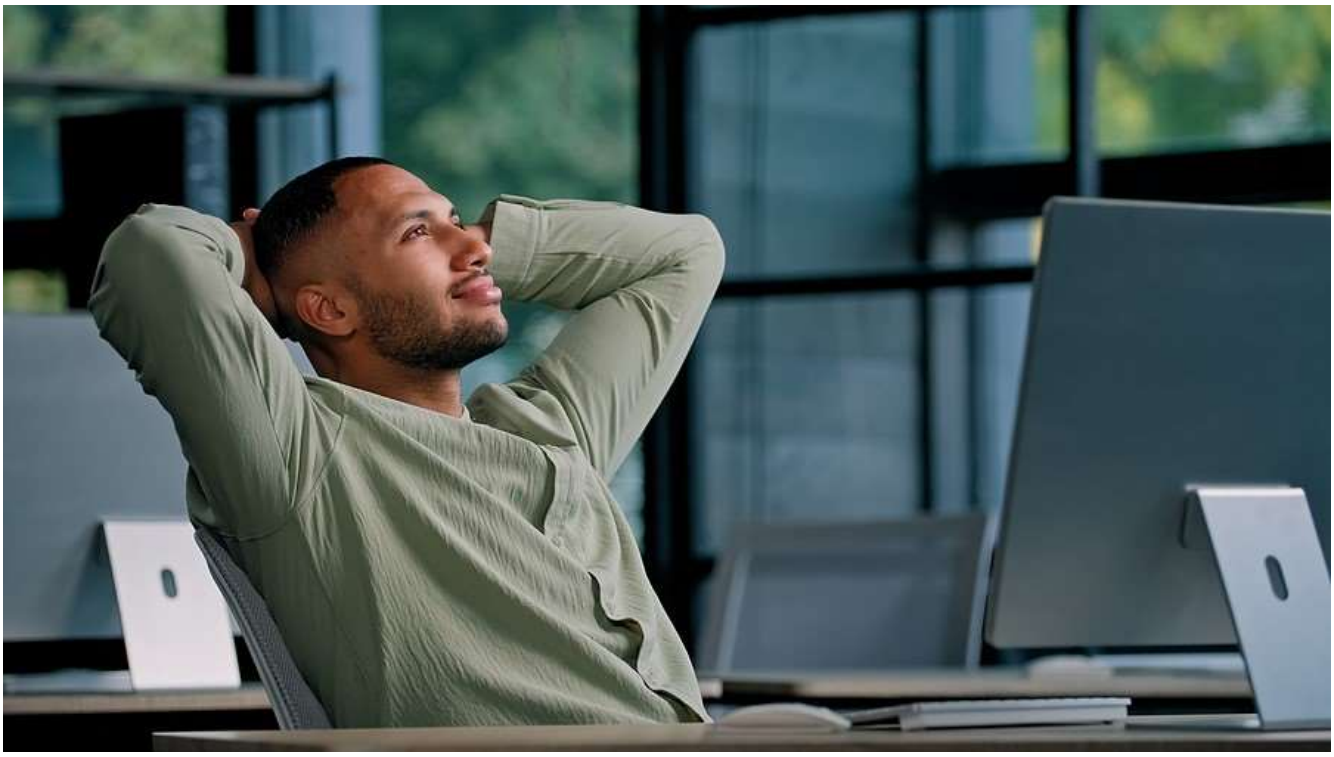
Tackle Cyber Threats Head on with Affordable, Scalable Cyber Security Solutions



Cyber security has emerged as a leading business concern affecting organizations of all sizes and in all industries. Defending devices, systems and data from malicious attack requires the right blend of cyber security solutions. These solutions must adapt to address specific business needs, such as cloud computing and remote work, as well as an evolving threat landscape.

The certified cyber security professionals at eMazzanti deliver a menu of security services, ranging from 24/7/365 monitoring to email protection, security awareness training and penetration testing. Cost-effective and scalable, these solutions take a proactive approach to security, reducing risk and downtime and delivering peace of mind.

Network Security and Monitoring

Protect any device, anywhere with cloud-delivered network security and web filtering. 24/7 monitoring, enhanced by big data analytics and machine learning, means even small businesses benefit from enterprise-grade threat detection. And the solution stops 50 to 98 percent more attacks than firewalls and antivirus alone.

eCare Secure Route provides automated, comprehensive threat protection. Stop phishing and malware infections early, quickly identify and isolate infected devices and prevent unauthorized data transfer. Additionally, the cloud services report delivers visibility into off-network usage of cloud services, a critical tool in securing a remote workforce.

Take security a step further with eCare Security Operations Center (SOC). This SOC-as-a-service solution provides 24/7 automated monitoring of on-premises and cloud environments. Our security engineers utilize multiple security information and event management (SIEM) technologies, backed by dedicated security experts providing "eyes on" analysis.

With eCare SOC, customers gain access to highly trained security experts. Using industry best practices, response teams initiate threat mitigation and remediation either remotely or on-site. This managed detection and response (MDR) proactively protects against ransomware and other threats.

Email Protection and Security Awareness Training

More than 90 percent of targeted cyber attacks begin with an email. For instance, unwitting users click a malicious link, respond to a cleverly disguised phishing attempt, or send sensitive data through email. A combination of technology and security awareness training provides essential protection.

Designed specifically for small to medium businesses, MXINSPECT leverages leading technologies to protect organizations from email threats. This includes filtering both inbound and outbound emails to block harmful content and protect against inappropriate sharing.

Additional features include dynamic analysis of URLs and attachments, policy-enforced encryption and data loss prevention and social media account protection. With a cloud-based platform, administrators manage user and account settings from a single dashboard. Email classification and filter rules deliver the granular control you need.

Because technology alone will not ensure protection, MXINSPECT also includes security awareness training modules designed specifically for small businesses. Customized for your organization, engaging training content reduces successful phishing attacks and malware infections by changing user behavior. Phishing simulations enhance learning.

Dark Web Monitoring and Identity Theft Protection

Cyber criminals know that stolen credentials, such as usernames and passwords, provide the keys to the kingdom. Consequently, the Dark Web includes a brisk trade in digital credentials. Users typically do not know when their credentials have been compromised. And because employees often re-use passwords, a stolen credential poses a significant threat.

With Dark Web monitoring through MXINSPECT, your organization can detect and respond to compromised credentials or stolen customer data before a major breach occurs.

Penetration Testing

One of the best ways to identify security gaps involves penetration testing. Pen testing simulates a real-world attack in controlled conditions. During testing, an expert ethical hacker attempts to locate and exploit system vulnerabilities using the same tactics a malicious hacker will use.

Conducting pen testing reduces security risks by highlighting weaknesses and suggesting strategies for improvement. Our pen testing team has conducted thousands of pen tests, combining manual testing with a world-class penetration testing framework. Customers use the results to determine security investments and mature their strategy.

Additional Cyber Security Solutions Ensure Comprehensive Protection

eMazzanti offers a full selection of customizable cyber security solutions. For instance, in addition to the solutions described above, customers can benefit from an affordable, easy-to-implement multi-factor authentication (MFA) solution. And our eCare Cloud Backup mitigates risk with unlimited backups and data protection for Microsoft 365.

To pull it all together, eMazzanti provides a series of on-demand cyber security workshops on essential security topics. These include endpoint security, MFA, securing the remote workforce, ransomware and more. By partnering with eMazzanti, your company benefits from world-class security tools and award-winning cyber security expertise.