{e}mazzanti technologies

Cyber Crime: Challenges and Solutions

Microsoft Solutions Partner

eMazzanti.net

WatchGuardONE PLATINUM PARTNER

The eMazzanti Team

Carl's QR code

Carl Mazzanti

Co-Founder & President of eMazzanti Technologies

carl@emazzanti.net
(844) 360-4400 x4410
www.emazzanti.net

Over 20 Years of Experience in IT and Solutions for Organizations

Quick Facts

- Founded in 2001, over 20 years of customer success
- Average accelerated revenue growth 20% each year
- Nine years on Inc. 5000's list for fastest growing privately held companies
- WatchGuard 5x Partner of the Year, First International Platinum Partner
- Microsoft 4x Partner of the Year & Finalist. Multi-year Microsoft Recognition.
- Microsoft GOLD Partner & Top 200 Worldwide VAR
- Member of PCI Security Standards Council
- QIR and CISSP Certified Employees
- IAMCP P2P Awards 2022 Americas Winner
- 2x Recognition of Tech Elite 250 List
- 5x Recognition of MSP500 List
- 3x Recognition of NJBIZ Digi-Tech Innovators Award
- 6x Top 100 Retail Vertical Market MSP
- Clutch: Global 1000-Top B2B Companies Globally, #1 NYC Managed IT Service, Ranked 2nd Among Top NYC IT Consultants
- 2x EY Entrepreneur Of The Year® Award Finalist
- 2020 Cover of Entrepreneur Magazine: Businesses that have thrived in uncertain times
- 2020 World's Best 101 SMB Managed Service Providers
- CIANJ - 2019 Companies That Care: Champions of Good Works Award
- 2018 NJMEP Innovator of the Year Finalist
- 2018 Acquisition of Messaging Architects
- 2017 NJBIZ New Jersey Business of the Year & NJMEP Manufacturer Innovator of the year
- 2017 Acquisition of ForceWorks Microsoft Partner of the Year in Dynamics
- 2016 Acquisition of Liqui-Site, award-winning Digital Marketing Agency
- 2016 NJBIZ Business of the Year Award
- 2015 Acquisition Cloud Services Team dedicated to Azure Services & implementation
- 2015 US SMB Champions Club Eastern Regional Compete Partner of the Year

Microsoft Solutions Partner

WatchGuard 5x Partner of the Year

Inc. 5000 9x Recognized

#1 Retail MSP USA
#4 MSP NYC

Support

{e}mazzanti technologies

International Support in Multiple Languages

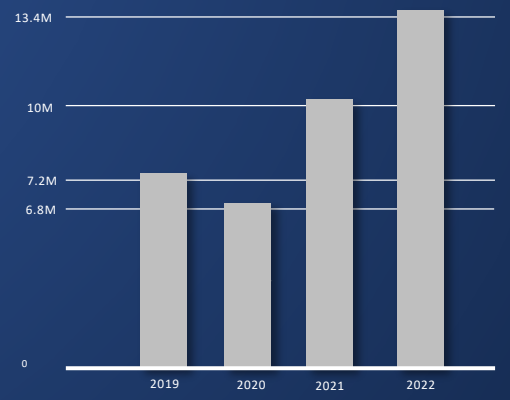
Spanish, Italian, French, Albanian, Sinhalese

Support Available 24/7 x 365

Offices on the East and West Coast

Global offices in Canada, Europe, Middle East & Asia

Certified Engineers & Developers to perform Network Services, Cloud Support, and Digital Marketing



Growth

What is Cybercrime?

Cybercrime is big business. In 2022, the FBI's Internet Crime Complaint Center (IC3), recorded more than 800,000 complaints with losses totaling $10.3 billion.

Top Threats Include:

- **Malware:** software used to gain unauthorized access to IT systems in order to steal data, disrupt system services or damage IT networks.
- **Ransomware:** a type of malware deployed by that disables files or systems until a form of payment or ransom is provided.
- **Cryptoviral** extortion can encrypt the victim's files, making them inaccessible unless payment is made to decrypt them.
- **Phishing:** online scams that use deceitful or misleading tactics to trick users into sharing private information.
- **Business Email Compromise** uses social engineering or computer intrusion techniques to trick users into enabling unauthorized transfers of funds.

Scope of Cyber Crime and Latest Outbreaks

- Cyber-crime is growing exponentially — the cost is predicted to hit **$8 trillion** in 2023 and will grow to **$10.5 trillion** by 2025.
- **In March 2023**, hackers exploiting the GoAnywhere vulnerability took employee information from consumer products giant **Procter & Gamble**.
- In February 2023, unauthorized individuals gained access to the protected health information of up to 1 million **Community Health Systems** patients.

- In **March 2023**, 63 **breaches** of 500 or more records were reported to the Department of Health and Human Services' Office for Civil Rights, which is a 46.51% increase from February, 6.92% more than the 12-month average, and 40% more breaches than in March 2022.

Established & Emerging Threat Vectors

- Long-buried assets, including **credentials** in ex-employees' hands; or unused **credit** or other accounts at a retailer or professional services firm are easy targets for **hackers**.

- These assets are not actively monitored but retain **important data**, that, like Hollywood zombies, can be reanimated by hackers and sold on the "**Dark Web**."

- **Dark Web Monitoring Services** use human and sophisticated intelligence search capabilities to identify, analyze, and proactively hunt the Dark Web for compromised or stolen employee and customer data.

- **ChatGPT** is a powerful business tool, but competitors may use it to access sensitive data directly through data scraping, or indirectly via social engineering.

- **Layered defenses**, including **encryption, monitoring** network activity, **and limiting access** to sensitive information may **mitigate** this kind of threat.

Bots Never Sleep

- ChatGPT bots and other **bots** — which automate certain tasks — are useful, but also vulnerable to a takeover, where malicious actors use the bots to gain control of certain processes.

- Hackers do this by **exploiting vulnerabilities** in **code**, or by guessing a user's password.

- Using strong **authentication protocols**, keeping up with security updates and **software patches** may reduce vulnerability to this attack vector.

SOCs and SIEMs

- Threats are inevitable. **Security Operations Center (SOC)** monitoring, 24x7, is an answer.
- An **effective Cyber Security provider** should have the technology, people, and processes to deliver SOC services, featuring premium multilevel continuous monitoring that is cost-effective, and scales as client businesses evolve.
- **Security Incident Event Monitoring (SIEM)** is a kind of distant early warning system.
- SIEMs continuously review device and application logs on a **real-time** basis.
- They will **flag** suspicious activity and can, if enabled, launch immediate **responses** designed to shield the system.

Security on the Cloud

While Cloud Computing is now a common tool for businesses – **Security is still a concern and a big challenge for most.**

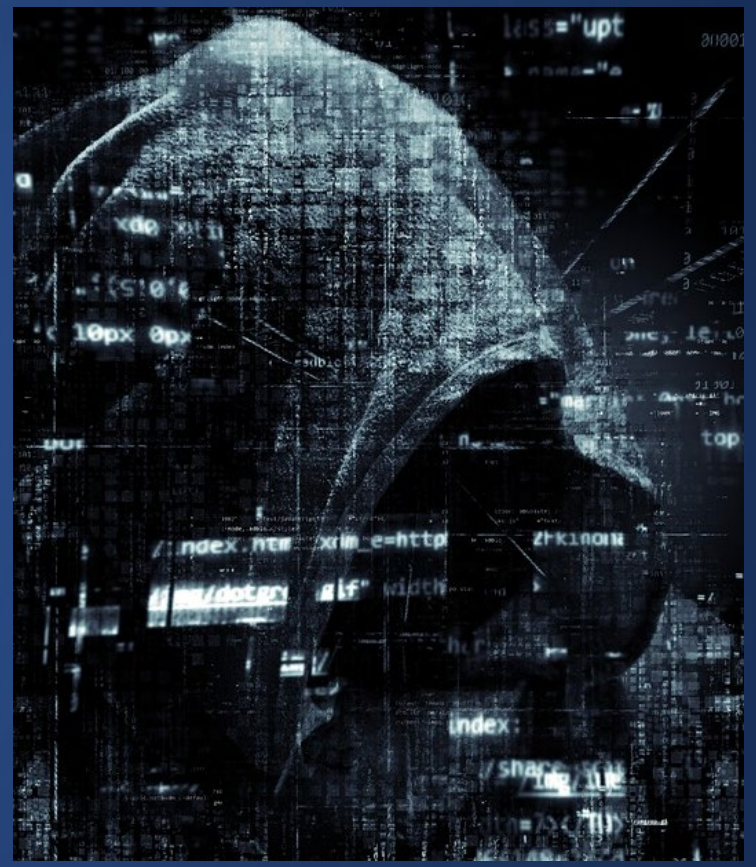
- Physical Security is not an option.
- Moving Data represents big concerns in terms of security and compatibility.
- Who owns the encryption/decryption keys?
- A common standard to ensure data integrity does not yet exist.
- Users must keep up to date with application improvements to be sure they are protected.

Can you Catch a Hacker?

The most seasoned and skilled hackers fake their web addresses and write self-erasing code.

Furthermore they can route their attacks through the devices of innocent victims and make it appear that they are in multiple countries at once.

This makes catching them very hard. That is why prevention plays a huge role in the game



Paying the Ransom IS NOT an Option

Paying Makes you a **great customer**, **be prepared to be hit again.**

What can you do now

- Automation such as eCare Agents
- Layers of Security
- Email Filtering
- Constant Vigilance
- Firewall Geo-Blocking

Automation such as eCare Agents

We provide system automation **premier security agent** designed to keep you protected. The entitlements are what you need to stay safe:

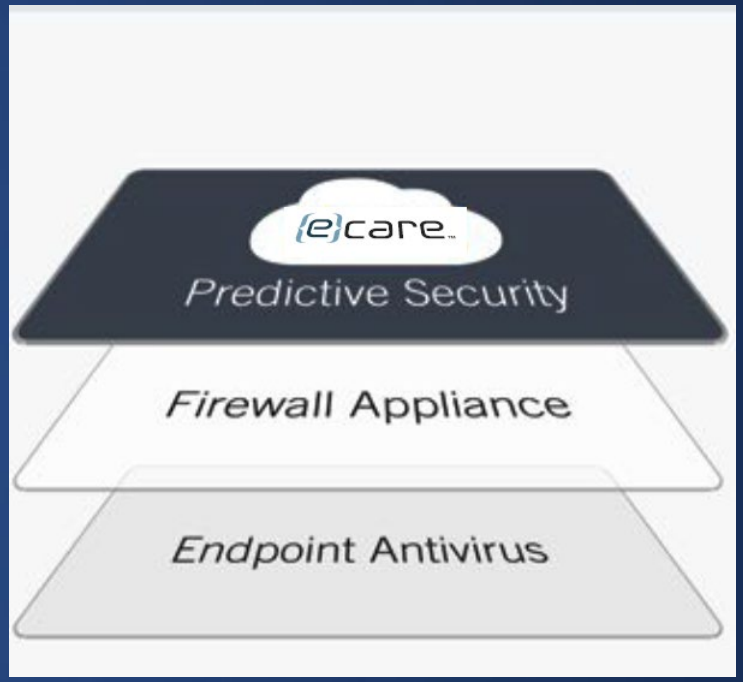
- **Lock down systems to stop malware, ransomware, zero-day, and non-malware attacks**
- **Built-in file-integrity monitoring, device control, and memory protection to block unauthorized change**
- **Harden new and legacy systems with broad support for embedded, virtual, and physical OS**

Layers of Security

- **eCare Secure Route** not only **blocks malware, botnets and phishing** over any port, protocol or app, but also **detects and contains advanced attacks** before they can cause damage.

- **eCare Secure Route stays always up-to-date** with no hardware to install, no software to maintain and no admin intervention required.

- **eCare Secure Route uses DNS** to intelligently route our users around Internet threats, but also to speed up the Internet and move the state of the art for the Domain Name System forward.



Email Filtering

- 30% of recipients open **phishing messages** and 12% **click on attachments**.
- 94% of **malware** is delivered via email
- **$17,700 is lost every minute** due to phishing attacks

In uncertain times, the last thing you need is to add panic about email security to your list of worries.

Instead, **partner with a trusted email consultant** and **Cyber Security provider** to implement the necessary protections that will provide peace of mind.

Geo-Blocking

Where are your offices headquartered?
Unless you have an international presence that MUST be open to all countries, you're leaving yourself open to international hackers.

Once you identify what countries would need access to your website for business, you can block the others! **Not doing business in Russia? Block them!** This can be easily filtered through your firewall or GEO based policies such as in Office 365.

Penetration Testing (PEN Testing)

Testing your systems, your website, and **infrastructure** simply means that we are attempting to discover your vulnerabilities before cyber criminals do.

These vulnerabilities may exist in operating systems, service and application flaws, improper configurations, or risky end-user behavior.

Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-user adherence to security policies.

Constant Vigilance

Things will never improve without a watchful eye and a proper partner.

How to Stay Protected – Best Practices

Though ransomware can be an expensive and difficult software to deal with, it is easy to prevent if you take the right steps:

- **Automation such as eCare Agents –** Preventative Controls
- **Layers of Security –** One system alone is not enough. Where one fails, another should succeed
- **Email Filtering –** For example, do not open any unexpected attachment or click any email links, even if they appear to be from a sender you know
- **Geo-Blocking –** Only allow connections to and from where you do business
- **PEN Testing -** Discover vulnerabilities before cyber criminals do
- **Constant Vigilance –** Security is an evolution

QUESTIONS?

THANK YOU

701 Grand St, Hoboken, NJ, 07030 | T 844.360.4400 | info@emazzanti.net | emazzanti.net

The eMazzanti Team

Carl's QR code

Carl Mazzanti

Co-Founder & President of eMazzanti Technologies

carl@emazzanti.net
(844) 360-4400 x4410
www.emazzanti.net

Over 20 Years of Experience in IT and Solutions for Organizations