CORE 6+

BUSINESS NETWORK SECURITY PLUS

Systemized, Real-Time Business CyberSecurity

Designed specifically for Small Businesses and Nonprofits, our CyberSecurity platforms provide multi-layered, comprehensive protection for your network's core components.

Understanding The Core 6+ Solution

The Most Cost-Effective CyberSecurity For Small Business And Nonprofits

It Is My Position That Small Businesses and Nonprofit Organizations Have Been Historically Under-Served, Over-Charged, Or Both…

Which Is Exactly Why I Created A New Managed Services CyberSecurity Offering Specifically For Today's Small Businesses And Nonprofits Without All Of The Hidden Fees And Over-Charging…

WHERE THEY ONLY PAY FOR THE SERVICES THEY ACTUALLY GET!

I've made it my mission to help every Small Business and Nonprofit get the Absolute Best CyberSecurity Available…

And Deliver It At A Rate They Can Actually Afford!

TRS Technology Solutions | CORE 6+ BUSINESS NETWORK SECURITY PLUS | NSP MS NETWORK SECURITY & PERFORMANCE | BASE 4+ PRIMARY COMPUTER SECURITY PLUS | 501(c)3 TECHNOLOGY INITIATIVE | 10G

Understanding The Six Core Components Of Your Business Network Security

Network Security Is All About Taking A Layered Approach…

There Is *NO* One-And-Done, All-Is-Protected Application!

You must have multiple layers of protection in your business network to make sure each single defense component has a backup, just in case of a flaw or missing coverage.

Core 6+ Is A Comprehensive, Multi-Layered Concentric Approach To Network Security.

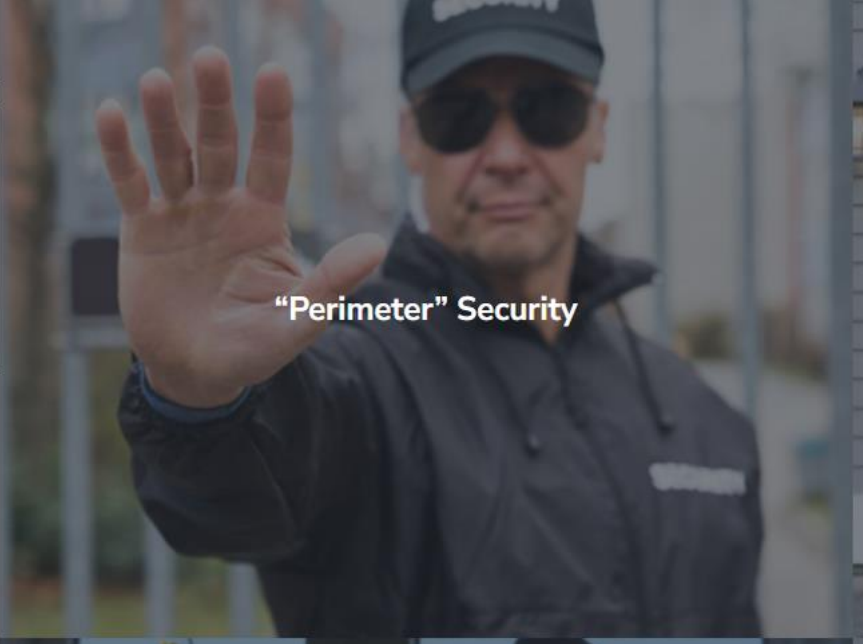
Our Goal Is To Make Understanding Your Business Network As Easy As Possible

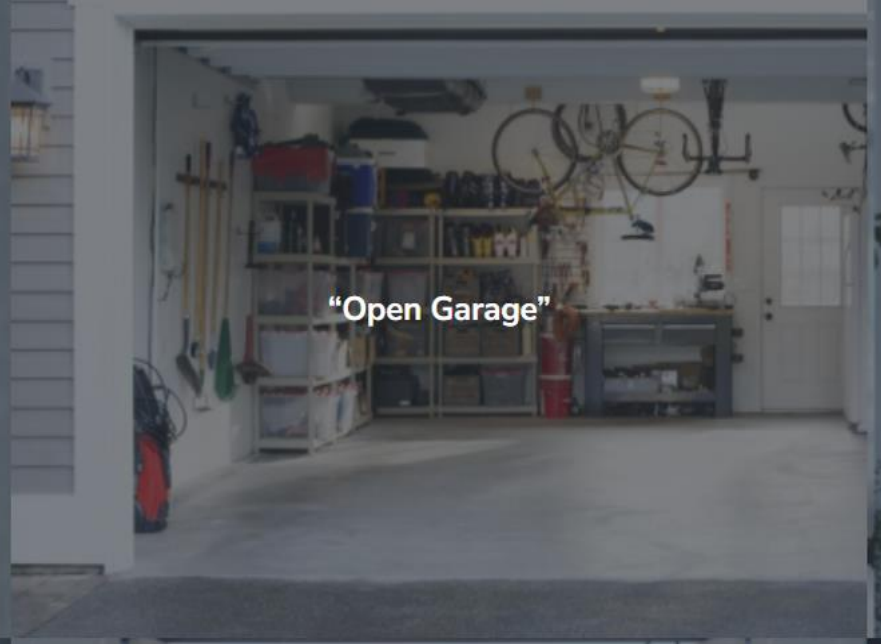
Understanding The Six Core Components Of Your Network

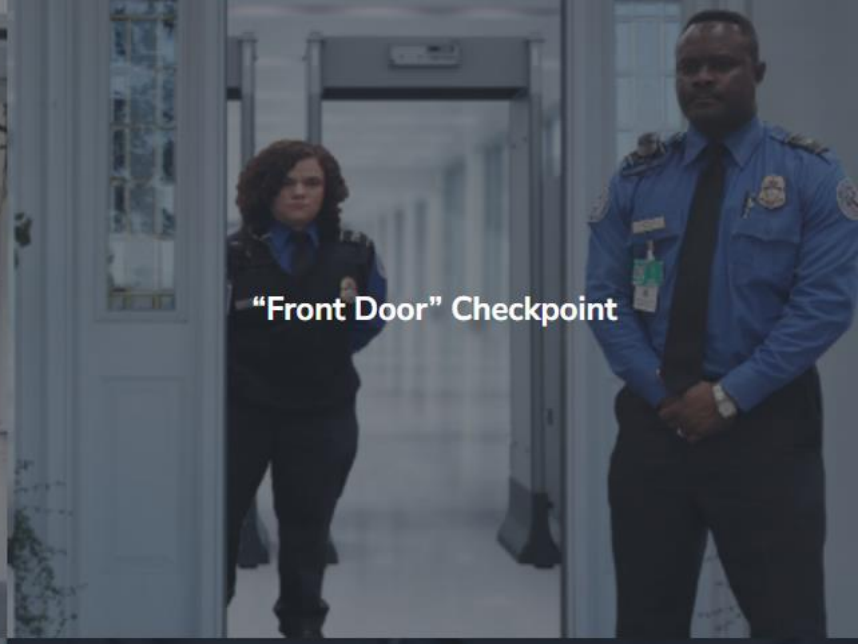
A Simple Analogy That Hits Home

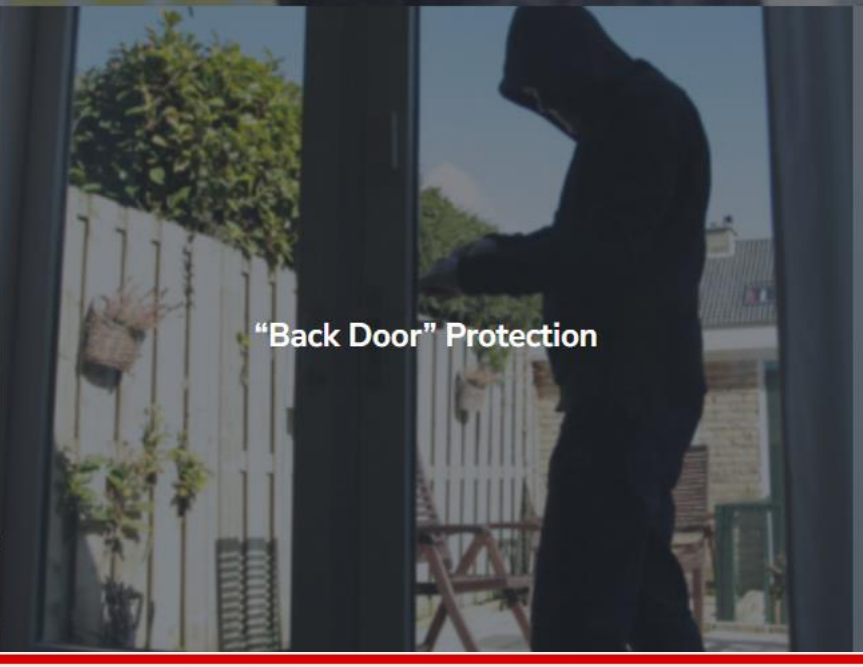
In an effort to make the Core 6 Components of Network Security easy to understand, we use The Homestead Analogy:

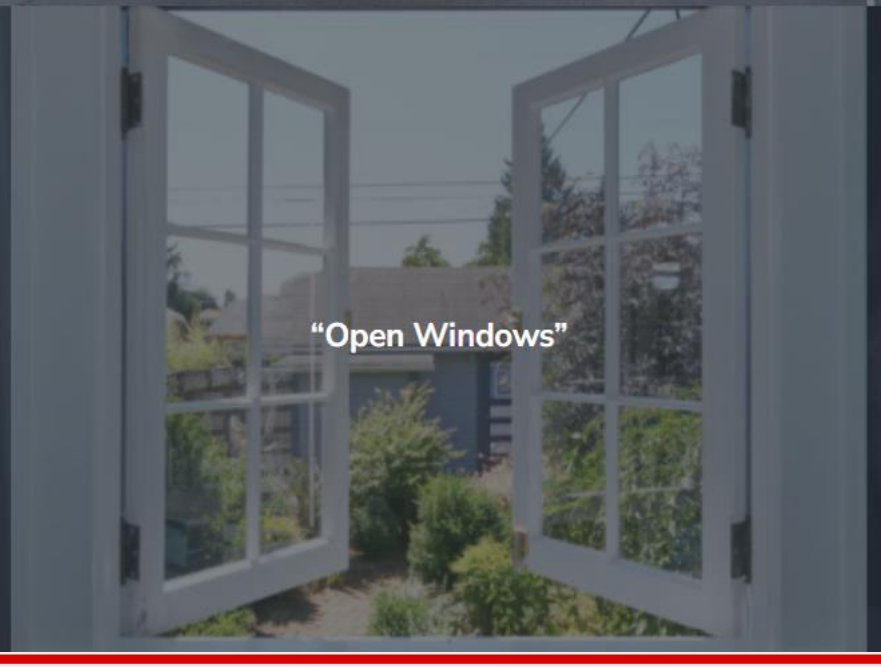
- **“Perimeter” Security**
- **“Open Garage”**
- **“Front Door” Checkpoint**
- **“Back Door” Protection**
- **“Open Windows”**
- **Extra “Insurance”**











TRS Technology Solutions

CORE 6+ BUSINESS NETWORK SECURITY PLUS

NSP MS NETWORK SECURITY & PERFORMANCE

BASE 4+ PRIMARY COMPUTER SECURITY PLUS

501(c)3 TECHNOLOGY INITIATIVE

Your Router Is Literally Your "Property's" Protection From The Outside World

Your Gateway Router Is Your First-Line Of Defense

It's Where The Internet Meets Your Business

Most routers, "screen" inbound traffic to determine whether they are allowed in, and to some extent—*depending on how sophisticated the router is*—they may also "screen" to verify the level of potential threat and/or risk to your "property."

Current "Next Gen" Security Routers Check In Daily With Multiple Sources To Get The Most Current Lists Of Threats And Cyber-Criminals To Make Sure They're Blocked At The "Gate."

Another thing *Only Current "NEXT GEN" Routers* do, is they will actually check all of your exiting Internet traffic (or network "visitors") to verify that "someone" they let in, thinking they were safe, isn't actually trying to do you harm or steal any of your information.

Your Wireless Network Is Often A Wide-Open Invitation For Unwelcomed Guests

This Is – BY FAR – The Biggest "Open Door" On Your Entire "House"

You Must Prevent Unauthorized Access

With wired networks, it's extremely difficult to steal bandwidth, which is one of the biggest problems with wireless. If not secured correctly, others can access your wireless and use your Internet even while they are in a neighboring building or sitting in a car outside.

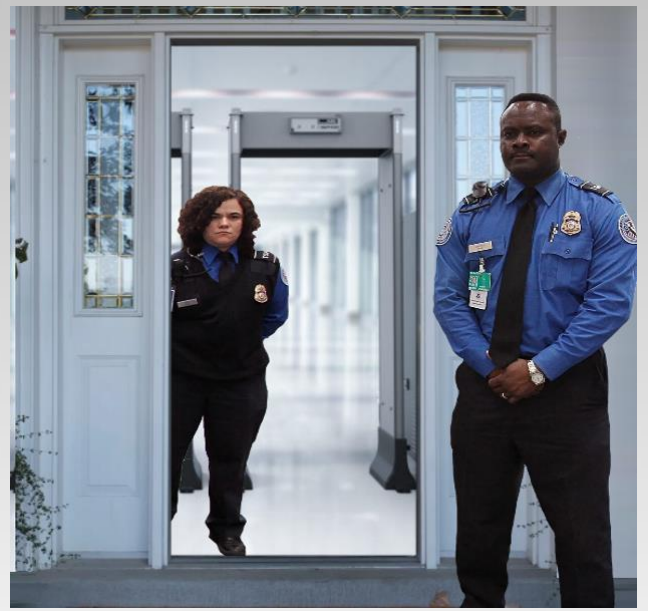
Unauthorized Wireless Users not only decrease your Internet access speed, but they are a HUGE SECURITY RISK because these unwanted users may hack your computers or share viruses and malware from their own computers…

Wireless network security is the process of designing, implementing and ensuring security on a wireless network. It is a subset of network security that adds additional protection for the wireless network to help prevent unauthorized and malicious access attempts.

Most Threats Come Straight In Through The "Front Door" – Like Your Incoming Email

Traditional Anti-Virus And Anti-Malware Is Not Enough

REAL-TIME! Managed EDR Is A Far Superior Solution



Traditional AntiVirus Tools are "scan-based" applications that **cannot** keep up with today's new, sophisticated and ever-growing malware threats.

Managed Endpoint Detection and Response (EDR) safeguards your computers, network and data, by providing REAL-TIME, ALL-OF-THE-TIME Monitoring, Protection, Detection, Response and Even Includes Automated Remediation and Rollback.

Managed EDR monitors ***(in Real-Time)*** your system processes Before, During and After execution and utilizes artificial intelligence (AI) to detect and prevent both current and emerging threats. ***Managed EDR Can Even "Rollback" Ransomware!***

“Back Door” Web Threats, Like Adware, And Phishing Sites Have Never Been Greater

Web Protection and Content Filtering
Helps Keep Your User’s Safe

Web Protection, and it’s included Content Filtering application, is very different than the Managed EDR. Digitally speaking, Web Protection helps eliminate the Internet Bad Guys from “***sneaking around back***” to find an unmonitored entrance and gain easy access to your “property” with you knowing.

Web Protection Provides A Safeguard For Your Users Who May Accidentally Surf Seemingly Innocent Websites That End Up Containing Concealed Malware.

We can even use this layer of protection to (individually) deny access to recreational, non-business, and non-productive sites, such as those used for social networking, gaming, instant messaging, etc., thereby increasing overall productivity of your staff.

By Keeping Your "Windows Locked" You Are Mitigating Your Most Serious Security Risks

Keeping Your Network Safe Requires Constant Vigilance

Keep Everything Up-To-Date

You need to always make sure all systems and applications are up-to-date with the latest security patches. So, even if an undesirable does get "on your property," there's still a very low probability they can and/or will actually get in.

Cyber attackers typically search for easy ways to breach a network. Often, this involves "soft targets," such as software that is not updated to protect against known malware.

Our Patch Management solution can handle every facet of patching on Windows, Mac and Linux operating systems. It discovers all relevant and essential service packs, security updates and other "hot-fixes" available for each of your protected devices, and if so desired, we can install the updates, or at the very least, notify you of the needed update(s).

Basic Document Backup and/or Full Data Backup Is The X-Factor… It's Your Insurance!

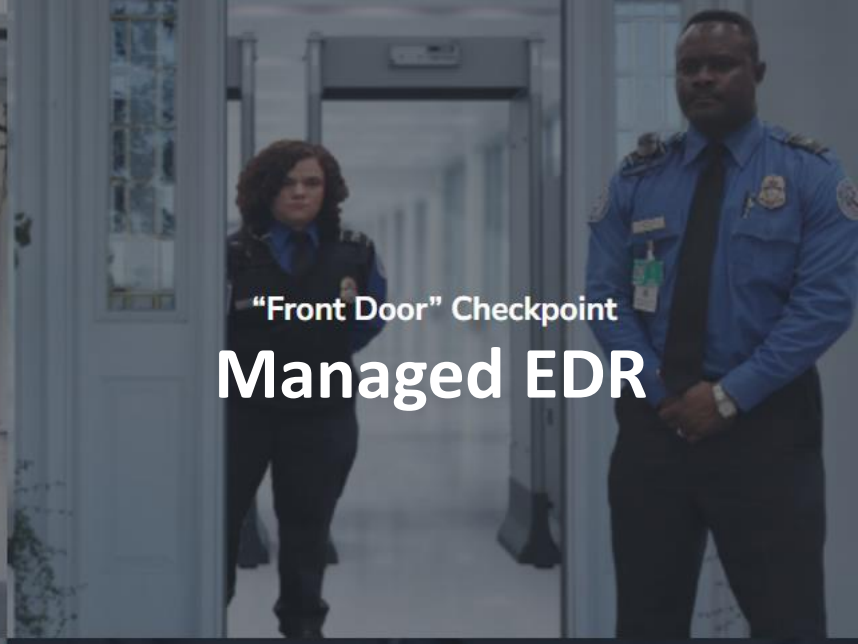
A Simple Truth: Hardware And Equipment Will ALWAYS Fail… Eventually.

You Must Protect Your Data!

People have accidents, make bad decisions, or sometimes just don't know any better… Occasionally, there ***is*** malicious intent from inside your trusted staff: People who will purposefully destroy, not only your trust, but your business data..

Data loss can cause serious financial hardships for a company, and system downtime can cripple productivity, preventing a business from providing good service to customers. That's why it's critical to be prepared with the right technology.

Our Basic Document Backup and Disaster Recovery layer provides customers with the confidence that if their data should ever become compromised, corrupted or deleted, it can be recovered safely and securely.



TRS Technology Solutions

CORE 6+ BUSINESS NETWORK SECURITY PLUS

NSP MS NETWORK SECURITY & PERFORMANCE

BASE 4+ PRIMARY COMPUTER SECURITY PLUS

501(c)3 TECHNOLOGY INITIATIVE

Gateway Router

“Perimeter” Security

SonicWall Network Security Next-Generation Firewalls (NGFW) Include Advanced Threat Protection, With The Security, Control And Visibility Small Businesses And Even Global Enterprises Need To Maintain An Effective Security Posture.

SonicWall TZ370 Series

Comprehensive Entry Level Next-Generation Firewall

SonicWall’s award-winning hardware and advanced technology are built into each firewall to give you the edge on evolving threats. With solutions designed for networks of all sizes, SonicWall firewalls are designed to meet your specific security and usability needs, all at a cost that will protect your budget while securing your network.

Protect your small business or branch location from intrusion, malware and ransomware with an easy-to-use, integrated security solution designed specifically for your needs. SonicWall TZ firewalls deliver enterprise-grade protection without the cost or complexity.

Managed EDR

"Front Door" Checkpoint

Endpoint Detection And Response (EDR) Actively Prevents, Detects, And Quickly Responds To Ever-Changing Cyberthreats With Behavioral AI Threat Detection, Automated Remediation, And Even Rollback… Including Ransomware!

Real-Time Managed EDR replaces the Scan-Based Managed Anti-Virus to protect your business against the latest threats in REAL-TIME, without having to wait for recurring scans or malware definitions to update.

Managed EDR harnesses the power of multiple AI detection engines to analyze new threat patterns and machine learning to evolve response.

Managed EDR responds effectively in REAL-TIME with automatic threat containment, as well as "Kill," Quarantine and Remediate, including the roll back of endpoints and compromised files to their pre-attack healthy state.

Wireless Security

"Open Garage"

By Having A Wireless Network In Your Business, You Certainly Get To Take Advantage Of The Convenience And Potential Cost-Savings Of Users Not Being On A Wired Connection, But There Are Significant Risks If Not Secured Appropriately.

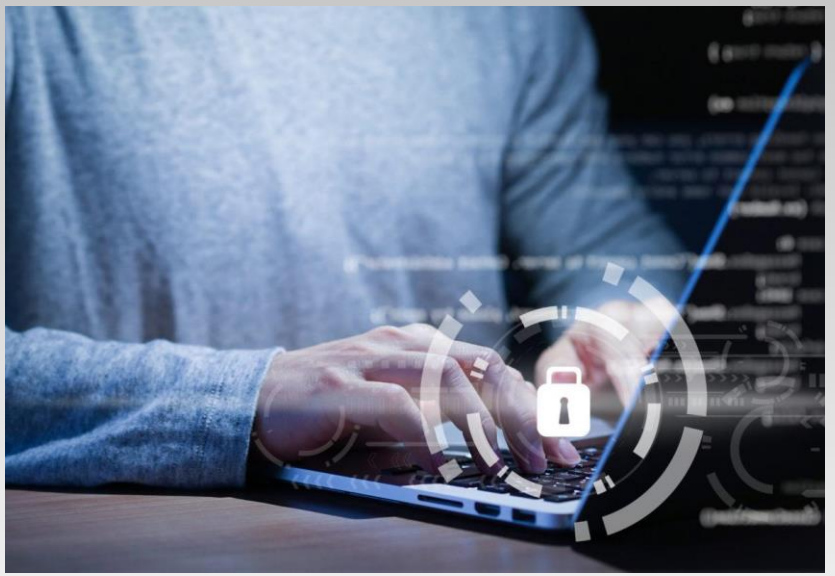
When your Wireless Network is not secured and "locked down" effectively, hackers can intercept any data/information you send or receive, as well as gain access to company files, or other computers on the network, or may even be able to access your online bank accounts or credit card portals.

There are a number of simple steps that can be taken to quickly and easily safeguard your Wireless Network. The more up-to-date and current your Wireless Access Point (WAP) is, the more options we have to provide more sophisticated security settings to protect your business and users.

Web Protection

“Back Door” Protection

Advanced Web Protection Is An Effective Way To Improve The Overall Security Of Your Business’ IT Systems. By Blocking Malicious Or Unwanted Traffic At The DNS Level, We Can Minimize The Threat Of Access To Your Systems And Data.



Businesses can be vulnerable to DNS Spoofing Attacks, in which attackers redirect DNS traffic to fake or malicious sites. Advanced Web Protection protects your computers against DNS spoofing.

Advanced Web Protection is a layer of security that complements and goes beyond traditional content filtering, antivirus, and firewalls. It helps keep your employees safe and productive as they browse the web by giving you granular control of the websites your employees can access.

Web Protection helps improve overall security and workplace efficiency.

Patch Management

"Open Windows"

With Cybercriminals Becoming More Sophisticated In Their Attempts To Access Company Systems And Data – And With Companies Taking On More IT Assets And Applications Than Ever Before – Patch Management Is Crucial.

Increasing concerns surrounding cybersecurity means that an effective patch management policy and implementations best practices are crucial for helping keep your business' computing environments secure.

Our Core 6+ systems can inventory your connected computer's hardware and software components, ensuring relevant devices and applications are accurately accounted for.

This way we can better align and stay on top of which devices need which security updates and patches and run or share as per our Patch Agreement.

Data Backup

Extra “Insurance”

There Are Multiple Types Of Data Backup Solutions And Tools That Deliver Different Levels Of Data Protection. Protecting Your Critical Data Is A Key Component To A Company’s Disaster Recovery Plans And Business Continuity Strategies.

Companies and people are very dependent on data. Whereas a person cannot survive without air, water, and food, businesses cannot survive without data. It is extremely important that your company has a backup strategy and solution in place. Otherwise, you could be a statistic.

Basic Document Backup is included with every Core 6+ and/or Base 4+ Solution. You can choose to upgrade to the Full “Metal” Backup Solution if you want true device level recovery or have pictures/videos to backup…

We also have a Microsoft 365 Backup Solution if you’re using Office 365.

Email Protection

"Add-On" Service

Mail Assure Helps Safeguard Against Phishing, Spam, Viruses, Ransomware, Social Engineering, And Other Email-Borne Threats. Mail Assure Blocks 99.84% Of All Malware, As Tested And Validated By "VIRUS BULLETIN" Product Test Suite.

Mail Assure is a cloud-based email security solution that protects both inbound and outbound email using collective threat intelligence, 24/7 email continuity, and even includes long-term email archiving.

Mail Assure safeguards clients from email threats and downtime, stopping constant phishing attacks and other malware emails.

Even if a business has a primary layer of security, as with MS365, Mail Assure provides added control and additional defense, built to protect against spam, viruses, malware, phishing, ransomware, and other email threats.

Risk Intelligence

"Add-On" Service

Risk Intelligence Scans The Computers For Any Unsecured Data on The Network – Even In Persistent Storage – And Provides An Estimated Financial Figure For An Organizations Potential Liability In The Event Of A Data Breach.

Risk of exposure is always a possibility—until it isn't. Risk Intelligence locates sensitive and at-risk data across your managed networks and workstations, revealing how much a data breach might cost.

By deploying Risk Intelligence scans, we can identify vulnerable and/or exposed Personally Identifiable Information (PII) and Primary Account Number (PAN) in accordance with the Payment Card industry Data Security Standard (PCI DSS) and generate appropriate reports with estimate liability.

We like to run these reports on a bi-annual basis, unless needed more often.

Mobile Device Management

"Add-On" Service

Smartphones And Tablets Are Now Almost As Common In Business As Computers, Laptops And Servers. Mobile Device Management (MDM) Helps You Effectively Handle The Challenges Associated With Mobile Devices In Your Organization.

MDM allows you to easily manage and secure mobile devices. The mobile device management feature is scalable, easy to configure, and easy to manage. It makes device management more efficient and helps you to reduce risk with fast, automated setup and maintenance of mobile devices.

Today's IT service management solutions need to account for mobile devices and on-the-go employees. This means you need solid mobile device management software that lets them be more productive by using their preferred devices—while still keeping the business network safe and secure.

Security Awareness Training

FREE BASIC CYBERSECURITY AWARENESS TRAINING FOR ALL

Basic CyberSecurity Awareness Training Is Provided To Your Organization At No Additional Charge, And Is Designed To Help Educate Your Team On How They Can Safeguard Sensitive Information, And Remain Vigilant Against Cyber Threats.

Security awareness training helps organizations reduce the risks related to the human side of cyber security and can also help build a strong security-aware culture with a resilient and vigilant-minded team.

According to the 2022 Verizon Data Breach Investigation Report: 82% of all breaches involve a human element.

Well-trained users reduce these incidents, resulting in reduced costs related to lost productivity and system downtime.

Information Presented By:

Michael R. Baumann II

Director of Operations: Sales and Service

Phone Number: **254-651-1111** Email: **LearnMore@Core6Plus.com**

Areas of Expertise

- Creator of the Core 6+ & Base 4+ CyberSecurity Solutions
- Business Communication Systems Infrastructure and Design
- Customized Solutions for Businesses of All Sizes and Needs
- Very Knowledgeable In All Areas of Voice, Data, and Security
- Creative Financing Options for New Equipment and Services
- Personalized Solutions Designed With Your Future In Mind

Certifications & Authorizations

- SonicWall “SecureFirst” Partner
- Dell “Value-Added” Reseller
- Engenius “Elite Partner”
- Netgear “Powershift” Partner
- Certified On Panasonic iPro Extreme and Video Insight
- Certified On All Panasonic Unified Communications Systems

“I Am On A Personal Mission To Help As Many Small Businesses And Nonprofit Organizations Get ***REAL*** And ***TRUE*** Enterprise-Grade CyberSecurity Protection. I strongly Believe Small Businesses, ***And Especially Nonprofits,*** Have Been ***Historically Underserved And Overcharged*** When It Comes To CyberSecurity.”

- Michael R. Baumann II

TRS Technology Solutions | CORE 6+ BUSINESS NETWORK SECURITY PLUS | NSP MS NETWORK SECURITY & PERFORMANCE | BASE 4+ PRIMARY COMPUTER SECURITY PLUS | 501(c)3 TECHNOLOGY INITIATIVE

Information Presented By:

Michael R. Baumann II

Director of Operations: Sales and Service

Direct Number: **254-651-1111** Email: **LearnMore@Core6Plus.com**

Please Do Not Hesitate To Call With Any Questions…