A Systemized Approach to

Small Business Network Security

CORE 6+

BUSINESS NETWORK SECURITY PLUS

SYSTEMIZED, REAL-TIME BUSINESS CYBER-SECURITY

An Analogy That Hits *Home...*

It is our goal to make understanding your small business network as easy as possible. As such, we're using the homestead as a business network analogy. We want you to consider all of the entry points to your home as the entry points to your small business network… Think fence and gates, front door, garage, back door, and windows, etc. as possible openings - or Security Risks and/or Threat Points - to your small business network.

Understanding Layered 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 that each single defense component has a backup, just in case of a flaw or missing coverage. The individual strengths of each layer will help cover the gaps the other defensive layers may have.

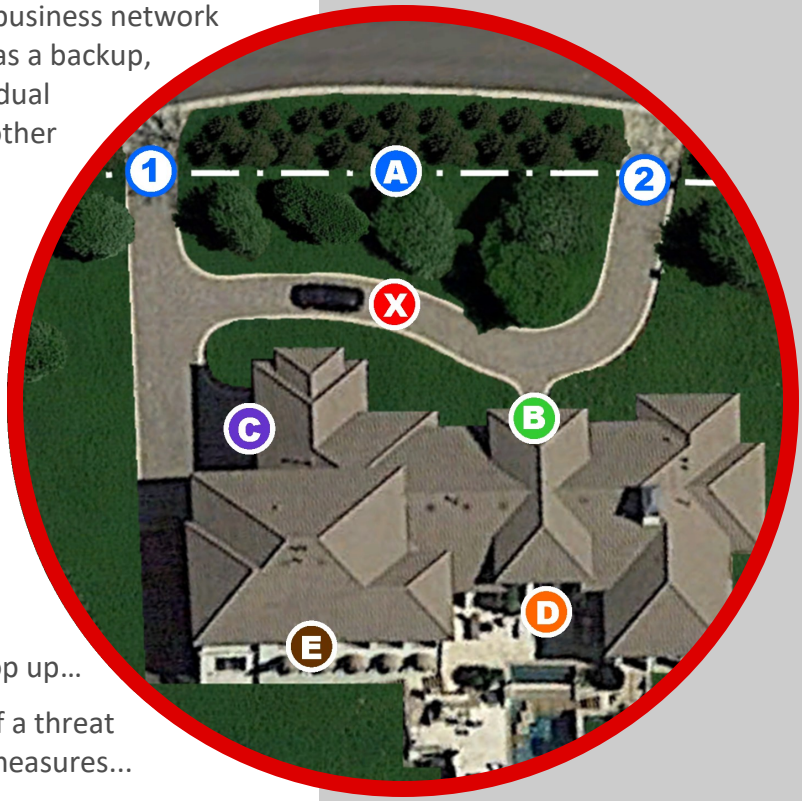
Unfortunately, there is no real way to ever achieve total security against today's Cyber-Criminals.

TRS, with security partners Presidigy, SonicWall and SolarWinds offer a layered security platform, based on the Core 6 Components that delivers the most comprehensive network security solution available, giving you the best proactive, detective and reactive security solutions available today:

Proactive: Stop threats before they start…

Detective: Catch emerging threats as they pop up…

Reactive: Recover systems and data quickly if a threat manages to circumvent the security measures...



Summary

Understanding the Core Components of Your Business Network Security...
Every small business owner, whether they believe it or not, needs to have a clear understanding of their network. Most importantly, there must be real clarity regarding the Core Components relating specifically to the Network's Security and Performance.

1 Router

Your Fence and Gates

CORE 6+
BUSINESS NETWORK SECURITY PLUS
SYSTEMIZED, REAL-TIME BUSINESS CYBER-SECURITY

The Router Protects Your Network

1 With most routers, your inbound traffic is always "screened" to determine whether they are allowed to be let in, and to some extent—depending on how sophisticated your router is—they are also "screened" to verify their level of threat or risk to your property.

Current Security Routers Check In Daily With Multiple Sources To Get The Most Current Lists Of Threats And Cyber-Criminals To Make Sure They Are All Blocked…

2 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.

TRS recommends SonicWall Routers which deliver a far superior level of protection (an Enterprise level of protection) for a Small Business price...

With SonicWall TZ-Series Routers you get:

Best In Class Threat Protection
A Much Stronger (more Secure) VPN
Deep Packet Inspection, and
Constantly Updated:

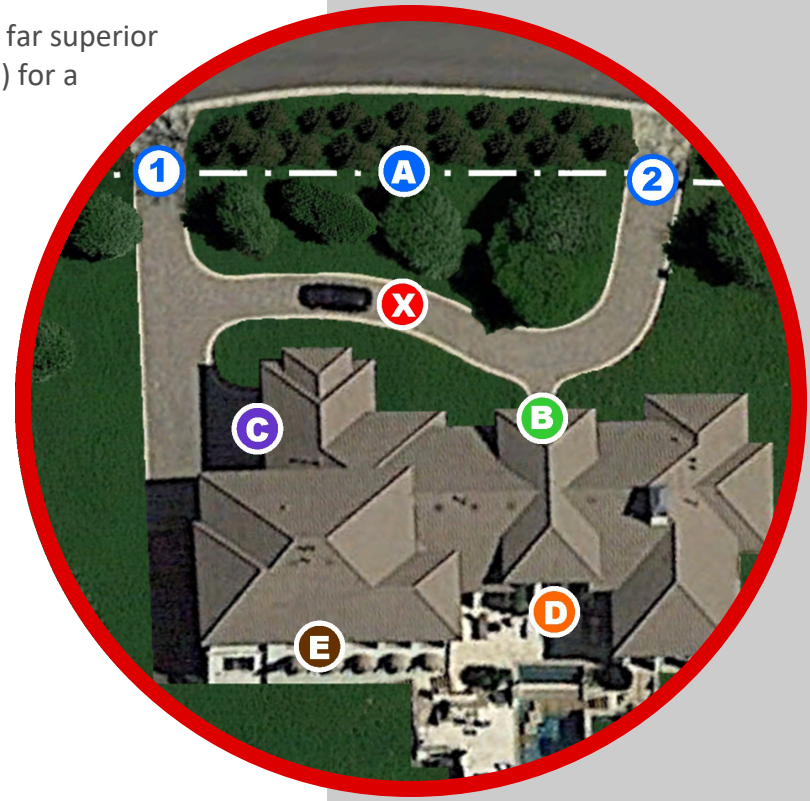
- Unified Threat Management
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Gateway Anti-Spam
- Gateway Anti-Malware
- Intrusion Prevention
- Content Filtering
- and *Enforced Client Anti-Virus*

Even includes Global Geo-Blocking

A The Analogy

Your Router is literally your property's protection from the outside world.

It is where the outside Internet is stopped, vetted, and then "let in" as per programming policies… just like a guard with an approved "guest list."



2 Anti-Virus/Malware

Your Front Door

CORE 6+
BUSINESS NETWORK SECURITY PLUS
SYSTEMIZED, REAL-TIME BUSINESS CYBER-SECURITY

Anti-Virus Is Not Enough

Anti-virus and anti-malware ("Anti-") applications are not sufficient on their own to combat the growing number of virulent cyber-attacks. Nevertheless, with Anti- vendors finding countless variations of viruses and malware every day, Anti- applications remain a core requirement in a layered security solution.

The Core 6 managed Anti– application helps to keep both known and emerging malware off workstations and servers. Our Anti- feature not only stays up to date with the latest threats using traditional signature-based protection, but also protects against new, "zero-day" viruses using sophisticated heuristic checks and behavioral scanning.

With new threats created each day, TRS can protect your businesses by using proactive methods to help ensure rock solid malware protection.

Stay Safe from Know and Emerging Malware:

- Active protection and behavioral scanning
- Extensive signature-based scanning
- Heuristic checks

Minimize Resource Drains:

- Outstanding performance
- Pinpoint accuracy
- Scheduling

Gain Complete Control:

- Default policies
- Powerful customization
- Control timing
- Easy configuration
- Proactive notifications

The Analogy

Your Incoming Email is where most outside sources enter your network. These threats are not "sneaking" around the back, they're coming straight in the "Front Door."

Depending on how adept (up-to-date) your "doormen" (Anti-Virus and Anti-Malware) are with current threats, determines the risks you endure every time you "open that door" with a new "send and receive" email request.

3 Wireless

Your Garage Door

CORE 6+

BUSINESS NETWORK SECURITY PLUS

SYSTEMIZED, REAL-TIME BUSINESS CYBER-SECURITY

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.

Not only do you risk a decrease in your Internet access speed (because of sharing Internet), but it's a huge security risk (because others may hack your computers or share viruses and malware from their computers).

The Core 6 wireless network security protects your wireless network from unauthorized and malicious access attempts.

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 - and via - the wireless network.

Typically, wireless network security is delivered through wireless devices (usually a wireless access point) that encrypts and secures all wireless communication by default and ancillary/enhanced programming.

If the wireless network security is compromised, the hacker will not able to view the content of the traffic/packet in transit.

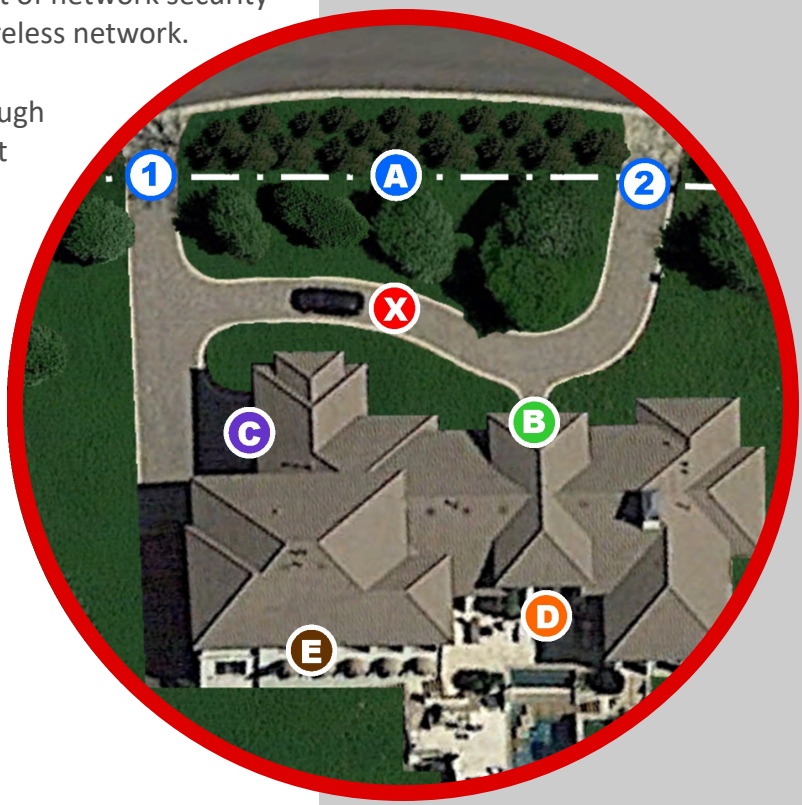
Security Measures:

- SSID Hiding
- MAC ID Filtering
- Static IP Addressing
- Restricted Access
- End-to-End Encryption
- Intrusion Detection and Prevention
- Wireless Administrator Alerting

The Analogy

This is, by far, the biggest "open door" on your entire "house..."
Digitally speaking it is often a wide-open invitation for unwelcomed guests to gain access to your network.

Sometimes, depending on how you serve your clients, it's OK to leave the big, "Outside Garage Door" open, but you must always be certain your "Inside Door" is always locked.



4 Web Protection

Your Back Door

CORE 6+

BUSINESS NETWORK SECURITY PLUS

SYSTEMIZED, REAL-TIME BUSINESS CYBER-SECURITY

Keep Your Internet Users Safe

The Core 6 web protection provides is a safeguard for all of those who surf seemingly innocent sites containing concealed malware. TRS can even use this layer to 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.

Denying access to bandwidth-hungry sites not only frees up bandwidth but also boosts the performance of your business applications and can significantly improve network resources.

Web threats have increased over the past few years. From phishing sites to drive-by downloads, the dangers have never been greater. To stay safe, you need to make sure you have advanced malware protection in place along with bandwidth monitoring, content filtering, and more.

The Core 6 web protection goes beyond enterprise antivirus software and firewall routers by letting you set your own content-filtering policies, website blacklists, time- and content-based browsing policies, and much more.

Keep Users Safe:

- Threat protection
- Bandwidth monitoring
- Access controls

Improve Workforce Productivity:

- Site blacklists
- Time-based browsing policies

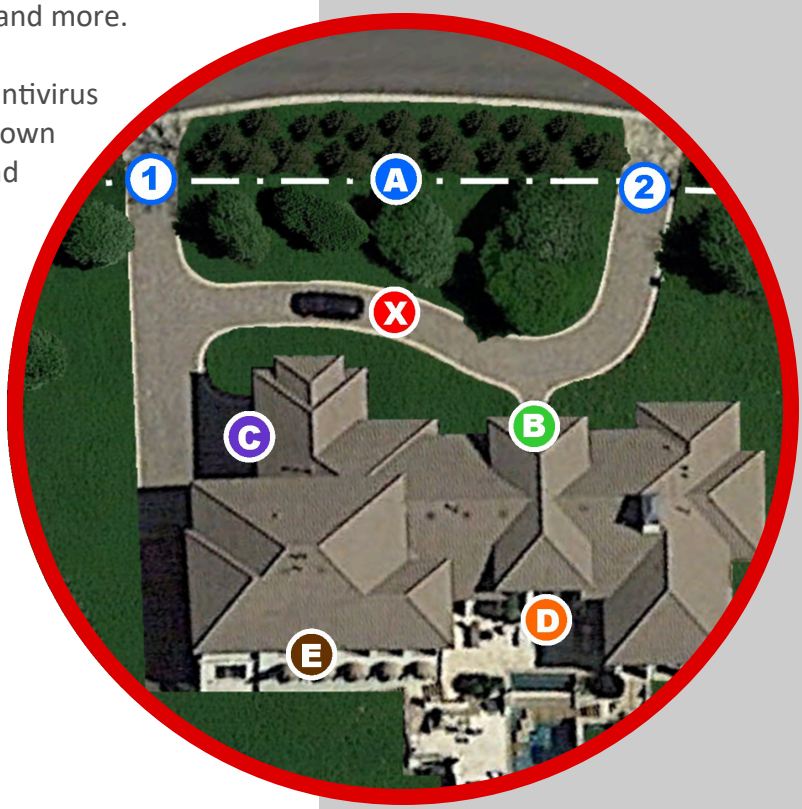
Complete Control:

- Easy administration
- Policy customization
- Individual site blocking

The Analogy

"Back Door" Web threats, like ad-ware, phishing sites and drive-by downloads have never been greater. Web Protection and Content Filtering are very different than Anti-Virus and Anti-Malware.

Digitally speaking, these threats are the Internet bad guys "sneaking" around back to find an unmonitored entrance and gain easy access to your property without you knowing.



5 Updates

Your Windows

CORE 6+

BUSINESS NETWORK SECURITY PLUS

SYSTEMIZED, REAL-TIME BUSINESS CYBER-SECURITY

Keep Everything Up-To-Date

Cyber attackers typically search for the easiest way to breach a network. Often, this involves pinpointing "soft targets," such as software that has not yet been updated to protect against known malware.

The Core 6 patch management solution handles 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, and then can install them on the appropriate machines.

Automating these tasks ensures the customer hardware and software stay up to date while eliminating the need to perform these tasks manually.

The patch management tasks we can automate include:

- Scanning computers, servers and workstations at periodic intervals to discover missing patches.
- Finding and downloading missing patches from the appropriate vendors' websites.
- Downloading only the patches required by vendors or approved by companies.
- Downloading and installing required patches on specific computers.

Complete Control:

- Convenient Approvals
- Automation
- Scheduling
- Reporting

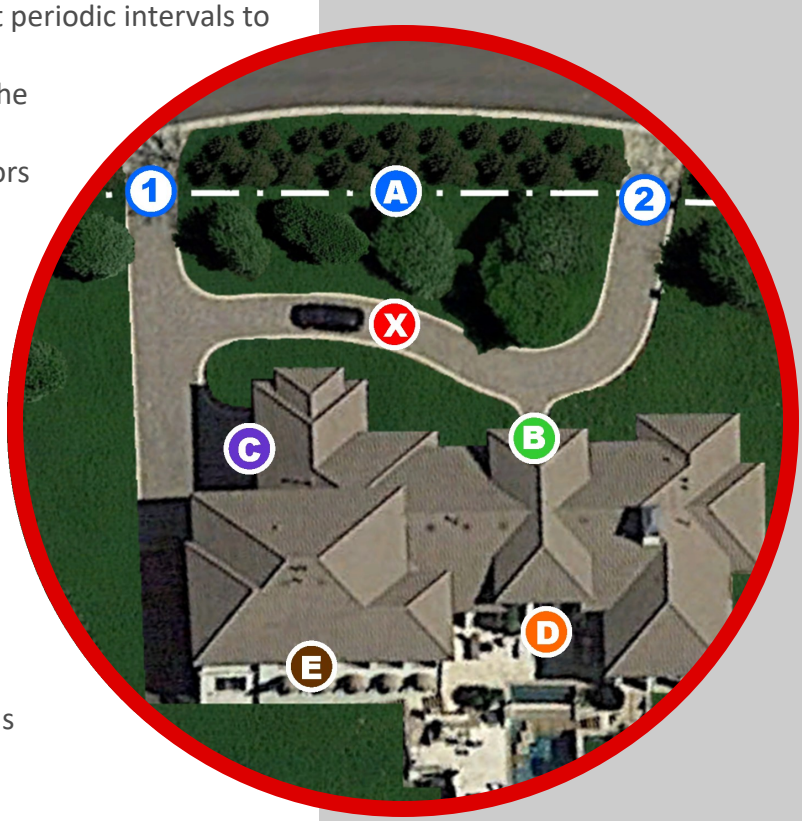
Support More Software:

- Wide software support
- Exchange and Office 365 support
- Heightened security for vulnerable programs

The Analogy

By keeping all of your "windows and doors locked" you are mitigating your most serious security risks.

Keeping your network safe requires constant vigilance. 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 get in.



6 Data Protection

Your Insurance

CORE 6+

BUSINESS NETWORK SECURITY PLUS

SYSTEMIZED, REAL-TIME BUSINESS CYBER-SECURITY

Protect Your 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.

The Core 6 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.

Local backup operations allow data to be recovered faster than remote backups from the cloud. And yet some companies that are bound by preference, policy or commitment to tight compliance standards (such as HIPAA, PCI DSS, and SOC 2) may require their data to be backed up to an offsite repository.

The backup and recovery feature also uses strong encryption both in transit and at rest, so you can breathe more easily knowing that data is kept safe.

The Core 6 backup layer gives you the best of both worlds, allowing you to back up customer data locally and remotely.

Experience the Hybrid Cloud:

- Back up a number of devices
- Best of both worlds

Back Up Fast, Recover Fast:

- Fast backup and recovery
- Bare metal recovery
- Automatic updates
- Minimum resource usage
- Bandwidth throttling
- Standby image back up

The Analogy

Data Protection Is Really Insurance!
Here's a simple truth: hardware and equipment will always fail, eventually.

Even worse, 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.