Business Network Security

Provided by TRS Technology Solutions

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

Core 6+ Security Platform Overview

includes the:

Homestead Analogy

Submitted by:
Michael R. Baumann II
michael@trsets.com
254-535-0490

TRS TECHNOLOGY SOLUTIONS
1202 Rio Boulevard, Building 6
Killeen, Texas 76543
254-526-8900

Daily Monitoring and Management

Overview

Remote Monitoring & Management
TRS streamlines network security into six core components:

- **Router**
- **Anti-Virus/Anti-Malware**
- **Wireless**
- **Web Protection**
- **Updates**
- **Data Backup**

When you have all of the components configured correctly, securely and working together, you eliminate and mitigate most of the security threats out there by today's cyber-criminals.

The problem is, everyday, the cyber-criminals do everything they can to circumvent the security parameters already in place, meaning you must remain vigilant in the protection of your business network.

With TRS's Core 6 Managed Business Network Security we make sure all of your devices and applications are monitored on a daily basis to verify their security and threat level status.

A Concentric Platform

CORE6+ Cyber-Security

Modern cyber-threats have figured out ways to circumvent conventional security tools, applications and practices. Today's businesses need comprehensive, multi-layered and reliable protection against attacks like ransomware, malware, viruses and all sorts of other advanced cyber attacks.

TRS's Multi-Layered Security offering utilizes hardware and software together with multiple integrated applications - as well as User Awareness and Training - to provide a sophisticated defense with accurate threat detection across ALL threat vectors and deployment platforms, including physical and virtual infrastructures.

TRS's **CORE6+ Managed Security** offering provides in-depth, real-time protection by utilizing sophisticated detection methods like signature, static and behavioral analysis. With daily updates (from the Global Threat Intelligence Network) **CORE6+** maintains up-to-date threat data from diverse sources around the world and even includes heuristic, comprehensive "sandboxing" to help further provide accurate detection of attacks.

The most common Internet threats are malicious attacks and hacking-bots targeted at Edge of the Network devices (like routers) looking for Remote Access; they also target Internet Users and Web Applications; and, of course, Email. Now, more than ever, these are very sophisticated attacks requiring extremely sophisticated protection.

Unfortunately the bigger network failures (in every business) are with more controllable and less sophisticated aspects that, for the most part, seemingly just go overlooked or undervalued by the business: Hardware Stability; Operating System, Application and Software Security Updates; lack of adequate, or even current Data Backup and Disaster Recovery platforms; and last but certainly not least, there's the human element (Users, Remote Users and Guests on the Network) need training.

TRS's **CORE6+** covers six core layers of protection, ***plus Real-Time Monitoring and User Training***, to prevent cyber attacks and protect business's from today's advanced threats:

- ***"Gates & Fences"*** - Managed Firewall Security Router…
- ***"The Garage Door"*** - Managed Wireless Network Security…
- ***"The Front Door"*** - Managed Anti-Virus and Anti-Malware
- ***"The Back Door"*** - Web Protection and Content Filtering
- ***"The Windows"*** - Security Updates and Patch Management
- ***"The Insurance"*** - Basic Document Backup
  (*With Additional Full Data Backup Options*)

+ ***Real-Time Monitoring and Management Of All Client Devices***

+ ***User Training To Help Minimize User-Error And Manage Risk***

CORE6+

TRS's **CORE6+** and **BASE4+** concentric approach protects your network and users by delivering multi-layered security, device diagnostics, performance management and even basic document backup applications into one seamless, proactive platform to maximize cyber protection, simplify network support and minimize overall costs.

The only difference between **CORE6+** and **BASE4+** is that **CORE6+** includes the Router and Wireless Devices.

While we're not wholly exclusive, it is the TRS preference to manage the SonicWall TZ-Series Firewall Security Routers. We believe these routers are the most cost-effective next generation firewalls (NGFW) that are ideally suited for any size organization that requires enterprise-grade network protection—and today, ***that means every business!***

Managed Firewall Security Router:

- On-box and Cloud-based Anti-Malware
- On-box and Cloud-based Anti-Spyware
- Application Intelligence and Control
- Intrusion Prevention
- URL Filtering
- Traffic Inspection (Across All Ports)
- Reassembly-free Deep Packet Inspection (RFDPI)
- Suspicious File Isolation And Examination
- Native SSL VPN Secure Mobile Access
- Multiple Zones Of Controlled Access
- Unified Threat Management Firewall
- Backed by SonicWall Global Response Intelligent Defense (GRID) Network
- ProActive Monitoring of Connectivity
- ProActive Monitoring of Functionality
- Scheduled Firmware and Maintenance Updates

Wireless Networking is more challenging than ever. It takes time, experience and truly dedicated planning to be able to engineer, deliver, implement and manage an optimal, secure, wireless network.

Managed Wireless Network Security:

- Secure, Segmented Wireless Network
- Secure, Segmented Guest Network
- Segmentation and VLANs as Required
- Configuration of Multiple SSID's
- Configuration of Hidden SSID's
- Security and Firmware Updates
- ProActive Monitoring of Connectivity
- ProActive Monitoring of Functionality
- Scheduled Reboots and Maintenance

If you haven't figured it out yet, TRS's **CORE6+** and **BASE4+** are so much more than just Anti-Virus and Anti-Malware. These tools are a comprehensive set of security and performance tools designed as a singular platform to efficiently secure, maintain and improve your network.

The following four components are known as the **BASE4+** Security Components.

Managed Anti-Virus and Anti-Malware Platform to Help Protect Email Clients and Users:

- Protect Against Known Viruses
- Catch New and Hard-to-Detect Malware Threats
- Extensive Signature-Based Scanning
- Heuristic Checks and Sandboxing
- Behavioral Scanning
- Active Protection
- Minimal Resource Requirements

Web Protection and Content Filtering to Protect Internet Usage and Web Applications:

- Keep Users Safe On The Internet
- Protects From Phishing Sites
- Protects From Drive-By-Downloads
- Content-Filtering Policies
- Website Blacklists
- Time and Content-based Browsing Policies
- Reporting

Fine-tune Patch Management to Optimize System Performance and Prevent Cyber-Attacks:

- Automation
- Customizable Policies and Scheduling
- Patch and Update Roll-Back
- Exchange and Office 365 Support
- Heightened Security for Vulnerable Programs
- Ability to Disable Device Updates
- Deep Scans

Basic Workstation Document Backup and Recovery (in Secure and Certified Data Centers):

- Unlimited Documents and File Size
- Automated Backup Twice A Day
- Detailed Reporting
- Infinitely Scalable Without Investment
- 24/7/365 Monitoring and Management
- Storage in Secure, USA Certified Data Centers
- Supported Documents = .DOC - .DOCX - .ODT - .PAGES - .PDF - .RTF - .TXT - .WPD - .WPS - .KEY - .PPS - .PPT - .PPTX - .CSV - .XLR - .XLS - .XLSX

+ ***For An Additional Fee:*** *Full System (True Delta, Encrypted) Backup and Recovery*

TRS's CORE6+ provides Real-Time Monitoring and Management of All Client Devices, including Desktops, Laptops, Servers and Mobile Devices across Operating Systems and Platforms. TRS will remotely monitor these key elements of protection to ensure your business's network remains healthy and safe:

- Alerts and Automatic Notifications for Security and Performance Status
- Performance Checks of Hardware and Software on Workstations and Servers
- Security Monitoring and Event Log Scanning
- Windows, Mac and Linux Compatibility
- Network Performance Monitoring
- Mobile Device and Virtual Machine Monitoring
- Background Maintenance and Maintenance Windows

TRS's CORE6+ User Awareness Training is designed to help network users to both "KNOW" and "DO" the *Right Thing at the Right Time* with accuracy and consistency to further help the business manage the risk associated with these Modern Cyber Attacks.

Five Key Elements To Help Protect Business Data Online:

- Strengthen Computer Defenses
- Avoid Downloading Malicious Software
- Protect Company Data and Financial Assets
- Create Strong Passwords and Keep Them Private
- Guard Data and Devices When You're on the Go

TRS's CORE6+ and BASE4+ Business Network Security Platform services both include multiple other valuable Monitoring, Management and Business Service.

Eight Included Services To Better Serve And Protect The Business:

- Remote Automated Device Monitoring
- Remote Device Management
- Remote Device Access and Control
- Asset, Software and Hardware Tracking and Reporting
- System Tray Links:
  - Support Request
  - Managed AntiVirus Status
  - Web Protection Status
  - Basic Document Backup Status
  - Basic Document Backup File Access
- Virtual CIO/CTO with Scheduled Quarterly Business Reviews
- End-User Cyber Security Awareness Training
- Daily, Weekly, Monthly and Quarterly Reporting

TRS offers additional, ancillary Security and Management services directly related to the CORE6+ and BASE4+ Platforms, including:

- Managed Mail - Spam and Virus Filtering (with Optional Archiving)
- Managed Mobile - Support and Reporting
- Managed Compliance - Vulnerability and Risk Assessments with Reporting
- Managed Full Data Backup for Workstations and Servers:
  - Off-site Storage to a Secure Data Center
  - Backup Status Reporting
  - Local Encrypted Backup

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.

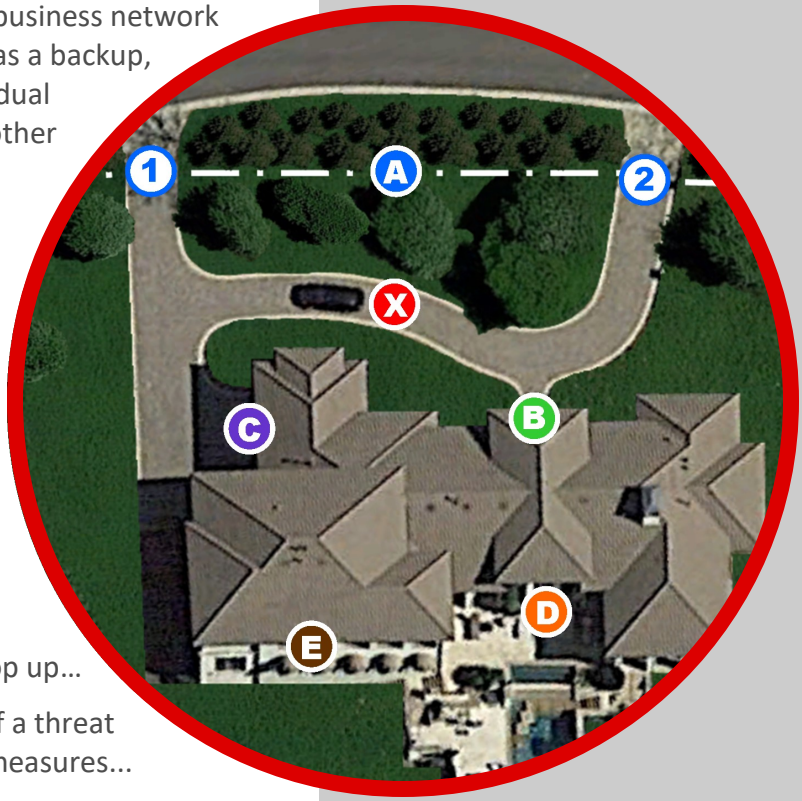
Unfortunately, there is no real way to ever achieve total security against today's Cyber-Criminals.

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:

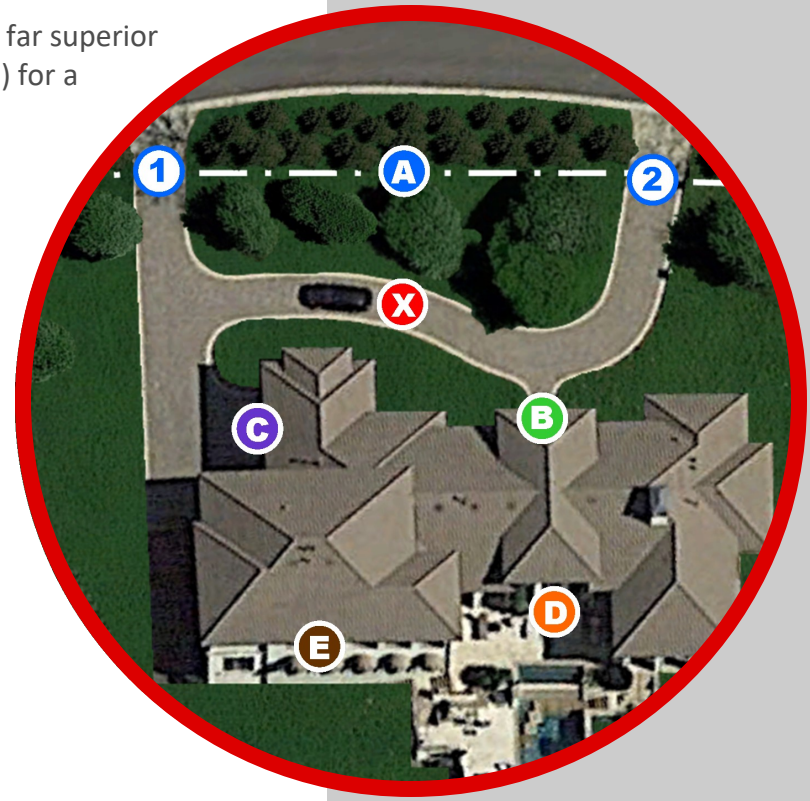
- Unified Threat Management
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Gateway Anti-Spam
- Gateway Anti-Malware
- Intrusion Prevention
- Content Filtering
- and *Enforced Client Anti-Virus*

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+** and **Base 4+** 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 Known 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

B 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.

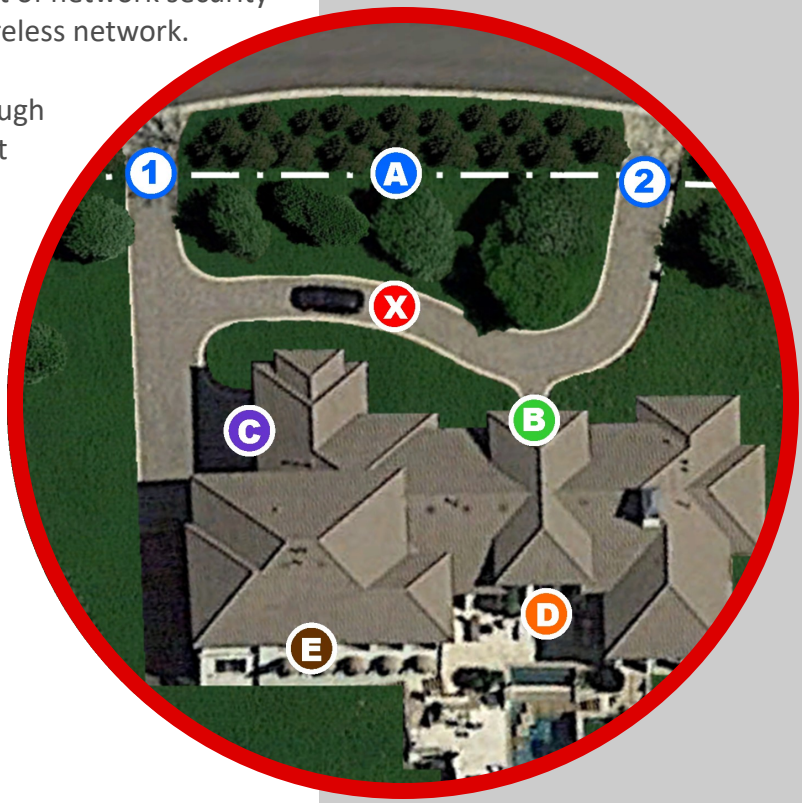
Security Measures:

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

C 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+** and **Base 4+** web protection provides 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, or gaming, or 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.

Core 6+ and **Base 4+** 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 more.

Keep Users Safe:

- Threat protection
- Bandwidth monitoring
- Access controls

Improve Workforce Productivity:

- Site blacklists
- Time-based browsing policies

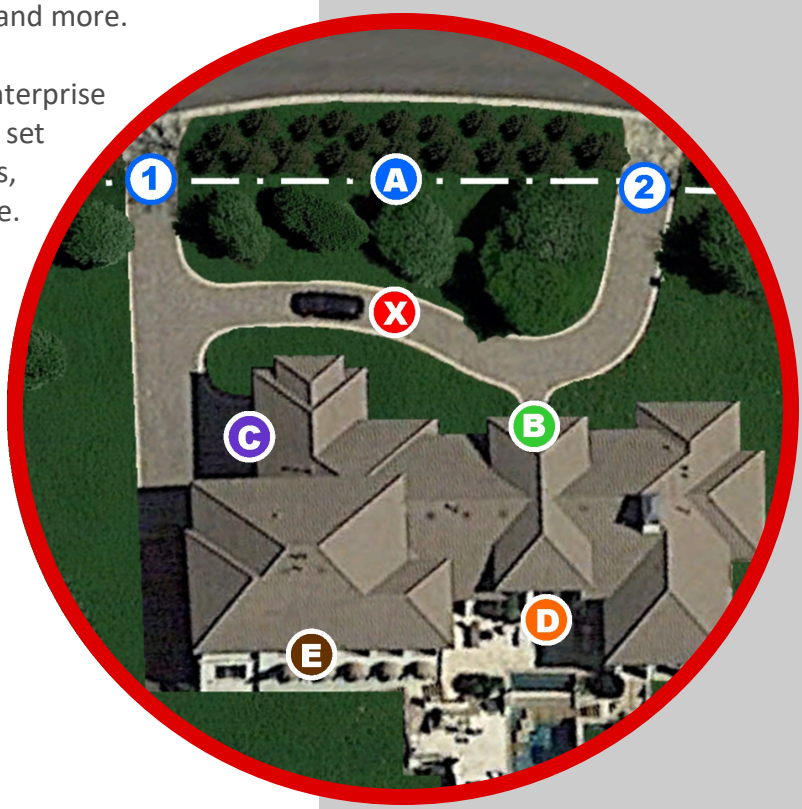
Complete Control:

- Easy administration
- Policy customization
- Individual site blocking

D 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+** and **Base 4+** 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

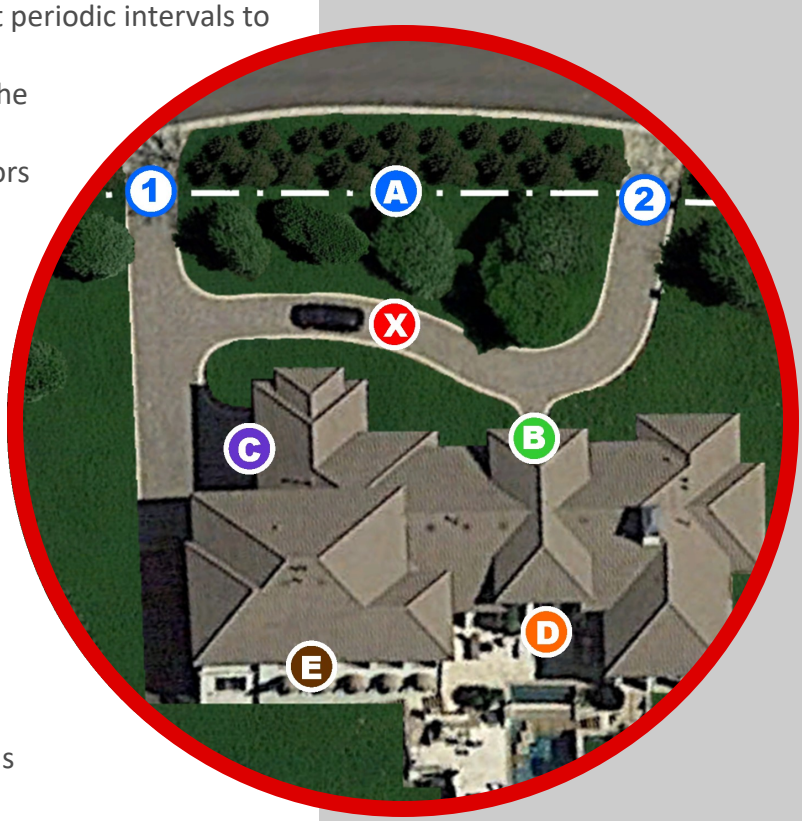
Support More Software:

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

E 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+** and **Base 4+** basic document backup and the *recommended* full data backup and disaster recovery layer provides our clients 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+** and **Base 4+** backup options give you the best of both worlds, allowing you to back up your data both locally and remotely.

Basic Document Backup:

- Automatically backs up documents
- Twice-daily, 28 days, 56 iterations
- Self-service, end-user recovery

Full Data Backup:

- Physical & Virtual Servers and Workstations
- Storage in Global, Private Cloud
- AES 256-bit encryption in transit and in rest
- Several Recovery and Restore Options

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.