



Eight Essentials of Internet Security:

and why traditional approaches fall short

Sure Signs of Outdated Internet Security

- Web filters are easily bypassed with anonymous proxies - creating liability issues
- Decreased user productivity
- Users hog bandwidth
- Critical Internet applications and resources run slowly
- Spyware infections negatively impact productivity and help desk resources
- Troubleshooting becomes difficult - causing lingering network issues
- Content controls are limited to "on" or "off" rather than controlling content by priority

Sure Sign... Cymphonix Delivers

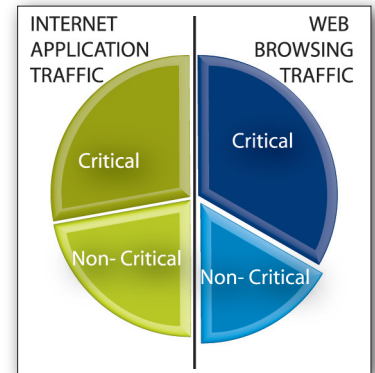
- **Visibility** - real-time, historical and automated reporting shows exactly what users are doing
- **Protection** - unparalleled anonymous proxy and filter bypass controls ensure content policies are enforced
- **Bandwidth Prioritization** - deep packet inspection and application signatures control bandwidth for websites, applications and users - allowing access to content, but ensuring critical applications and websites have the bandwidth they need
- **Security** - web-threat security features eliminate spyware from your network

The Evolution of Content Requires the Evolution of Internet Security

Internet content has evolved well beyond traditional controls. Critical applications have migrated to the web and non-browser generated web traffic like kaza@ and iTunes@ has skyrocketed.

Now, only 50% of any organization's Internet connection is used for web browsing. While some of the browsing activity is critical, like CRM tools and collaboration sites, some of it is non-critical, like social networking and porn. The other 50% is used for web-enabled applications - both critical, like VoIP or remote databases; and non-critical, like peer-to-peer, streaming media and music downloads.

Because demand for content is increasing exponentially and content access methods are multiplying, the latest Internet security solutions require eight essential features to be effective.



Evolved Internet Security: Reveals

Imagine being able to see - in real time or historically - what users are doing online, how much bandwidth they're using and how all that activity has impacted your critical applications. Combine all three, and you'll see that your top web users probably aren't your top bandwidth users. Organizations need an easy way to see how Internet resources are being used so they can more accurately troubleshoot issues and solve problems. If you could see exactly what's happening, would it affect your approach to security?

Optimizes

What if you could easily configure policy to give priority to your critical applications, websites that absolutely HAVE to be fast and users that need quick access? What if you could instantly eliminate spyware infections or concerns about users bypassing your web filter? Network Composer™ allows you to effortlessly set policy and *optimize* how your Internet connection is used - so you get the most out of what you're paying for.

Automates

Regardless of whether content is accessed via a browser or a web-enabled application, organizations need an easy way to ensure critical content has the bandwidth resources it needs. Rather than manually manipulate bandwidth levels based on estimations, now you can manage bandwidth by priority for both websites and applications - allowing access to non-critical traffic, but only when it won't impact resources for critical traffic. And, best of all, Network Composer takes care of bandwidth management and policy enforcement automatically - so you don't have to!

The Eight Essentials of Internet Security

1. Inline Deep Packet Inspection Device
2. Layer 7 Application Control
3. Dynamic Content Shaping
4. Dynamic Real-time Anonymous Proxy Detention
5. Dynamic Real-time URL Filtering
6. Full HTTPS Traffic Inspection
7. Web-based malware blocking
8. Event and User Correlation

The Eight Essentials >

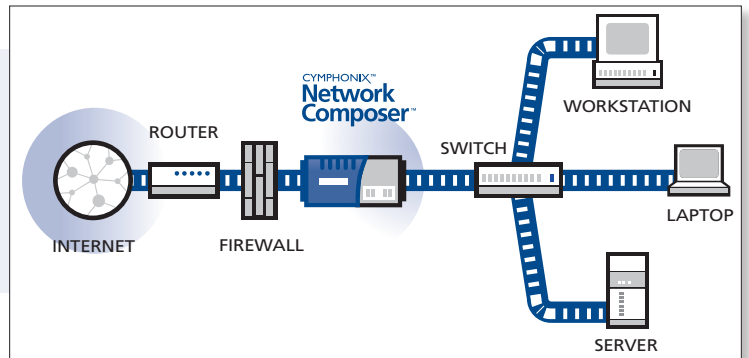


THE EIGHT ESSENTIALS

1. Inline, Deep Packet Inspection Device

Only an inline device can see and effectively manage traffic. Add deep-packet inspection, identification and prioritization and you'll be able to control traffic effectively.

Out-of-date approaches including web proxies and firewalls are easily bypassed and don't provide the web-enabled application controls organizations need.

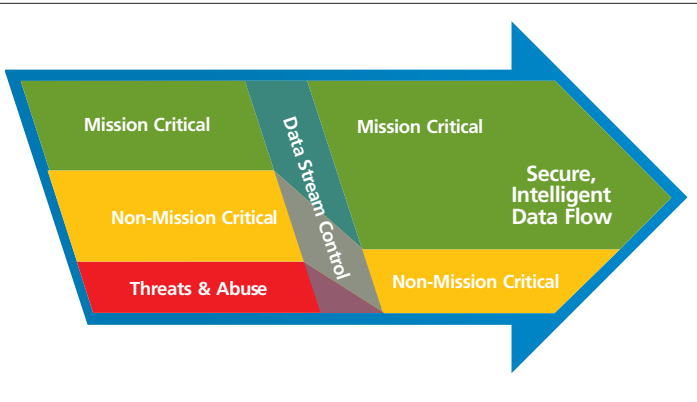


2. Layer 7 Application Control

Effective Internet security must include the ability to control web-enabled application traffic - either prioritizing it because it's critical, limiting it because it's non-critical or eliminating it because it's detrimental. Network Composer includes signatures for all major applications - providing you with the control you need.

3. Dynamic Content Shaping

Out-of-date content filters only allow websites to be turned "on" or "off". Effective Internet security allows administrators to set priorities on traffic dynamically. This way, users can access non-critical websites when bandwidth is available, but when bandwidth is needed by a more critical site or application, the non-critical traffic gets scaled back dynamically.



4. Dynamic, Real-time Anonymous Proxy Detection

Anonymous proxies allow users to easily bypass most Internet security devices. Organizations must implement a solution that dynamically detects and controls anonymous proxies in real-time.

5. Dynamic, Real-time URL Filtering

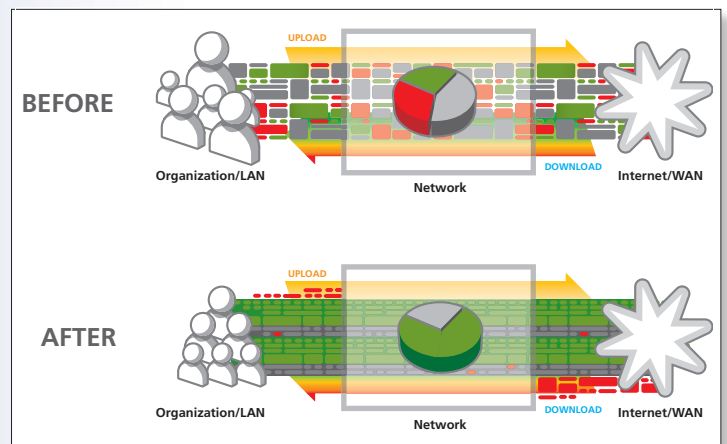
Out-of-date attempts at controlling Internet content include using just a database of URLs to categorize websites. With millions of websites being created daily, these databases become out-of-date almost immediately. Effective Internet security devices include both a database and dynamic, real-time filtering capabilities. This way websites are categorized on the fly - ensuring users are safe from inappropriate content.

6. Full HTTPS Traffic Inspection

HTTPS connections prevent filters from seeing what's contained inside of the encrypted session. Unfortunately this renders most filters completely useless. Effective Internet security decrypts and re-encrypts HTTPS sessions to ensure policy is applied to all content.

7. Web-based Malware Blocking

Effective Internet security prevents malware downloads - even if malware is served up by trusted sites or contained in HTTPS web traffic.



8. Event and User Correlation

Effective Internet security combines visibility into what users are doing online, with what applications they're using, what threats they're exposed to and how much bandwidth they're consuming. It also tells you how the actions of one user impact the Internet connection as a whole. Without this level of correlation out-of-date approaches cause administrators to misdiagnose issues.

