Trend Micro™ Titanium™ 3.0 and the Microsoft™ Windows™ Firewall

Faster, Easier, Smarter

How the Titanium 3.0 Family Boosts Protections for the Windows Firewall

A Trend Micro Whitepaper | June 2010
Table of Contents

1. EXECUTIVE SUMMARY: TREND MICRO TITANIUM™ 3.0 AND THE MICROSOFT™ WINDOWS™ FIREWALL ...... 3
2. FIREWALLS COMPARED: TREND MICRO PERSONAL FIREWALL VS. THE WINDOWS FIREWALL .................. 4
   LOCATION CHANGE DETECTION .......................................................... 6
   FIREWALL PROFILE CONCEPT ......................................................... 6
   APPLICATION FILTER ........................................................................ 7
   OUTBOUND FIREWALL RULES ............................................................ 7
   IPv6 SUPPORT ................................................................................. 8
   MY HOME NETWORK ........................................................................ 8
3. TITANIUM FIREWALL BOOSTERS AND COMPLEMENTARY PROTECTIONS ........................................... 9
   FIREWALL BOOSTERS ....................................................................... 10
   Network Virus Scan .......................................................................... 10
   Intrusion Detection System (IDS) ....................................................... 10
   COMPLEMENTARY PROTECTIONS .................................................. 10
   Internet and Email Controls .............................................................. 10
   Unauthorized Change Prevention ...................................................... 11
   Malicious Script Prevention .............................................................. 11
4. CONCLUSION: BUILDING A BETTER CONSUMER ENDPOINT SECURITY PRODUCT ............................ 12
1. Executive Summary: Trend Micro Titanium™ 3.0 and the Microsoft™ Windows™ Firewall

Consumers often complain that their endpoint security software is too intrusive, is overly complex, and eats up system resources, even as they continue to demand the best antimalware protection their money can buy. In response, Trend Micro has created Trend Micro™ Titanium™, Titanium™ Internet Security, and Titanium™ Maximum Security—a new three-sibling family of consumer endpoint security products, that’s leaner, smarter, and simpler to use than ever before. Not only is the Titanium family more user-friendly than its predecessors, it has reduced its impact on system resources, while maintaining the comprehensive security protections users require.

Trend Micro has accomplished this feat in part by removing its own firewall, deferring to the now maturing Microsoft™ Windows™ Firewall. To address what’s missing in the Windows Firewall, Titanium Internet Security and Titanium Maximum Security, the mid-range and high-end versions respectively, add “firewall boosters;” while the whole Titanium family adds other security enhancements, including Web threat protections, to strengthen the security posture of consumers’ machines.

This whitepaper outlines the rationale and benefits of this strategy; explains how it affects Windows™ XP, Windows™ Vista™, and Windows™ 7 users; and profiles the additional security enhancements Titanium provides.
2. Firewalls Compared: Trend Micro Personal Firewall vs. the Windows Firewall

In the past, when customers installed Trend Micro™ Internet Security (TIS) or Trend Micro™ Internet Security Pro (TIS-Pro)—the immediate predecessors of Titanium Internet Security and Titanium Maximum Security respectively—the Trend Micro™ Personal Firewall (TMPF) was enabled and the Windows Firewall disabled by default. While this had some advantages (all the main network security controls were under one Trend Micro roof), it also had some drawbacks, both from a technology and a user perspective:

- TMPF added to the system resource footprint, since the disabled Windows Firewall components were still present in memory, though they were turned off.
- Some pop-up messages in TMPF confused naïve users, ironically exposing them to more threats (as when they clicked “allow” to a system change when they shouldn’t have).

Such drawbacks aside, a comparison of TMPF with the Windows Firewall shows that Windows XP SP3 users in particular would appear to have diminished network protection now that TMPF is removed. Windows Vista and Windows 7 users are also affected, though to a lesser degree. What this whitepaper will show is that Titanium’s “Firewall Boosters” and complementary protections mitigate the removal of the TMPF.

Note: The table below only addresses the firewall components most relevant to our discussion. Not all features in the firewalls are listed in the table.
TREND MICRO™ TITANIUM™ 3.0 AND THE MICROSOFT™ WINDOWS™ FIREWALL

Table 1. Trend Micro Internet Security Pro 2010 | Microsoft Windows Firewalls | Titanium 3.0 Additions

<table>
<thead>
<tr>
<th>Firewall Function</th>
<th>Trend Micro Internet Security/Pro 2010</th>
<th>Windows Firewall on XP SP3</th>
<th>Windows Firewall on Vista</th>
<th>Windows Firewall on Win7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Change Detection</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Firewall Profile Concept</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Application Filter</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Inbound Firewall Rules</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Outbound Firewall Rules</td>
<td>√</td>
<td>Partial*</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>My Home Network</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Support</td>
<td>√</td>
<td>M</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Network Virus Scan</td>
<td>√</td>
<td>T1</td>
<td>T1</td>
<td>T1</td>
</tr>
<tr>
<td>Intrusion Detection System</td>
<td>√</td>
<td>T1</td>
<td>T1</td>
<td>T1</td>
</tr>
<tr>
<td>Complementary Protections</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet and Email Controls</td>
<td>√</td>
<td>T2</td>
<td>T2</td>
<td>T2</td>
</tr>
<tr>
<td>Unauthorized Change Prevention</td>
<td>√</td>
<td>T2</td>
<td>T2</td>
<td>T2</td>
</tr>
<tr>
<td>Malicious Script Prevention</td>
<td></td>
<td>T2</td>
<td>T2</td>
<td>T2</td>
</tr>
</tbody>
</table>

Key:
* Some outbound protection is provided via Trend Micro Proxy (TMProxy); See Section 3 following.
√ = Feature Available
M = Absent in Windows Firewall, but Additional Install Available from Microsoft
T1 = Absent in Windows Firewall, but Titanium 3.0 Firewall Booster Provides the Feature
T2 = Absent in Windows Firewall, but additional Titanium 3.0 Protections Complement it
Blank = Feature Absent

To address these missing elements, Titanium 3.0 supplements the Windows Firewall protections with “firewall boosters” and other network-related security enhancements, which we’ll discuss in Section 3 of this whitepaper.

For those it won’t supplement, it offers the following assessments and remedies, for Windows XP SP3 users in particular.
**Location Change Detection**

To achieve better protection when a user is on the road (roaming through different networks), TMPF in TIS/TIS-Pro implements “Location Change Detection” to correctly identify which physical network environment a user’s PC is connecting to. By doing this, TMPF can set different firewall rules for different network environments. For example, in a public Wi-Fi network environment, TMPF can disable file-sharing-related network ports to better protect the user.

Both Windows Vista and Windows 7 provide Home, Work, Public, and Domain network location settings to adjust for the type of network you’re connected to.

The Windows Firewall in Windows XP SP3 does not provide a Location Change Detection function and though it does provide some of the building blocks of location awareness (such as Network Interface Card (NIC) and IP Address detections), these cannot be leveraged in Windows XP without the rule structure to apply them to the firewall engine. That said, Windows XP laptop users can “harden” the inbound Windows Firewall rules when they’re out of the office by checking the “Don’t Allow Exceptions” function for extra security. In addition, users of any member of Titanium family obtain additional protection via the Domain Reputation Service in the Trend Micro™ Smart Protection Network™ (SPN) infrastructure, which maintains an up-to-date database of good and bad domains. Finally, Titanium Maximum Security also provides a Wi-Fi protection feature that displays a warning when connected to potentially unsafe wireless networks or hotspots.

**Summary:** Mobile users of Windows XP don’t have Location Change Detection, but a combination of native and Trend Micro technologies can address the issue.

**Remedy:** Users of laptops running Windows XP can “harden” the default inbound firewall restrictions by not allowing exceptions when travelling and using Wi-Fi connections. Moreover, Trend Micro’s Domain Reputation Service in the Smart Protection Network (SPN) adds an additional layer of protection by checking good and bad domains, blocking the bad ones. Finally, Titanium Maximum Security users also get an extra layer of Wi-Fi protection: the user is warned when they try to connect to unsafe wireless networks or hotspots.

**Firewall Profile Concept**

As described above, TMPF provides the capability to detect a location change. TMPF then implements the “Firewall Profile” concept in TIS/TIS-Pro by associating one set of firewall rules (the so-called “firewall profile”) with network location, to achieve automated location-aware firewall protection. So a firewall profile (like “Direct Internet Connection”, “Home network”, “Office network”, etc) represents a group of “firewall rules” that a user might set, which would then automatically come into play when a new location is detected.

TMPF also combines the “Firewall Profile Concept” with that of “Security Level” (maximum, medium, low, and minimum) to greatly simplify the configuration effort when a user adjusts the firewall strength. For example, the user will likely set the security level to “maximum” on a “Direct Internet Connection” firewall profile.

The Windows Firewall in Windows XP does not support this feature through its UI, though it does in Windows Vista and Windows 7. For instance, selecting “Windows Firewall with Advanced Security” in Windows Vista or Windows 7 Administrative Tools brings up a window to add and manage Advanced Firewall Settings such as inbound/outbound rules or connection security rules, then applies them to Domain, Private, or Public profiles.

**Summary:** Mobile users of Windows XP don’t have a Firewall Profile Concept, but a combination of native and Trend Micro technologies can address the issue.
Remedy: The situation is almost identical with the one above. Users of laptops running Windows XP can “harden” the default inbound firewall restrictions by not allowing exceptions when travelling and using Wi-Fi connections. Moreover, Trend Micro’s Domain Reputation Service in the Smart Protection Network (SPN) adds an additional layer of protection by checking good and bad domains, blocking the bad ones. Finally, Titanium Maximum Security users also get an extra layer of Wi-Fi protection: the user is warned when they try to connect to unsafe wireless networks or hotspots.

Application Filter
Generally speaking there are two types of firewall rules provided by modern stateful firewalls (including the TMPF, Windows XP SP2, Windows Vista, and Windows 7 firewalls):


2) Program control firewall rules (or the so-called TMPF Application Filter).

For not so tech-savvy users, the TMPF “program control” firewall rules are easier to understand and set. The TMPF Application Filter will also trigger system tray pop-ups to notify the user there is an application program trying to connect (for outbound packets) or bind (for inbound packets) to the network protocol stack (TCP/IP). Unfortunately, this feature is no longer considered effective because it relies on the user’s decision to allow/block the application program. And most of the time the user will just allow the connection. Secondly, the TMPF outbound application filter is no longer considered effective because the majority of malwares today actually use Windows components as a proxy to redirect their outbound traffic. The most famous targets today are Internet Explorer® and svchost.exe; Internet Explorer alone takes 42% of the outbound traffic, according to internal Trend Micro reports. Hence, the decision to default to the Application Filter function in Windows Firewall, particularly for Windows Vista and Windows 7, even though Windows XP only provides inbound application filtering for applications like FTP, Internet Mail, Web, and Telnet Servers.

The key way Titanium Internet Security / Titanium Maximum Security addresses this problem is through its Unauthorized Change Prevention module, which protects the computer from suspicious changes to the system. It does this by monitoring the behavior of executables via black and white application lists, as well as the program’s digital certificate, thus blocking the bad behaviors. Users are protected from outbound bad behavior, such as unauthorized “phoning home,” by proactively preventing such infections in the first place.

Summary: The Windows Firewall in Windows XP only provides inbound application protection, while the Windows Firewall in Windows Vista and Windows 7 provides it in both directions. Titanium addresses Windows XP’s shortcomings by monitoring applications.

Remedy: Titanium’s Unauthorized Change Protection module protects end-user computers from suspicious changes on the host system, protecting users on the Application layer via a Black/White application lists and digital certificates, among other functions. See the second section below for more details.

Outbound Firewall Rules
The protection of a stateful firewall is achieved by applying firewall rules to a firewall engine. (Firewall rules are applied by the active network profile). Firewall rules can be categorized by “connection” or direction—such as inbound rules (incoming to the PC) or outbound rules (outgoing from the PC). Note that the Windows Firewall in Windows XP provides inbound rules, but not outbound ones; while Windows Vista and Windows 7 provide both. That said, even though Windows Vista and Windows 7 have outbound firewall engines, their
default outbound firewall rule is “Allow ALL except rule matched.” Moreover, there are no default “Block” outbound firewall rules in Windows Vista and Windows 7, though the user can add rules to change that.

Why should you enable a firewall’s Outbound protection? The answer is fairly simple: to prevent malwares and viruses from sending confidential information back to their botnet servers. When backdoor worms attack your computer, they steal the information and then connect to an external hacker’s server to send the data. Enabling Firewall Outbound Connection will prevent any outbound connection except for the applications you define, thus keeping your system more secure.

Since the Windows Firewall in Windows XP does not provide outbound rules, removing the TMPF can expose users to “phone home” malware behavior. However, this presumes that the malware has been able to bypass the inbound firewall rules in the first place. The way it might do this on a consumer’s endpoint machine would be through a Web, Email, or File exposure vector. Fortunately, Titanium provides such protections with its Web Threat Protections (WTP)—Web, Email, and File Reputation Services. These are supplemented in Titanium Internet Security and Titanium Maximum Security with its Unauthorized Change Protection module (see section below).

Note too that Trend Micro Proxy (see section 3 following) can block some but not all outbound requests. It can block HTTP/S on any port, but the current implementation just uses the standard HTTP/S ports such as 80, 8080, 8081, 443, etc.

Note: Some command-and-control malwares use the Internet Relay Chat as the protocol to communicate to their server. In this case, the malware’s “phone home” will not be blocked by Trend’s Web Threat Protection (WTP). However, if the command-and-control malware uses the HTTP protocol and the domain/URL is in our WRS database, the “phone home” will be blocked.

Summary: Although Windows Firewall in Windows XP does not have outbound rules, which could allow a malware to “phone home” if it got installed, Windows XP users can obtain the protection accorded Windows Vista and Windows 7 users by means of Titanium’s WTP and behavior monitoring modules.

Remedy: Titanium’s Web Threat Protection function, which includes Web, Email, File, and Domain Reputation Services; and its Unauthorized Change Prevention module in the mid-range and high-end Titanium products, can together proactively prevent this kind of malware infection from ever occurring. Malwares never get a chance to install and phone home.

IPv6 Support
TMPF and the Windows Vista and Windows 7 Firewalls support IPv6 by default. While the default Windows XP firewall does not support IPv6 by default, a separate downloadable firewall package from Microsoft supplements Windows XP to support IPv6.

Summary: Windows Firewall in Windows XP does not support IPv6 by default.
Remedy: Download and install the IPv6 package from Microsoft.

My Home Network
My Home Network in TMPF provides users with a Home Network Map of all computers on the local network (Network Discovery), which they can use to block wireless network users from accessing any computer on the network (Wi-Fi Protection), or to manage and update compatible security software (TIS/TIS-Pro) for those
computers (basic Remote Administration). My Home Network is implemented by sending Address Resolution Protocol (ARP) broadcast packets to the local LAN to identify all neighboring network devices (including other PCs). While this feature is nice to have, in practice, consumer users rarely use it.

Windows XP does not have a similar feature for its Windows Firewall, but Windows Vista and Windows 7 provide the basic layer (only the first of the above three functions) for insight into what’s active on your network. This is implemented as a Network Discovery setting that affects whether your computer can see or find other computers and devices on the network and vice versa. Network Discovery can be On or Off, or users can define a Custom mixed state in which some services are enabled and some aren’t. As long as the Windows Firewall exception for network discovery is enabled and other firewalls are not interfering with it, the network discovery state is active and shown as Custom.

Summary: This is a “nice to have” feature; Windows XP users do not have a similar function, but the feature is not used much by the average consumer.

Remedy: Windows Vista and Windows 7 can use Network Discovery for basic insight into devices and computers on the home network.

3. Titanium Firewall Boosters and Complementary Protections

As Table 2 reminds us, Trend Micro proposes to supplement the Windows Firewall in two main areas, using firewall boosters (T1) and complementary protections (T2), which together provide an up-to-date response to the removal of TMPF. Most of these functions were originally included in TIS/TIS-Pro, though Titanium 3.0 adds a new “browser guard” feature that prevents Microsoft Internet Explorer from running malicious scripts on infected websites.

Table 2. Titanium Firewall Boosters and Complementary Protections

<table>
<thead>
<tr>
<th></th>
<th>Trend Micro Internet Security Pro 2010</th>
<th>Windows Firewall on Windows XP SP3</th>
<th>Windows Firewall on Vista</th>
<th>Windows Firewall on Windows 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Virus Scan</td>
<td>√</td>
<td>T1</td>
<td>T1</td>
<td>T1</td>
</tr>
<tr>
<td>Intrusion Detection System</td>
<td>√</td>
<td>T1</td>
<td>T1</td>
<td>T1</td>
</tr>
</tbody>
</table>

**Complementary Protections**

| Internet and Email Controls | T2 | T2 | T2 |
| Unauthorized Change Prevention | T2 | T2 | T2 |
| Malicious Script Prevention | T2 | T2 | T2 |

Key: √ = Feature Available

T1 = Absent in Windows Firewall, but Titanium 3.0 Firewall Booster Provides the Feature
T2 = Absent in Windows Firewall, but additional Titanium 3.0 Protections Complement it
Blank = Feature Absent
Firewall Boosters

Network Virus Scan
The Network Virus Scan (NVS), the first Windows Firewall Booster, allows Titanium to check payloads in TCP, UDP, ICMP, and ICMPv6 packets against rules in a pattern, then to drop or accept packets based on the results. NVS can do both inbound and outbound network packet scans using rules (though the majority of rules are for inbound scanning). These rules are subject modification by Trend Micro’s anti-malware team.

For example, because the Conficker/Downad worm uses an exploit to a particular vulnerability to spread, users can create a NVS rule based on distinct exploit-related characteristics in the payloads of Conficker/Downad packets. NVS is then able to drop Conficker/Downad packets and possibly other malicious packets that contain the same exploit.

In general, malware detected using NVS are considered "network viruses" because of their ability to directly spread from one computer to another without user intervention. Network viruses typically achieve this by sending specially-crafted code that exploits system vulnerabilities to target computers. NVS can detect not only the payload of the network viruses, but also the underlying network packet level vulnerabilities used by these viruses, therefore stopping all variants of viruses exploiting the same vulnerability.

The pattern used by Network Virus Scanning is updated regularly by TrendLabs™ whenever a major network level vulnerability is found. The pattern updated automatically to endpoint. Description of the pattern file is at: http://www.trendmicro.com/ftp/products/nvwpattern/nvp-new.txt.

Intrusion Detection System (IDS)
The Intrusion Detection System (IDS) provided by TMPF will be included in Titanium 3.0 and provides strong detection capability* for a variety of network intrusions, including such things as the “Ping of Death,” “Trace Route,” and “SYN Flood”—typical indicators that an intrusion may be taking place. While most of these attack techniques have been around for quite some time and are not the latest-and-greatest in a hacker’s arsenal, Trend Micro still considers them dangerous enough to continue to provide them as a Windows Firewall Booster. (Note though, that home routers/Wi-Fi access points often provide similar features by default.)

*Note: A January 2009 report from West Coast Labs entitled Trend Micro Worry-Free Business Security [WFBS] Comparative Testing Report, which gave the results of comparative lab tests of Trend Micro™ Worry-Free™ Business Security 5.0 and three competitors, included important details about the IDS function in Worry-Free Business Security’s firewall—the same Trend Micro IDS component used in Titanium. When compared with the IDS function in the competitors’ products, Trend Micro’s WFBS 5.0 IDS detected and logged some 30,000 intrusion attempts, while Symantec’s Endpoint Protection 11.0 logged only one, and McAfee’s Total Protection Advanced 4.5 and Microsoft’s Live OneCare for Servers (Beta) logged none.

Complementary Protections
Titanium 3.0 also bolsters the network-layer security posture of the consumer’s computer by complementing the Windows Firewall protections at the application layer.

Internet and Email Controls
Trend Micro’s cloud/client-based Internet (aka Web Threat Protection) and Email Controls are important parts of the Smart Protection Network (SPN) and are comprised in part by Web, Email, File, and Domain Reputation Services (the newest addition to the SPN, which blocks the DNS query when the domain name is suspicious).
These gather the respective reputations of websites, IP Addresses, files and applications, as well as domains, to protect users from exposure to the malware in bad URLs, emails and instant messages, and files and domains. These cloud/client-based services are correlated with each other and include intelligent feedback loops, to provide state-of-the-art, real-time protections for the global community of Trend Micro customers, including users of endpoint protection solutions such as Titanium.

According to TrendLabs threat statistics data, the majority of threats come from the Internet via malware posted on malicious, hacked websites. Titanium blocks malicious web sites automatically when the user browses the internet, but also comes into play when malicious URLs are placed in phishing emails or instant messages. If a user clicks the link in the email, they’re automatically blocked. In short, Titanium anti-malware strategy focuses on prevention, blocking malware from getting to your computer in the first place.

In addition, as part of its Internet Controls, Titanium provides Wi-Fi protection, which displays a warning when connected to potentially unsafe wireless networks or hotspots.

Finally, Titanium includes a process brought over from TIS/TIS-Pro called Trend Micro Proxy (TmProxy), an ISO OSI (Open System Interconnection) Layer 7 (Application Layer) traffic scanning process that runs on the user’s local machine, scanning for malware like spam, viruses, private data, bad URLs, as well as changes to the Hosts file, etc. TmProxy receives network traffic redirected by a subcomponent, then parses the network protocol and scans the content inside. The whole process works like a local network proxy on the user’s machine—which is why the component is called TmProxy. Currently, the network protocol parsers supported by TmProxy include HTTP/S, SMTP, POP3, and popular IM programs. Additionally, Trend Micro Proxy can block some but not all outbound requests. It can block HTTP/S on any port, but the current implementation just uses the standard HTTP/S ports such as 80, 8080, 8081, 443, etc.

Unauthorized Change Prevention

Titanium 3.0 employs a behavior monitoring module that provides increased security for host computers via host intrusion prevention (HIPS) techniques. These watch running processes on the system for unauthorized and potentially malicious system changes, then block them according to rules.

The assumption here is that a new malware variant has already somehow bypassed WTP as well as the firewall—perhaps because it resides on a portable drive and is executing via autorun—and is now attempting to install on the system. If it tries to execute and make system changes, such as a malware injecting code in Internet Explorer to connect out (without triggering a firewall warning), it’s blocked.

The newest feature of the module includes behavioral feedback and containment with a significant level of detection with lower false positives and can block both individual and multiple malware activities. For this reason, it can proactively stop malware in its tracks before the infection happens, though even a partially or fully infected system can also benefit from the module.

Malicious Script Prevention

The new Malicious Script Prevention (MSP) feature in Titanium 3.0 provides a “browser guard” for Internet Explorer that helps detect malicious scripts that infect Web pages on websites and adds the bad link to our URL reputation database in the Smart Protection Network. This includes scripts that are packed or obfuscated. Scripts are unpacked and analyzed to determine what they look like, if they’re malicious, where they come from, what they do (their behavior), and they are then controlled or cleaned.
MSP uses heuristic analysis to detect generic shell codes and exploits without requiring signature updates. It can proactively detect/block exploits such as the 0day MS10-002 exploit. (See http://us.trendmicro.com/us/trendwatch/current-threat-activity/zero-day-attacks). MSP currently supports IE JavaScript in obfuscated format, which means that MSP is able to intercept and scan obfuscated JavaScript content before the script executes. If shell code is found in the script, MSP can stop the script from executing and display a warning message. MSP sends detected URLs to the SPN backend, enhancing the overall Web Threat Protection (WTP) blocking rate for all Trend Micro products, including Titanium.

4. Conclusion: Building a Better Consumer Endpoint Security Product

As the threat landscape has changed—with threats now coming primarily from the Web—consumers need endpoint security products that more adequately address the latest threat vectors. At the same time, they’re tired of bloated endpoint security software that needlessly consumes computer resources. Trend Micro Titanium has addressed both concerns by providing state-of-the-art Web threat protections, while lightening the load on the endpoint by removing its personal firewall in favor of the firewall already present in the Windows operating systems. And where concerns might be raised over any missing network security features, Titanium steps up to the plate and compensates for the handicaps.

As this whitepaper has shown, the missing features in Windows XP SP3 in particular can be largely addressed by taking some precautions using the Windows Firewall settings themselves and by utilizing the Firewall Boosters and Complementary Protections in Trend Micro Titanium 3.0, which apply to all current Windows versions. The Network Virus Scan and Intrusion Detection System boosters still provide the core network-layer protections for Windows users, blocking most intrusion attempts; while the Trend Micro Internet and Email Protection, Unauthorized Change Prevention, and Malicious Script Prevention modules take up the slack, providing state-of-the-art complementary protections on the Web or right on the host computer itself. Windows XP’s missing outbound filtering, for example, is taken care of by the multiple protective layers in Titanium—by the cloud/client Web and File reputation services, or by the behavior monitoring module residing locally on the computer.

In short, building a better consumer endpoint security product has meant trimming the fat from the software, while at the same time enhancing it for the modern threat landscape. The Trend Micro Titanium family does just that—and is faster, simpler, and smarter because of it.

June 2010