Management buy-in from day one.

and convincing arguments though. Let them work for you for a change, and make sure that you get Senior

required, whitelisting can take some time to deploy. And sometimes whitelisting runs into resistance from

large-scale deployment has the potential to become political. Ultimately, there must be policy and

auditors, which makes compliance with industry regulations much easier.

FPT or P2P) that are security risks. Additionally, whitelisting can help you show stringent controls to

software developers giving you as an administrator the option to auto-approve these updates via the

The intelligence in the Cloud service automatically approves /files updated by Microsoft and other large

Update Management

Architecture Management

CPU, very little disk space utilization and miniscule network overhead.

the cloud when encountered for the first time. This type of traffic is hardly measurable. In short: super low

database on your workstation or server is empty when installed.

check a process against a list of checksums. This means you can run whitelisting on all systems without any

No Performance Penalty

communications mechanism to keep your local lists up-to-date, is the only way to keep whitelisting simple

Keeping cloud-based lists of known-good with all their related meta-data, combined with an efficient

whitepaper: Whitelisting Without The Complexity

endpoint TCO actually goes down, you have (a lot) more control, and the end-user productivity goes up.

itself. With that deployed, your security will improve significantly, support tickets decrease, your total

desktop.

AV on the desktop level. You can decide if that needs to be on-demand or on-access AV scanning at the

AV scanning of web-traffic in your firewall, combined with AV scanning on your Email gateway/server and

whitelisting is a great asset to any IT administrator who just wants the phone to stop ringing for a change.

since traditional security defenses are becoming less effective by the year. A smart deployment of

work" is something that needs to be prevented from happening. The benefits of whitelisting are enormous,
potential end-user resistance up front is an important tactic to make the roll-out a success. You need

approach. Whitelisting allows IT to get control back and rule with an iron fist in a velvet glove. Handling

with PCs under their own control. In the current security environment this is no longer a responsible

As we stated above, security needs to be turned on its head and a shift from blacklisting to whitelisting

Steps For Success

for granular customizations, and is the future of IT's first-line malware defense. Customization for your own

whitelist that's crucial to an end-user. It really takes less than a minute. Having a fast process prevents

start off with. Have some end-users do their normal job on these test machines to see if there is any

Causing end-user productivity issues is the last thing IT wants. Run the whitelisting app in a test-bed to

Sometimes it is needed to have a few baseline images, each for a different department or business unit.

organizations create a single master PC that has all the apps installed that could run in the organization.

whitelist. Run this for a few weeks, review and make changes before rolling out deny-mode. Some

'dknown-good' to run. It's a simple, powerful idea that stops malware dead in its tracks. It allows you to run

doubled from 17 Million to 40 Million. During that same period, the amount of 'known-bad' malware has
The Endpoint Security Advantages of Whitelisting: A Whitepaper for System Administrators

In the 10-year time frame from 2002 to 2012, the volume of ‘known-good’ executable code has roughly doubled from 17 Million to 40 Million. During that same period, the amount of ‘known-bad’ malware has skyrocketed 40 times from 2 million to over 80 million. In 2002, keeping out the bad guys with antivirus was a correct and rational decision. Now, in 2012 that is no longer the case. The more rational decision is to continue using traditional (blacklist) antivirus but combined with gray- and whitelisting and only allow ‘known-good’ to run. It’s a simple, powerful idea that stops malware dead in its tracks. It allows you to run your network with an iron fist in a velvet glove.

Essentially, it’s time to put your endpoint security on its head. This whitepaper tells you why.
**Introduction**

Malware has skyrocketed in volume in the last decade, and at the same time has ‘gone pro’. Malware has become highly sophisticated; the Zeus trojan is a good example. Traditional antivirus has trouble keeping up, as cybercrime generates 100,000 new malware executables per day. Antivirus companies have struggled trying to improve their product and added lots of new features, without being able to change their blacklisting model to what by now really is required: whitelisting. The result is antivirus bloatware, with a significant performance impact on workstations, and ineffective protection against malware.

C-level executives frown as they see the yearly Total Cost of Ownership per workstation rising, while at the same time security effectiveness going down. IT is being asked to do more with less budget and a lower headcount. It’s time to put endpoint security on its head. We are not advocating throwing your existing antivirus out the window. Antivirus has its place, and should be kept, but it only provides half the functionality it needs to. Whitelisting, also sometimes known as Application Control, can stop malware dead in its tracks and actively lowers the cost of maintaining systems across your network.

The smart approach is to add whitelisting as an additional layer to your defense-in-depth strategy. Next, use intelligent graylisting to decide about the code that falls in between the white- and black lists. The most successful strategy for the next decade is a combination of white-, gray- and blacklists which requires an absolute minimum of admin time. This combination will dramatically reduce malware infection rates and improve network security without end-user productivity problems.

**Block Zero-Day Attacks**

Small, but very high risks are zero-day exploits. No known security tool except whitelisting has a guaranteed defense against zero-day attacks. Being able to block any unknown process to run protects your network against all malware, zero-day and targeted attacks.

**Whitelisting Complexities**

There are several drawbacks to first-generation whitelisting however, from a system administrator perspective. Let’s have a look at these:

- Updates, how are they managed?
- How about users with lots of apps?
- How much additional IT workload to manage the lists, and add apps?
- How fast can IT respond regarding an end-user approval request?
- Is whitelisting agile enough for our environment?

First-generation whitelist solutions have been forced to deal with this complexity by adding a substantial management layer, causing additional IT workload. A new approach was needed to make whitelisting a workable solution for IT at all sites, not just the Fortune 500. That solution was not available at the time first-gen solutions were designed. A next-generation, cloud-based whitelisting solution was needed and that architecture does solve the whitelisting complexity.

**Cloud-based Lists**

There is twice as much malware as there is known-good, and that ratio is getting worse by the day. Tracking every Trojan, virus and worm has become literally impossible. The problem is that when antivirus vendors can’t keep up, malware makes its way through, infecting workstations and opening up your network to the bad guys.
Keeping cloud-based lists of known-good with all their related meta-data, combined with an efficient communications mechanism to keep your local lists up-to-date, is the only way to keep whitelisting simple to manage. It needs to be a ‘set-it-and-forget-it’ solution that noticeably cuts IT workload, and shows a dramatic decrease in malware infections.

**No Performance Penalty**
Antivirus software has lots of moving parts to keep all kinds of malware out, and can cause considerable overhead on systems, especially when scans are performed. However, the CPU cycles needed to decide if a process is Good/Bad is less than 5% of what an antivirus application takes, as whitelisting only needs to check a process against a list of checksums. This means you can run whitelisting on all systems without any performance degradation, and add it to any system that has AV running without penalty. The local database on your workstation or server is empty when installed.

The cloud-based lists are as close as possible a real-time picture of all valid processes, as well as the processes that are defined as part of the Gray and Black lists. Your local database (on your local server and local workstations will be build up gradually as the whitelisting software is being used, and contains little more than the hash-values, so there is hardly any local disk space used. New processes are being checked in the cloud when encountered for the first time. This type of traffic is hardly measurable. In short: super low CPU, very little disk space utilization and miniscule network overhead.

**Architecture Management**
There are three components. The master list with all its metadata lives in the cloud. A local server contains a subset of that master list, related to all the files within your organization. Each workstation contains a small subset of the list on the server. Workstations only communicate to your local the server, they do not directly talk to the cloud. Your admin console lives on your local server, and talks to the cloud.

**Update Management**
The intelligence in the Cloud service automatically approves files updated by Microsoft and other large software developers giving you as an administrator the option to auto-approve these updates via the management console.

Whitelisting is also a great way to stop applications that other methods like tightened security permissions or ‘least-user privileges’ are unable to block. The best example is the Chrome browser which can be installed by any nonprivileged end-user without admin rights or permissions.

**Whitelisting Helps With Compliance**
You can keep an eagle eye on costly software licenses and prevent users from running programs (such as FPT or P2P) that are security risks. Additionally, whitelisting can help you show stringent controls to auditors, which makes compliance with industry regulations much easier.

But, let’s be real. Whitelisting is not just a bed of roses. It can have its own challenges. If not done right, a large-scale deployment has the potential to become political. Ultimately, there must be policy and agreement on an approved list of applications. Combine that with a process to add new apps when required, whitelisting can take some time to deploy. And sometimes whitelisting runs into resistance from end-users that feel they should be able to run anything they want. Compliance and security are very strong and convincing arguments though. Let them work for you for a change, and make sure that you get Senior Management buy-in from day one.
Running in Audit Mode

Whitelisting programs are able to run in audit-mode so you can create baseline lists to start with. You can set up a (virtual) machine with a standard image; then run the audit process, and the program builds the whitelist. Run this for a few weeks, review and make changes before rolling out deny-mode. Some organizations create a single master PC that has all the apps installed that could run in the organization. Sometimes it is needed to have a few baseline images, each for a different department or business unit. You can do that using virtual machines.

Causing end-user productivity issues is the last thing IT wants. Run the whitelisting app in a test-bed to start off with. Have some end-users do their normal job on these test machines to see if there is any adverse impact. Only when that’s successful, deploy in audit mode and see what is going on in your production environment. Servers usually are much more stable and have less variables compared to end-user workstations, so they are a lot simpler to set up and manage. Have a backup plan in place, and plan a rollback (with written procedures) just in case. That can save your bacon in a worst-case scenario. Test your rollback plan in the test-bed to make sure it works as planned.

Admin Console

The admin console has easy access to the cloud-based lists so you can approve a comprehensive set of known apps up front. It is extremely easy for an administrator to add some obscure program to the whitelist that’s crucial to an end-user. It really takes less than a minute. Having a fast process prevents end-users from complaining that IT is not responsive to their needs. The admin console includes a way for an end-user to submit an .exe for analysis to be included/excluded from the whitelist. The gray list allows for granular customizations, and is the future of IT’s first-line malware defense. Customization for your own environment is the interesting part.

Steps For Success

As we stated above, security needs to be turned on its head and a shift from blacklisting to whitelisting needs to occur. Since the early eighties, IT departments have suffered from end-users running rampant with PCs under their own control. In the current security environment this is no longer a responsible approach. Whitelisting allows IT to get control back and rule with an iron fist in a velvet glove. Handling potential end-user resistance up front is an important tactic to make the roll-out a success. You need top-management buy-in from day one, as VPs complaining to the CEO that “IT does not let them do their work” is something that needs to be prevented from happening. The benefits of whitelisting are enormous, since traditional security defenses are becoming less effective by the year. A smart deployment of whitelisting is a great asset to any IT administrator who just wants the phone to stop ringing for a change.

Defense-in-Depth

Any professional IT team has a defense-in-depth approach that allows for maximum flexibility. You need AV scanning of web-traffic in your firewall, combined with AV scanning on your Email gateway/server and AV on the desktop level. You can decide if that needs to be on-demand or on-access AV scanning at the desktop.

And you need to add a layer that wasn’t needed a few years ago. The ROI is simple: whitelisting pays for itself. With that deployed, your security will improve significantly, support tickets decrease, your total endpoint TCO actually goes down, you have (a lot) more control, and the end-user productivity goes up. Now, who wouldn’t want all that in one neat package?
Management buy-in from day one. And convincing arguments though. Let them work for you for a change, and make sure that you get Senior end-users that feel they should be able to run anything they want. Compliance and security are very strong required, whitelisting can take some time to deploy. And sometimes whitelisting runs into resistance from auditors, which makes compliance with industry regulations much easier.

Whitelisting Helps With Compliance

The admin console has easy access to the cloud-based lists so you can approve a comprehensive set of whitelist. Run this for a few weeks, review and make changes before rolling out deny-mode. Some potential end-user resistance up front is an important tactic to make the roll-out a success. You need with PCs under their own control. In the current security environment this is no longer a responsible approach.

The cloud-based lists are as close as possible a real-time picture of all valid processes, as well as the installed by any nonprivileged end-user without admin rights or permissions. A local server contains a subset of that master list, related to all the files within your organization. Each workstation contains a small subset of the list on the server. Workstations only communicate to your local the server, they do not

There are three components. The master list with all its metadata lives in the cloud. A local server contains a subset of that master list, related to all the files within your organization. Each workstation contains a small subset of the list on the server. Workstations only communicate to your local the server, they do not

As we stated above, security needs to be turned on its head and a shift from blacklisting to whitelisting needs to occur. Since the early eighties, IT departments have suffered from end-users running rampant on their desktop. AV on the desktop level. You can decide if that needs to be on-demand or on-access AV scanning at the firewall, combined with AV scanning on your Email gateway/server and

Steps For Success

Now, who wouldn't want all that in one neat package? With that deployed, your security will improve significantly, support tickets decrease, your total cost of ownership drop substantially. And you need to add a layer that wasn't needed a few years ago. The ROI is simple: whitelisting pays for itself. With that deployed, your security will improve significantly, support tickets decrease, your total cost of ownership drop substantially.

But there is another layer. Whitelisting helps to implement the zero-day attack prevention strategy. Whitelisting can help you to detect suspicious activity. Whitelisting can help you to detect suspicious activity. Whitelisting can help you to detect suspicious activity. Whitelisting can help you to detect suspicious activity.

No Performance Penalty

There is twice as much malware as there is known-good, and that ratio is getting worse by the day. Malware has skyrocketed in volume in the last decade, and at the same time has ‘gone pro’. Malware has

Essentially, it’s time to put your endpoint security on its head. This whitepaper tells you why.

‘known-good’ to run. It’s a simple, powerful idea that stops malware dead in its tracks. It allows you to run

There is twice as much malware as there is known-good, and that ratio is getting worse by the day.

IT vendors can’t keep up, malware makes its way through, infecting workstations and opening up your network to the bad guys.

There is twice as much malware as there is known-good, and that ratio is getting worse by the day. Malware has skyrocketed in volume in the last decade, and at the same time has ‘gone pro’. Malware has

© 2011 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.