



Datasheet

Outpost Network Security 3.0

Overview

In these challenging economic times, businesses are putting reliability, efficiency, and cost-effectiveness at the top of their security solution shopping lists. Outpost Network Security 3 (ONS 3.0) is the smart choice when it comes to controlling costs while maintaining solid network security. Low per-seat price, simplicity of deployment, management and configuration, robust performance with minimal resource impact, flexibility and customization options combined with award-winning technologies make ONS 3.0 the perfect solution to protect your company's digital assets.

With Outpost Network Security 3.0, your organization is protected on all fronts against all possible types of security threat: hackers, operational disruptions and downtime, viruses and malware, web- and email-borne attacks, data loss, and inappropriate Internet usage. Central management capabilities deliver easy-to-use, trouble-free endpoint protection for any organization with limited in-house IT resources.

The SMB Security Challenge

A turbulent economy has brought with it exponential growth in attacks targeting electronic communications and other valuable data, compelling organizations to rethink the way their business-critical assets are protected. Software vulnerabilities pave the way for zero-day malware attacks and data breaches, so organizations must mitigate these threats before an attacker is able to exploit them. At the same time, the number of mutating and polymorphic viruses that can't be detected with conventional signature-based methods is skyrocketing, and sophisticated root-kits and Trojans require the adoption of new and more intelligent response mechanisms. And of course, humans remain the single biggest weak point in any security infrastructure, with users visiting inappropriate websites, taking confidential data out of the organization on USB drives and then losing or selling their contents. The widespread and inappropriate use of social networking, online videos and chat sites only makes the situation worse.

While users are busy challenging security controls at the endpoint level, those who must act as IT or security administrators are faced with the uphill task of keeping protections properly configured and up-to-date in order to tackle the latest threats. Even businesses with a couple of dozen PCs need a centralized way to deploy, configure and manage protection remotely without the need to visit every workstation individually – or have a degree in information technology.

The ONS 3.0 Solution

At a Glance

Outpost Network Security works by creating a secure environment across the network, from endpoint to server and everything in between. Its automated protection tools run in background on client PCs, protecting endpoints against the latest threats and ensuring malware cannot spread across the network and beyond. Client protection is deployed from a single administration console that can be accessed on any computer, enabling the designated administrator to remotely control workstation protection; managing configuration, running protection tasks and updating client software can all be accomplished from a single location.

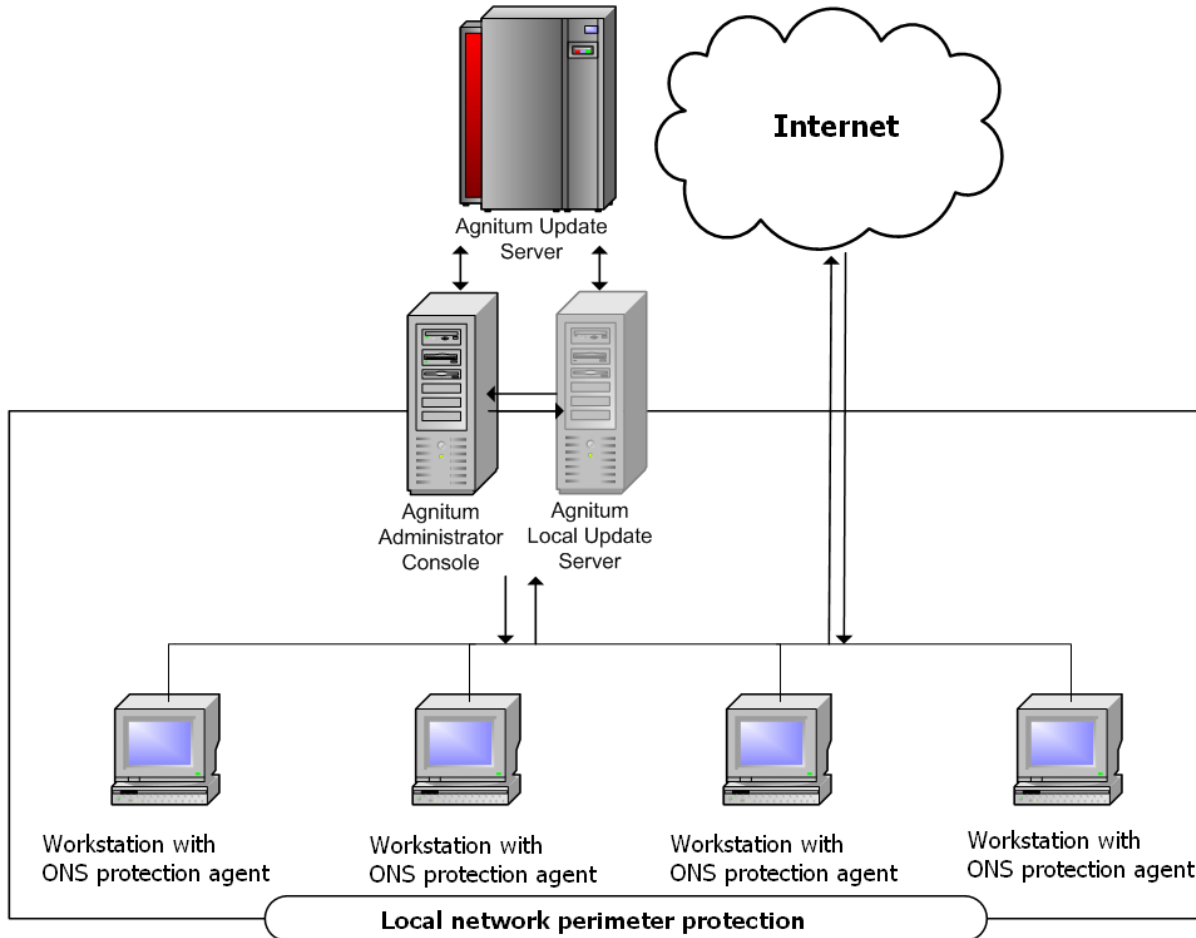
Outpost Network Security is the ideal choice for organizations with:

- Networks from 5 to 500 PCs
- Mobile, telecommuting or travelling workers
- Multiple branch offices
- Restricted budgets

ONS Protection Highlights

- Automated virus and spyware filter controls endpoint security in real-time
- On-demand security scanner checks remote machines for malware
- Bidirectional firewall monitors connections and protects against internal and external network attacks
- USB block keeps company data under your control and prevents leakage
- Host protection adds an extra layer by proactively blocking activity of unknown malware
- Web control ensures users can't access dangerous or restricted web sites
- ID theft prevention restricts the transfer of predefined text blocks like passwords and credit card numbers
- Self-protection prevents malware performing an unauthorized shutdown of endpoint protection
- Process- and network activity monitor tracks remote events in real time
- Remote logs let you view past records for auditing purposes

Outpost Network Security 3.0 protects the digital perimeter of your organization



Outpost Network Security 3.0 Benefits

No security incidents

Information is the most prized asset within an organization. Outpost ensures the integrity of your data by offering a number of robust security mechanisms:

- **Antivirus to ensure malware-free environment**

The VB100-certified engine combining virus and spyware defense is constantly on guard against malicious software arising internally (i.e. received as an email attachment) or acquired externally (i.e. spreading via an infected USB flash drive). The threat is instantly neutralized before it can harm other member machines. On-demand remote and centralized virus scans can be initiated on select endpoints at any time.

- **Bidirectional firewall to bolster LAN connectivity**

The award winning firewall technology ensures safety and continuity of your company's network operations. Encompassing a unique intrusion detection system to shield traffic against eavesdropping, packet- and application-level filtering to block unwanted or malicious connections, embedded code protection to shore up vulnerable web elements, Outpost Network Security is the ultimate deterrent to all manner of data compromises and hacker attacks.

- **USB access lockdown to guard company's digital assets**

Your internal data is at risk of being copied and extracted from the organization. Outpost Network Security blocks access to mass storage USB devices on target hosts, preventing unauthorized leak of company data and malware propagation from connecting flash memory drives.

Effortless rollout and hands-free updates

- **Centralized deployment to minimize IT workload**

With intuitive tools that map organization's network domain structure, mass deployment can be carried out almost in no time.

- **Online and offline updates to keep protection current**

Security updates for intranet-connected machines are deployed daily from a single network repository, such as Agnitum Server, a local updates server or a local folder with updated bases.

Centralized management and setup

- **Group segmentation for more targeted protection**

Connected computers can be broken out into multiple groups with each group having its own security properties. This helps to better manage and target protection recipients, as well as assign tougher policies for more susceptible groups (i.e. a group of mobile users that connect to 3rd party networks on the go).

- **Remote configuration for easy, hands-on management**

In the new version of Outpost Network Security, interconnected computers can be managed from any member workstation through a universal management console. Administrators can designate custom Internet access policies and specify the blacklisted URL addresses that will be inaccessible across the network.

Better visibility into remote events

- **Real-time control of endpoint activity for total transparency**

Once your network is up and running, it's hard to control events that are taking place on individual machines. Outpost deals with this limitation by offering real-time monitoring of system and network activity for any remote host. With this handy tool, administrators can see what sites are being accessed or what programs are currently active on any computer on the network. This also enables administrators to quickly edit existing access policies for the target hosts.

- **Remote logging system for better understanding past activity**

Outpost's remote logger shows history of all past events occurring on remote machines, enabling IT managers to quickly find a problem and correct it without leaving their desks.

Lightweight protection that stays on all the time

- **Faster, resource-friendly operation for smoother protection with SmartScan 3**

Thanks to numerous optimizations and unique performance-boosting technologies, client Outpost protection is performed in the background without taking up vital system resources. Security checks complete up to ten times faster than some of the competition.

- **Unauthorized termination prevention to guarantee continuity of protection**

Workstations' Outpost protection cannot be switched off by targeted termination attacks, meaning your networked clients are protected 24/7.

Universal compatibility

- **Modern hardware and software support for broader deployment**

Outpost Network Security protection can be installed on any recent Windows platform, simplifying deployment and eliminating learning overhead. Outpost protection can be deployed on company's gateway PC that is already running 3d-party security products such as antivirus or anti-spam software. Native support for 64-bit Windows versions lets you experience all the benefits of modern computing.

Outpost Network Security 3.0 Features

Data security and confidentiality

- **Powerful malware protection**

Outpost Network Security delivers comprehensive protection against all forms of malware threat, including viruses, spyware, Trojans and worms; it will protect your company's workstations 24/7, no matter the level of user experience. The automated background scanner prevents malware infections in real time, while the centralized on-demand file scanner uses Agnitum's unique SmartScan 3 technology to provide fast and efficient detection and disinfection for all data storage areas – local, remote, and shared. An IT administrator can initiate arbitrary remote scan on any selected workstation (provided that it has the administrative console installed), plus the organization's computers are checked against new infections at regular time intervals via the scheduled scans feature. Updated threat signatures are distributed daily through a designated point on your network – Agnitum Server, local updates server or a local folder with updated databases.

- **Continuity of network operations**

The client-based ONS firewall protects incoming and outgoing network connections, filtering all traffic according to administrator-defined access policies and blocking unwanted or malicious transmissions. Unique Ethernet protection guards against man-in-the-middle attacks designed to intercept network data, ensuring data in transit always reaches the designated recipient.

- **Lock down USB devices**

To prevent malware propagation from external sources, as well as the unauthorized copying of internal company data, businesses can implement USB storage device usage restriction on specific employees.

- **Secure storage vault for critical data**

ONS 3.0 includes targeted data protection to prevent confidential corporate information from ever being removed from an Outpost-protected workstation. Companies can specify items of critical importance to be blocked from transmission by employees over IM, email or the web.

- **Web security**

The web is the number one source of corporate security threats today. Outpost Network Security keeps productivity up and risk down by limiting the amount of web content that can be run or displayed on individual workstations. From blocking unsafe scripting to suppressing unnecessary web graphics, animation and ad banners, ONS prevents drive-by downloads and other stealthy web-based attacks. Additionally, managers can block access to specific unsafe Internet domains on a user-by-user basis.

- **Self-defense ensures round-the-clock protection**

ONS 3.0 includes self-defense technology to block attempts by unauthorized third parties to shut down its protection, ensuring that protection is never interrupted.

Control and manageability

- **Centralized deployment and administration**

Client protection is deployed from a central administrative console simply by selecting the target recipients. In just a few minutes, all designated endpoints are protected. All subsequent administration procedures can be managed from any workstation on the network.

- **User group segmentation**

Support for user groups enables different configurations and access policies to be deployed to different users depending on their risk level.

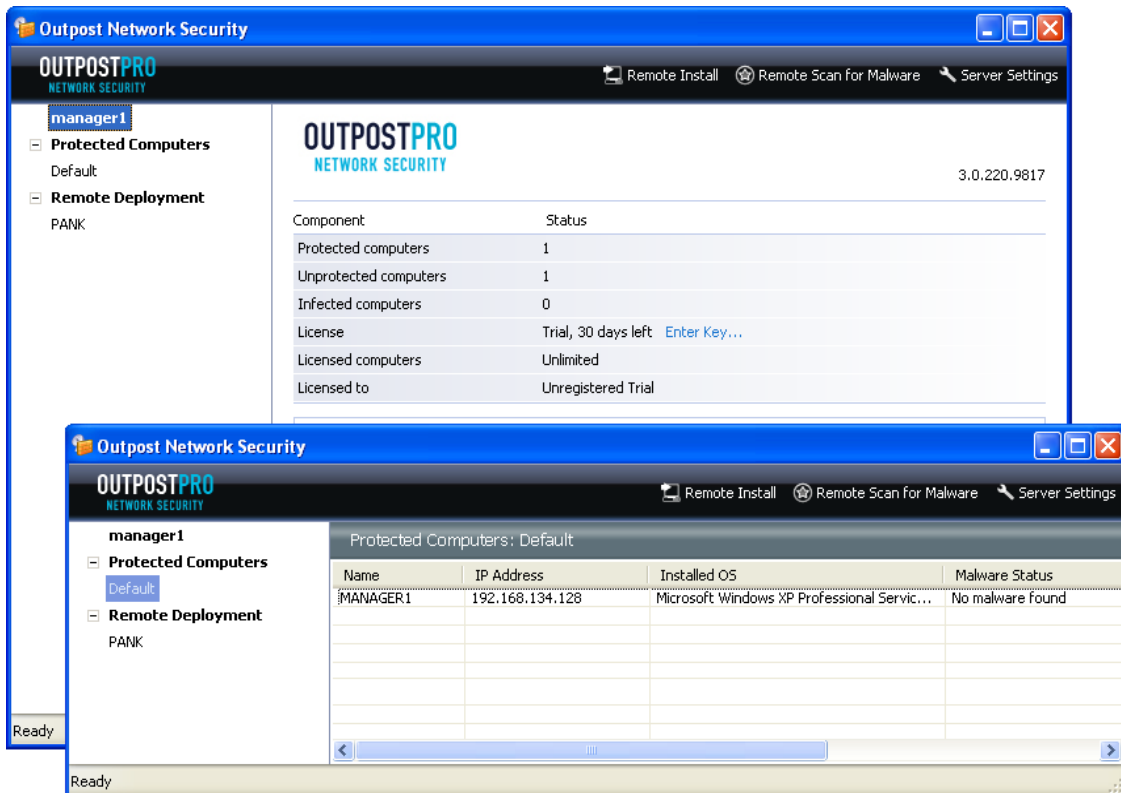
- **Detailed visibility into remote events**

ONS 3.0 uniquely enables administrators to control events on remote machines in real time. Activity reports include information such as active programs and processes, network addresses being accessed and other current statistics.

- **Comprehensive event logger**

With extensive logs of endpoints' past activity, administrators can easily find and fix connection problems, view malware removal status, and access other maintenance-related information.

Management Console is the essential part of ONS 3.0 operation – this window offers access to all program features and remote deployment options



Outpost Network Security 3.0 Version Progress

Product version	Outpost Office Firewall (former title, year 2005)	Outpost Network Security 2.0 (year 2007)	Outpost Network Security 3.0 (year 2009)
Firewall for protecting endpoint connections	yes	yes	yes
Antispyware for basic malware protection	yes	yes	yes
Antivirus for total malware protection	no	no	yes
Simplified deployment through cloud installation	no	no	yes
Secure storage for company-critical data	no	yes	yes
Remotely executable on-demand malware scans	no	no	yes
USB storage devices access lockdown	no	no	yes
“Host Protection” for 0-day attack defense	no	no	yes
Centrally managed blacklisted URLs	no	no	yes
User group segmentation for more targeted protection	no	yes	yes
Remote viewing of past event logs	no	no	yes
Real-time endpoint activity monitoring with instant access to policy editing option	no	no	yes
File servers compatibility for server/client agents	yes	yes	yes
Native 64-bit Windows support	no	no	Yes
Streamlined performance	no	no	yes
Administrator console support for modern Windows versions (Vista and Server 2008)	no	no	Yes

Outpost Network Security 3.02 System Requirements

Supported platforms:

Client side: Windows XP (SP1, SP2, SP3), Windows Vista (32- and 64-bit versions, including SP1 and SP2), Windows 7
Server side: Windows 2000 SP4, Windows Server 2003, Windows 2008 server (32- and 64-bit versions, SP1 and SP2)

Hardware:

800 MHz or faster CPU(x-86/x-64/multi-core), 256Mb RAM, 100MB free disk space.

Your Next Step

To find out for yourself how easy it is to protect your small business against the threats of today and tomorrow, to go <http://www.agnitum.com/products/networksecurity/index.php> and download a full-function 30-day trial of ONS 3.0.