



DELIVERING SECURE MOBILITY®



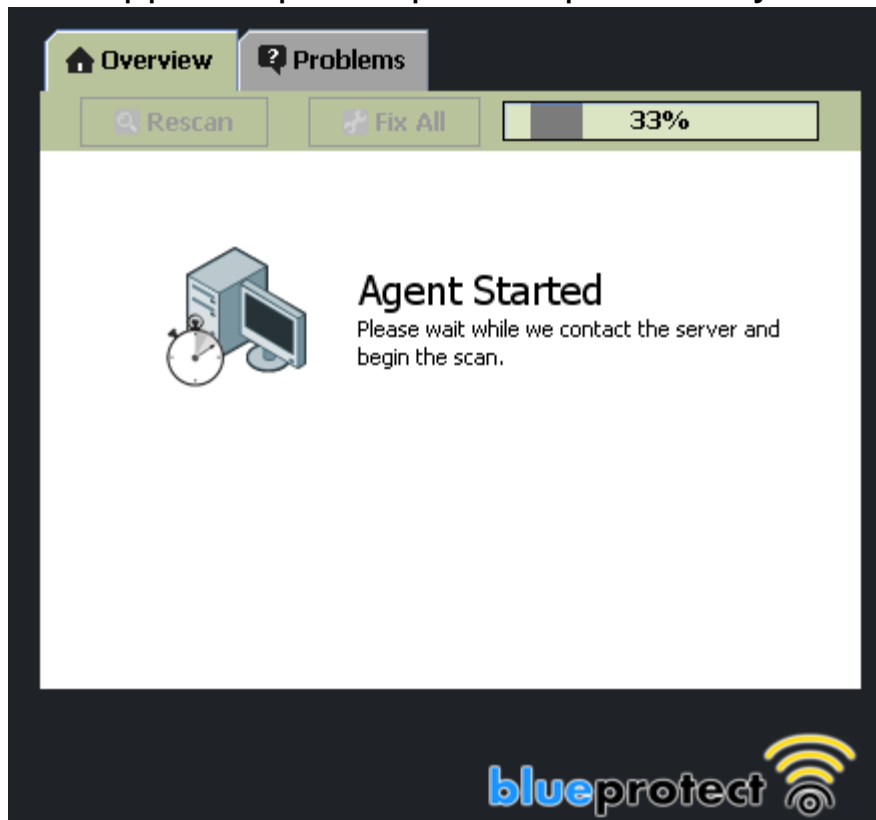
**BlueProtect™**

***Trusted Endpoint Assurance***

# BlueProtect™ Overview

BlueProtect™ ensures that a client device is a trusted end-point.

- A scan detects the presence and state of administrator-specified security applications.
- A successful scan is a required before allowing the device onto the network.
- Support separate policies per identity/role (i.e. faculty versus student)



## Scans for

- Antivirus
- Antispyware
- Firewall
- OS/Patch level
- P2P Programs
- Files
- Registry
- Processes

<b>General</b>
<b>Policy Details</b>
<b>Antivirus</b>
<a href="#">Windows</a>
<a href="#">Mac OS X</a>
<a href="#">Linux</a>
<b>Antispyware</b>
<a href="#">Windows</a>
<a href="#">Mac OS X</a>
<b>Firewall</b>
<a href="#">Windows</a>
<a href="#">Mac OS X</a>
<a href="#">Linux</a>
<b>Patch Management</b>
<a href="#">Windows</a>
<b>Peer to Peer</b>
<a href="#">Windows</a>
<b>Files</b>
<a href="#">Windows</a>
<b>Registry</b>
<a href="#">Windows</a>
<b>Process Control</b>
<a href="#">Windows</a>

# BlueProtect™ Key Differentiators

- No client-side software.
- Single box integrated solution.
- Support for 976 unique products →
- Supports 8 categories of client scanning.
- One-click Remediation.
- Complete system scan in less than 60 seconds.

OS	Type	Count
Windows	AV	448
Windows	FW	229
Windows	AS	174
Windows	Patch	6
Windows	P2P	69
Mac	AV	19
Mac	FW	16
Mac	AS	1
Linux	AV	23
Linux	FW	1

# Client Applet

- The client must have or install java (1.4.2 or later).
  - BlueProtect uses a java based dissolvable client.
- Supported Operating Systems (Firefox 1.5+ is supported for all OS)
  - Windows (2000, 2003, XP, Vista)
    - Also supports Internet Explorer (5.5+)
  - Mac OSX (10.3+, PowerPC and Intel)
    - Also supports Safari
  - RPM Based Linux Distributions (RedHat 4/5, Fedora Core 5+)
  - Debian Linux Distributions (Ubuntu 6.10+)
- Unsupported Clients and Operating Systems:
  - iPhone, Blackberry, Symbian, Windows Mobile and PocketPC
  - Administrator can choose to deny or allow unsupported clients
    - typically Allow, as these don't have the same exposure as laptops

# Policy Generator

- Multiple policies can be created, even one per role.
  - Allows for granular rollout.
- Individual policy rules for Windows, Mac OS and Linux.
  - Can enforce policies on just Windows.
- The scan result is based on:
  - Software being installed on the system
  - Real-time updates being enabled
  - Date of definition file
  - Signature of definition file
  - Last time the system was scanned against the definition file
- Each rule will **Warn** or **Restrict** users.

**Edit BlueProtect policy - Corp Scan**

Back Delete Save Next Category

Enable Peer to Peer Category

**Select Products**  
Check all Uncheck all


- Anatomic P2P
- Ares Development Group
- Azureus, Inc
- BitComet
- Bitmap Multimedia
- BitTorrent, Inc.
- CruxP2P LLC
- Deepnet Technologies
- East Bay Technologies

**Check P2P Application Installed**  
Enable Application Installed Check  
Yes

Activate to enforce this rule.  
If P2P Application is Installed  
Restrict User

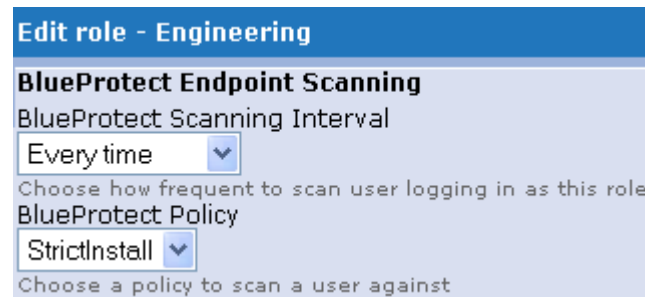
Restrict: User will be blocked  
Warn: User will be notified.

# Remediation

- When an endpoint fails the security policy scan, it is blocked. To become compliant, the following methods are used:
  - Auto Remediation
    - User clicks “Fix All” which performs updates to anti-virus definitions, enables firewall, etc. When complete, the client is automatically rescanned.
  - Manual Remediation 
    - User is required to manually address the failures which might include visiting Anti-spyware website to download the latest definitions. User then clicks “Re-Scan” on the applet to restart the scan.
- BlueSecure Controller Zero Config Remediation
  - Admin chooses Unregistered role or ‘BlueProtectRemediation’ role.
  - The role intelligently opens destination IP addresses in the firewall to allow endpoints to reach remediation sites.
    - If administrator requires McAfee antivirus, www.mcafee.com is allowed.
  - Feature is configured in GUI via “Enable Zero Config Remediation.”
- Customizable Scanning page
  - Includes Policy Based Remediation message (call the Mac helpdesk)

# BSC Integration

- **Universal Authentication Support**
  - External Server
  - Transparent Authentication (NTLM/802.1x)
  - MAC Authentication
  - Guest Access
  - Integrated into Role ->
- **Database Support**
  - Configuration Replication
  - Backup and Restore
  - Secure Mobility Matrix



**Edit role - Engineering**

**BlueProtect Endpoint Scanning**

BlueProtect Scanning Interval  
Every time

Choose how frequent to scan user logging in as this role

BlueProtect Policy  
StrictInstall

Choose a policy to scan a user against

# License is Required

- Request is made via the Bluesocket Support Portal
  - Based off hardware specific BSC serial number.
  - Emailed back within 48 hours.
  - Multi-box setups require license for each box.
  - Enables BlueProtect feature and ability to receive definition updates
- License renewals
  - New license Renewals available after first year.
  - After expiration, feature is still active but auto updates are disabled.

Manage Licenses for BSC-5200

Reset Save Licenses

**BlueProtect Endpoint Scanning**

License

Expires 5-01-10

Enter your License.  
Click [here](#) to proceed to enable and configure endpoint scanning.

**BSC Users License**

Current Max User Count: 4000  
BSC key: 00:15:17:16:01:78

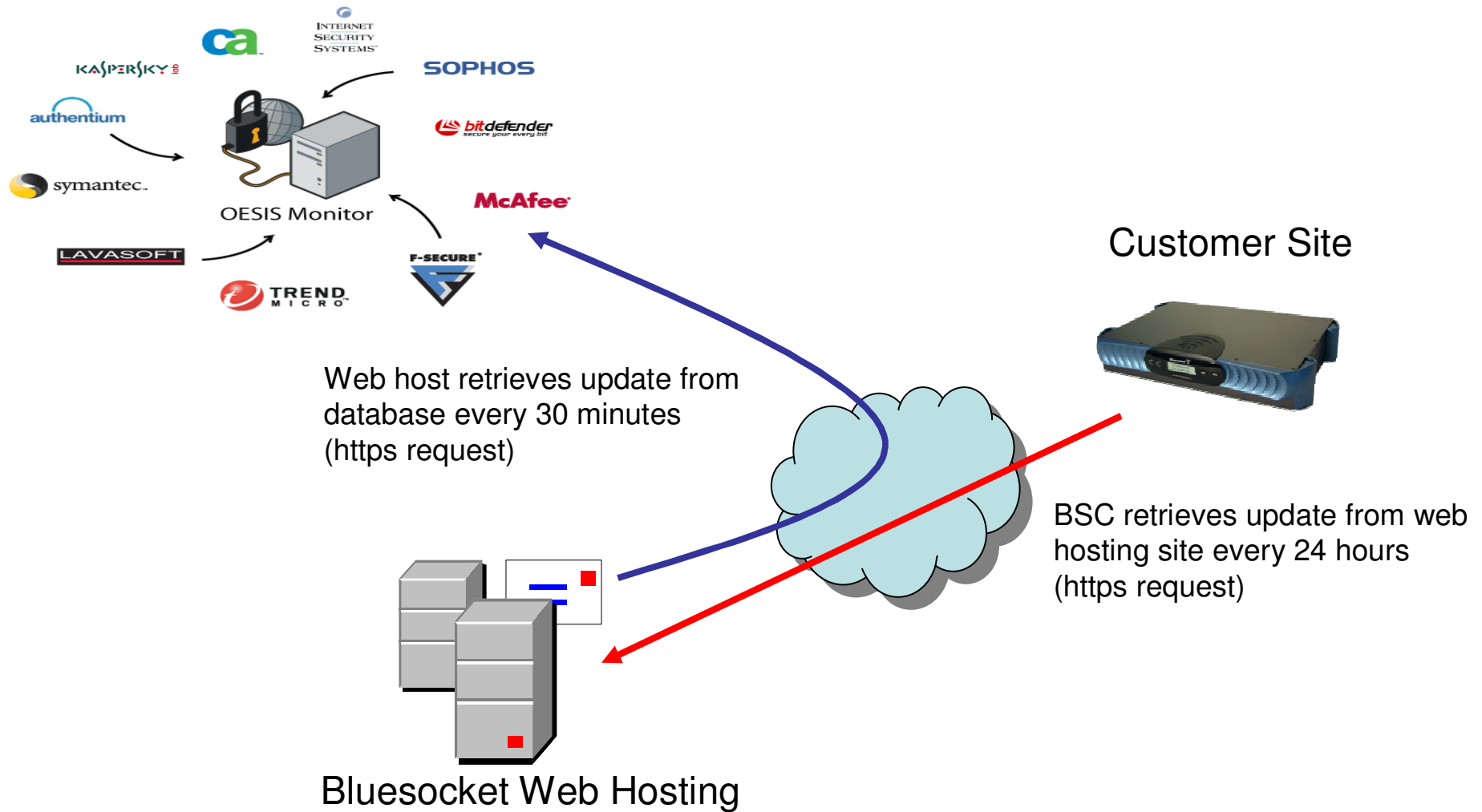
[Bluesocket License Request](#)

User License

Browse...

Reset Save Licenses

# Auto Definition Updates



## 6.4 BluePatch 5 - Feature Set Support

- P2P Application Detection
  - Force client to uninstall bit-torrent, etc.
- Patch Detection
  - Ensure a client has Microsoft patches and auto-update enabled.
- File, Process and Registry Queries
  - Ensure client has a file in a specific state (C:\Windows\cmd.exe)
    - Existence/non-existence of file
    - Md5sum of file
    - Timestamp of file
    - Version of file
  - Ensure client has/doesn't have a process running
  - Ensure client has/doesn't have a registry key

# Case Study – P2P Applications

## Check P2P Application Installed

Enable Application Installed Check

Yes

Activate to enforce this rule.

If P2P Application is Installed

Restrict User

Restrict: User will be blocked

Warn: User will be notified.

## Check P2P Application Running

Enable Application Status Check

Yes

Activate to enforce this rule.

If P2P Application is Running

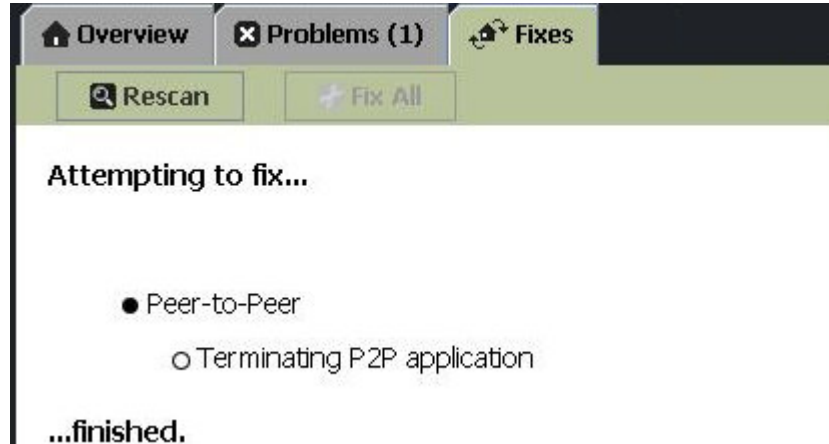
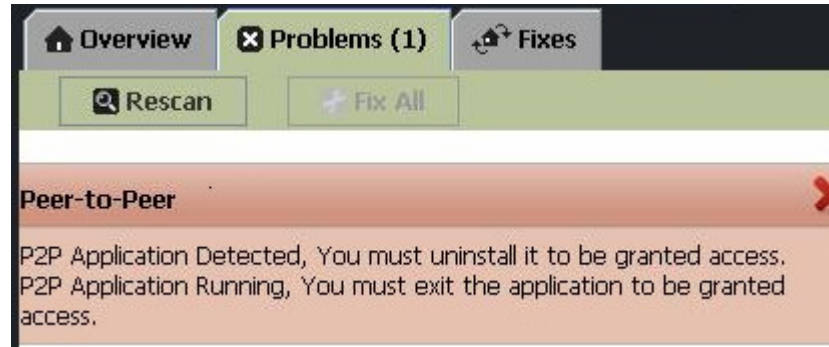
Restrict User

Restrict: User will be blocked

Warn: User will be notified.

## Select Products

- Anatomic P2P
- Ares Development Group
- Azureus, Inc
- BitComet
- Bitmap Multimedia
- BitTorrent, Inc.
- BitTorrent
- uTorrent
- CruxP2P LLC



# Case Study - Conficker Virus

- Conficker has infected over 10 million PCs worldwide
  - Must prevent a client with this virus from gaining access to the intranet and infecting other computers.
- BlueProtect Detection/Remediation
  - Ensure that real time protection is enabled.
    - Conficker will disable RTP for Windows Defender.
  - Ensure that AV definition is the latest.
    - Blocks user if definitions are 1 or more revisions old.
  - Ensure that AV scan has been successful.
  - Patch management checks for specific patches.
    - Conficker targets missing Windows patch (for buffer overflow).

# Sample Reporting – OS, Browser Breakdown

