



eEye[®] Digital Security

Blink[®]

End-Point

Vulnerability Prevention

Today's Protection Has Its Limitations

Perimeter Protection

- Does not protect from laptops, rogue machines and employees within the network
- Relies on knowledge of attack (signatures)

Patch Management

- Only protects from known vulnerabilities where patch is available
- Shrinking window of time to deploy patch
- Costly in resources and business disruption

Software Firewalls

- Does not prevent attacks that leverage unknown vulnerabilities
- Restricts connections or processes...
- ... or relies on user intervention

Security Must Evolve to Match Today's Threats

- **Protecting from Unknown Vulnerabilities**
 - Most malicious hackers are using unknown vulnerabilities in targeted attacks against enterprises
- **'Panic Patching' Is A Costly Endeavor**
 - Large enterprises are spending millions of dollars (measured in lost productivity and business disruption) when non-scheduled patching is required
- **Protecting (From) Mobile Workers**
 - Mobile workers and teleworkers, acquire infections “in the wild” and introduce them to the network once they reconnect
- **Protection from Internal Threats**
 - Majority of attacks originate from rogue employees within the network, and threats in which hackers leverage naïve employees into making their systems vulnerable

Today's Threats Require a New Approach

***Enterprises Need the Means to Protect Themselves
Even When Patching is Not an Option***

- **Protect digital assets from yet *undiscovered* vulnerabilities**
- **Implement defenses against internal, malicious or socially engineered threats**
- **Defer patching to regular maintenance schedules**

NEW PARADIGM

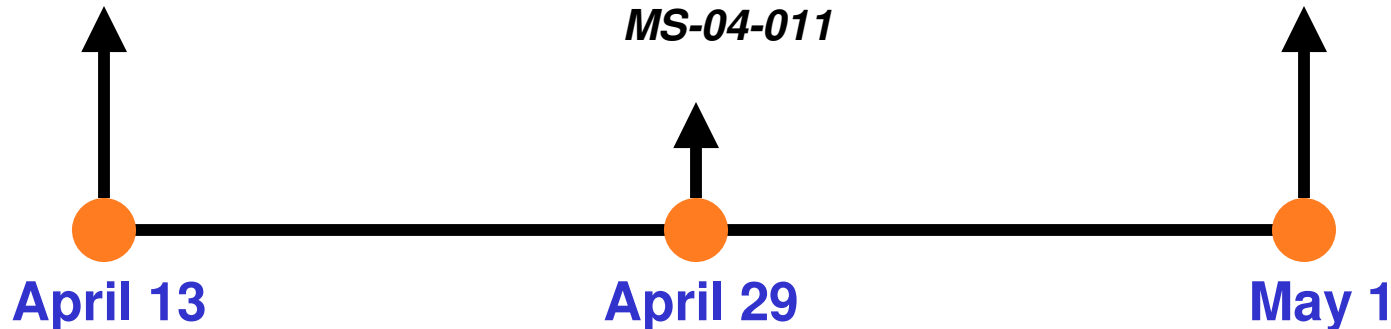
*Protect Individual Digital Assets – Not just the Network
Perimeter*

Sasser Appears 18 days after Microsoft Security Bulletin

Over 500,000 computers infected in first 24 hours

Microsoft releases
MS-04-011, a single patch
for 14 individual
vulnerabilities, including
LSASS

April 13



A horizontal timeline with three orange circular markers. An upward-pointing arrow connects the first marker to the text 'Microsoft releases MS-04-011...'. A second upward-pointing arrow connects the second marker to the text 'Exploit code appears on Internet...'. A third upward-pointing arrow connects the third marker to the text 'Sasser worm emerges...'. The dates 'April 13', 'April 29', and 'May 1' are written below their respective markers.

Exploit code appears
on Internet
*Due to size of patch and
number of applications
affected, many
organizations had not
deployed
MS-04-011*

April 29

Sasser worm
emerges,
leveraging
exploit code
released 2 days
prior

May 1

“...patching will always be reactive. So layered protection is still the best, starting with policy-based, centrally-managed desktop firewalls and anti-virus.”

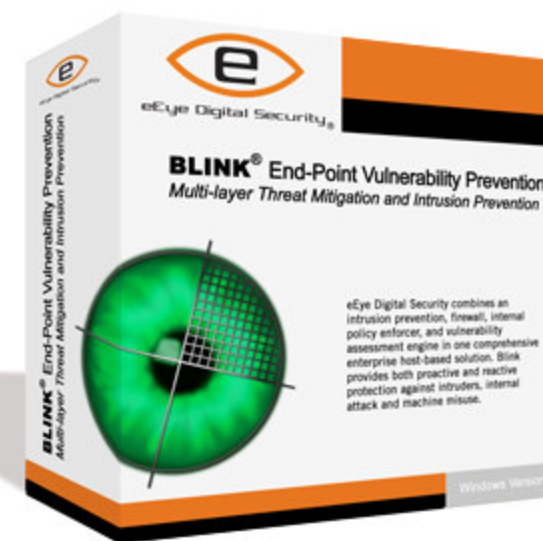
- SecurityFocus, “Companies Adapt to a zero day world” 7/13/04

Gartner Bottom Line: *“Host-based security brings strong security to complex environments. **Develop architectures that will incorporate host-based security** platforms no later than 2006”*

- Gartner, *It’s Time For Host Based Security Platforms 2004*

What is Blink?

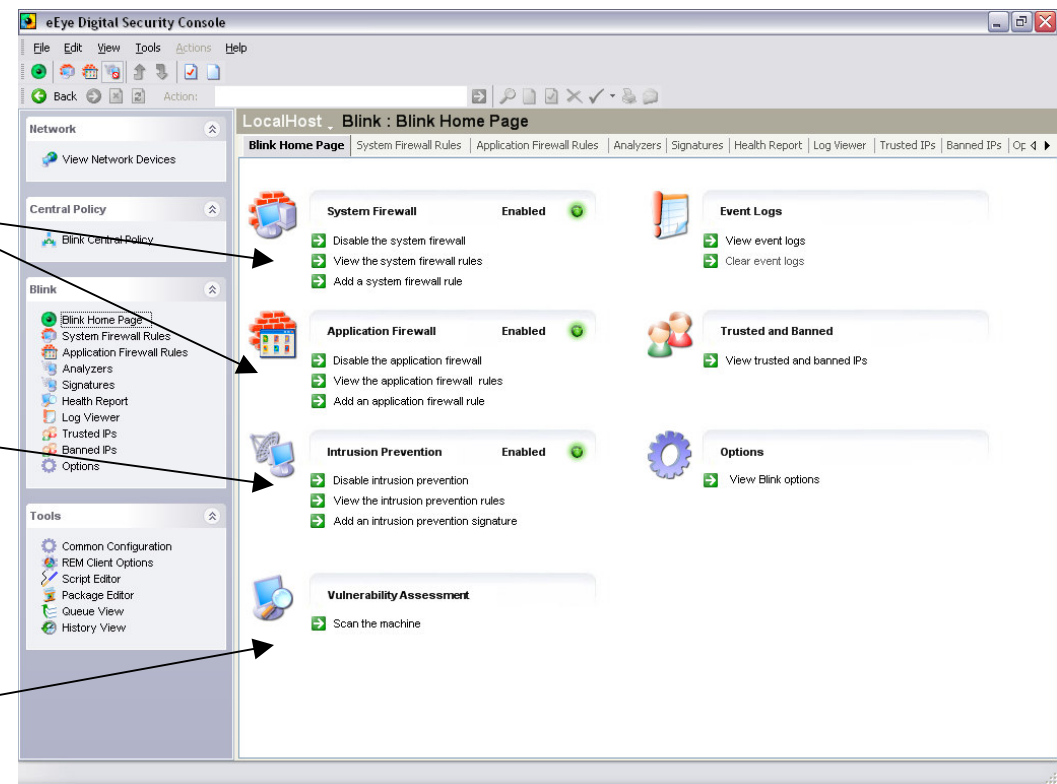
- **Agent resides on the asset – Server, workstation, laptop**
- **Shields the asset from intrusion – worms and targeted attacks**
- **Prevents asset from unauthorized connections to other machines**
- **Stops unauthorized applications from being deployed**
- **Requires no user intervention or security expertise**
- **Replaces software firewalls and complements anti-virus, malware**



Comprehensive End-Point Security

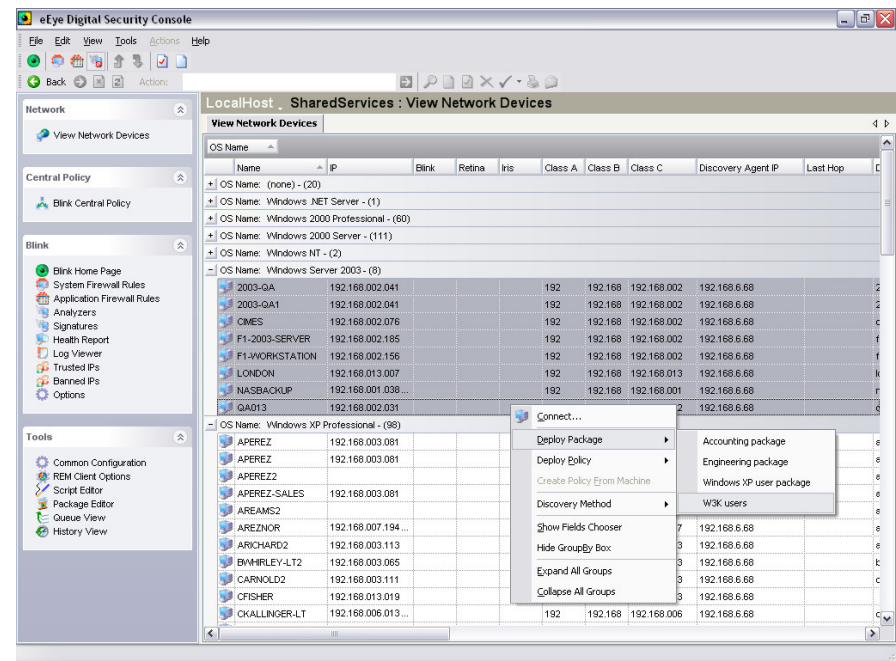
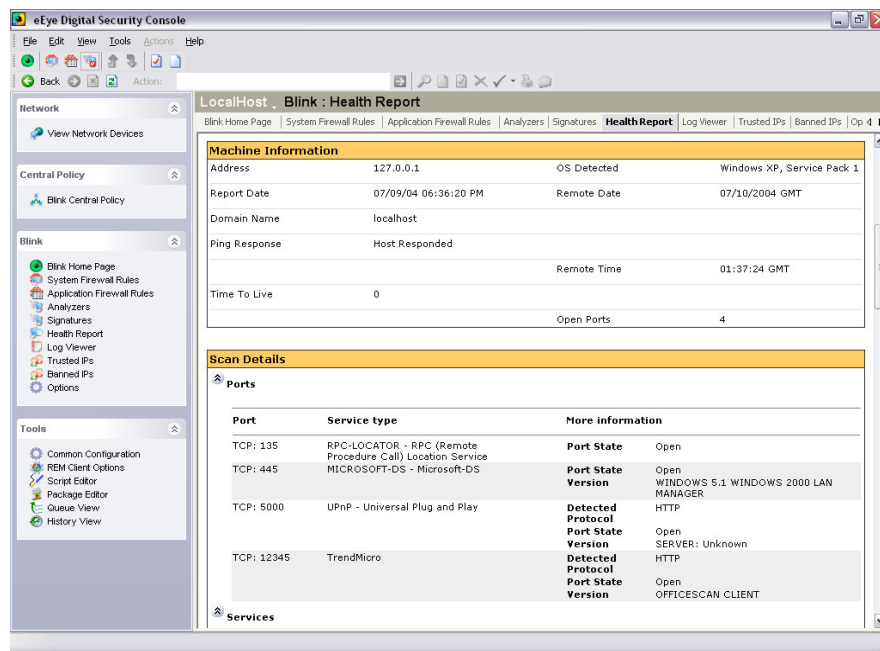
Combines multiple layers of protection to ensure absolute protection of and from asset

Protection Layer	Approach to Protection
Host-Level Firewall	Prevents unauthorized connectivity and applications from running
Intrusion Prevention System	Shields the asset from unknown attacks without the use of signatures
Vulnerability Assessment Scanner	Detects known security issues and policy non-compliance



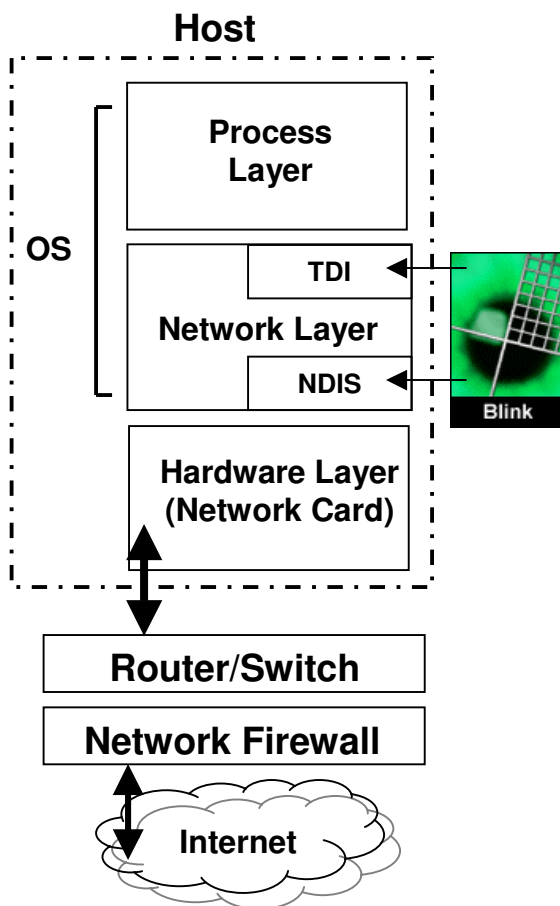
Enterprise-Class Intrusion Prevention

- **Designed for Enterprise Deployment**
 - Non-intrusive, transparent to end-users
 - Minimal impact to system performance



- **Enterprise Management Capabilities**
 - Remote deployment and management
 - Centralized administration
 - Events aggregation, correlation and analysis

Approach To Host-Level Protection



Multiple Layers of Protection

Layers of Protection	Blink
Non-Signature Based IPS	<input checked="" type="checkbox"/>
Rules Based IPS	<input checked="" type="checkbox"/>
Network Level Firewall	<input checked="" type="checkbox"/>
Application Level Firewall	<input checked="" type="checkbox"/>
Host Level Vulnerability Assessment	<input checked="" type="checkbox"/>
Non-Intrusive Process Activity Monitors	<input checked="" type="checkbox"/>

Enterprise Support

- Central Policy Management
- Central Agent Administration
- Remote Agent Deployment
- Central Events Management
- Central Workflow and Prioritization

Blink Competitive Landscape

Host Based Security Solution Comparison	eEye Digital Security Blink	Cisco Security Agent	McAfee Desktop Firewall	McAfee Enterccept Desktop	Sygate Secure Enterprise	Symantec Client Security	ZoneLabs Integrity	ISS RealSecure Desktop	Windows XP SP2
Security Layers									
Protocol Based Intrusion Prevention	●	○	○	○	○	○	○	●	○
Rules Based Intrusion Prevention	●	⊙	○	⊙	○	○	○	⊙	○
Network Based System Firewall	●	○	●	○	●	●	●	○	●
Network Based Application Firewall	●	○	●	○	●	●	●	⊙	⊙
Host Based Vulnerability Assessment	●	○	○	○	○	○	○	○	○
Process Based Buffer Overflow Protection	●	⊙	○	⊙	○	○	○	⊙	○
Enterprise Capabilities									
Enterprise Workflow Management	●	○	○	○	○	○	○	○	○
Enterprise Reporting and Analysis	●	⊙	○	○	○	○	○	●	○
Central Policy Server	●	⊙	⊙	⊙	●	⊙	●	●	⊙
Central Auto-Update Server	●	●	○	○	⊙	⊙	⊙	●	○
Central Event Server	●	⊙	○	⊙	⊙	○	○	●	○
Centralized Administration Capabilities	●	⊙	○	⊙	○	○	○	⊙	⊙
Remote Management Capabilities	●	○	○	○	○	○	○	○	○
Centralized Remote Deployment	●	○	○	○	○	○	○	○	○
Transparent End-User Experience	●	○	○	○	⊙	○	○	○	○

Legend:

- YES
- ⊙ LIMITED
- NO

```
if (argc < 3)
{
    printf ("\nwwwget - determine what httpd version a site is running\n");
    printf ("punkis@attrition.org ==\n");
    printf ("arg[1] is %s\n", argv[1]);
    return 1;
}
host = argv[1];
sport = atoi(argv[2]);
hostinfo = gethostbyname(host);
if (!hostinfo)
{
    fprintf(stderr, "Host: %s\n", host);
    exit(1);
}
servinfo = getservbyname("http", "tcp");
if (!servinfo)
```

VULNERABILITY IS OVER