

ServerShield™ Technology Brief



2007 Best of Interop
Security



2007 Technology of the
Year Award
Security



Best of VMworld 2007
Finalist
Data Protection



Ten Virtualization
vendors to watch in
2008

Overview

Blue Lane's VirtualShield and ServerShield products secure virtual and physical server farms, including OS, database and application services. Blue Lane's products are unique in that they protect servers more accurately and against more threats than existing technologies, without compromising uptime when deployed in full-protection mode.

Current host and network Intrusion Detection/Prevention technologies fall short when it comes to providing an operationally viable solution to meet the security and compliance mandates for servers, because of intrinsic architectural limitations. The onset of virtualization has further aggravated the problem.

Blue Lane's patented system has taken a fundamentally different approach to solving this security/operations dilemma. The products are built on next generation IPS technology, specifically aiming to resolve critical shortcomings of current IPS architectures.

Next Generation IPS technology is critical to provide deterministic yet effective server security as organizations accelerate their security, compliance and virtualization efforts. To summarize, the requirements for next generation IPS server security include:

- Secure physical & virtual servers, including inter-VM and intra-rack protection
- Accurate vulnerability detection without false positives or negatives
- Effective vulnerability protection without business disruption
- Complete coverage for OS, database, web services, and virtualization hosts
- Resilience in the face of IPS evasion techniques
- Operational viability without onerous tuning, testing and management

Blue Lane's ServerShield and VirtualShield product lines address these requirements, and provide compelling benefits over current IPS technologies.

Historical background

Current network-based Intrusion Prevention Systems (IPS) products evolved from Intrusion Detection Systems (IDS) products, and are based on two key architectural building blocks:

- Static regular expression signatures to pattern exploits, and more recently vulnerabilities.
- Deep packet inspection, with hardware regex processing, to match signatures. IPS products add the capability to block by resetting connections, if a signature match is found.

There are major shortcomings with this architecture.

- Static signatures cannot adequately pattern threats, for example:
 - ◆ Transient, polymorphic threats result in signature chasing and explosion.
 - ◆ Programmable SQL where there is no fixed pattern to base a signature on.
 - ◆ Non-contiguous threats exploiting cross request, cross session vulnerabilities.
 - ◆ Complex threats like cross-site scripting, sql injection, web form attacks.

- Hardware regex processing cannot adequately scale
 - ◆ Upgrades are required to handle additional signatures, higher bandwidth.
 - ◆ Augmenting regex with slow-path software kills stated performance metrics.
 - ◆ Migrating to software-centric, multi-core virtualization platforms is a challenge.
- Highly publicized IPS evasion techniques bypass IPS checks
 - ◆ Fragmentation/interleaving, etc, is beyond the scope of regex signature processing.
 - ◆ Exploding exploit rate and variance cause operators to turn off signatures.
- The “blocking” capability via connection resets causes applications to break
 - ◆ Impacts multi-session connections e.g. db connection pools, mail relays.
 - ◆ Inaccurate detection followed by blocking causes business outage.

Consequently, organizations turn on blocking for less than 20% of the available signatures, resulting in IPS technologies being little more than IDS technologies, used as early warning systems, and requiring onerous resources and external tools to sift through the thousands of false alarms. To address these shortcomings, vendors have augmented their products with heuristics like behavioural anomaly detection, classifying signatures as high fidelity, signature tuning wizards, etc, all of which bring up their associated set of issues. The net effect is that the onus of making false positive / false negative tradeoffs has been shifted from the security vendor to the customer, resulting in escalating cost of ownership for such technologies.

Other alternatives include using Host Intrusion Prevention Systems (HIPS), VLAN segmentation, or diligently applying security patches.

Host Intrusion Prevention Systems suffer from major drawbacks when it comes to protecting servers:

- Proliferation of agents that need to be constantly upgraded on hosts.
- They are typically OS specific, in fact largely Microsoft-centric.
 - ◆ Lack of a homogenous solution to protect against all servers.
- Solutions are intrusive and have high impact on server performance.

Security Patches fix the underlying root cause vulnerability. While applying security patches ought to be the staple of any defense-in-depth strategy, there are some obstacles to overcome nevertheless:

- Even the most diligent enterprise takes upwards of two weeks to apply Microsoft patches after Patch Tuesday, and much longer for Oracle CPUs, for example. Consequently, the exposure window from the time a vulnerability is known, to the time the vendor releases a patch, to the time the patch is tested and applied on every server or database, can run from weeks to months at best.
- Zero day exploits and vulnerabilities, and threats like cross-site scripting, or sql injection attacks, are not handled in a timely fashion by security patches.
- Operational issues are by far the stickiest issue. Devoting adequate resources, securing downtime to patch servers, and going through application testing cycles involve a significant logistics burden and elapsed time, causing organizations to question the risk-reward trade-off.

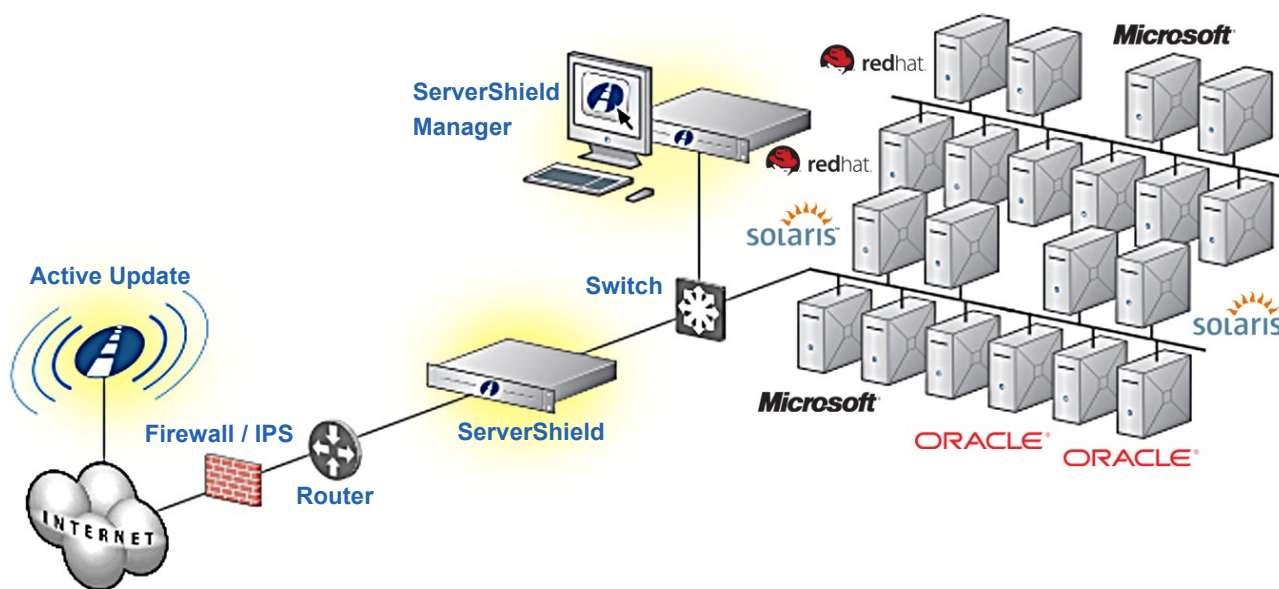
In summary, current security products fall short when it comes to protecting enterprise servers, databases and applications in an operationally viable fashion.

Blue Lane System Overview:

The Blue Lane system provides security and application control for virtual and physical server farms, including OS, database and application services.

The Blue Lane system consists of three key components:

1. **ServerShield** network appliance,
2. **ServerShield** Manager appliance
3. **ActiveUpdate** service for vulnerability content updates.



ServerShield Appliance

The ServerShield appliance is a scalable, high-performance network appliance that detects vulnerabilities present in client server protocols and protects the server from exploitation of these vulnerabilities, according to user-defined protection profiles.

The appliance resides at the aggregation point in front of server farms and operates as a transparent GbE (10/100/1000) bridge with no accessible IP on its working network interfaces. Initial deployment is straightforward, and entails setting up a management IP for communication with the ServerShield Manager.

On initial deployment, the ServerShield discovers all IPs behind it, the OSes that run on those IPs, open ports, what services run on those ports, and the version/patch level of those services. The user is presented with a point-and-click interface to turn on protection for the servers / services they wish to protect. Because of the accurate detection and protection system, the system now ensures that servers are protected. No additional tuning is required.

Fault tolerance is built into the appliance, and includes hot-swappable power, fans and automatic bypass-on-failure Ethernet interfaces. Appliances can be configured to fail open (meaning traffic would continue to pass if power is lost) and they can also be clustered in a high availability mode to ensure protection in the event of an appliance failure.

Along with the working ports, the appliance also provides an out-of-band management port to connect with the Enterprise Manager, and a scanning port to discover servers, applications and services behind the appliance. An intuitive command line interface is provided by the Manager and the appliance which can be accessed either remotely via SSH or directly from the DB-9 console port provided on the device. A single appliance can provide protection for hundreds of servers, which meets the scalability required by most critical server deployments.

Latency is less than a router hop – typical packet latency is around 500 microseconds.

The G/450 is primarily recommended for large network deployments where redundancy and throughput are the priority and can handle hundreds of servers with one appliance.

The G/250 is primarily recommended for smaller network deployments such as remote offices.

ServerShield Manager

The ServerShield Enterprise Manager is a dedicated appliance that provides configuration, management, auditing and reporting services for the ServerShield System.

A single Manager appliance is used to manage ServerShields locally in an enterprise or anywhere over the Internet. The Manager holds all the configuration data for each appliance it manages, including user, server and protection profiles. It also contains the working data-store that holds system and vulnerability history for the entire system. Reporting and monitoring of the deployed appliances is done using the Manager reporting infrastructure, which can create, display and export reports in multiple formats for use in tracking and decision-making processes surrounding the server security deployment process. The Manager also acts as the single point of contact and distribution point for vulnerability content updates and system software updates distributed by Blue Lane's ActiveUpdate service.

The Manager provides a rich set of reports, including executive overview, vulnerability events, vulnerability risk reports, applied and not-applied patches, and system events. This information can be viewed natively within the management interface or forwarded via email, SNMP, or syslog to other management consoles.

ServerShield ActiveUpdate Service

ServerShield ActiveUpdate is a subscription-based service that delivers vulnerability content updates to the ServerShield System. The ActiveUpdate service is hosted in a secure, redundant co-location facility in order to provide high availability to the overall System. The ActiveUpdate server communicates with the Manager to distribute ActiveFix updates in real time as they are made available to the ActiveUpdate service. These updates can be pulled from the ActiveUpdate service either automatically or manually depending on the configuration. Once the new ActiveFix resides on the local Manager, the ActiveFix can be distributed to the appropriate Gateway automatically, depending on the profile configuration.

Blue Lane covers a wide variety of threats including “zero-day” vulnerabilities and known vulnerabilities. Critical ActiveFixes are typically released within 24 hours of discovery, and Blue Lane is a member of various research groups that discover vulnerabilities. Blue Lane also releases ActiveUpdates that are mapped one-to-one with the corresponding vendor patch. This allows the Blue Lane ActiveFixes to be used as a compensating control to reduce patch cycles or for systems that are difficult or unable to be patched.

In addition to the broadest coverage of “patched” vulnerability protection and zero-day protection, Blue Lane provides additional policy coverage within the ActiveUpdates to maximize server protection. Some of these policies include the ability to white list servers to only access specific URLs, SQL injection blocking, Cross-Site Scripting Blocking, Database Policies to prevent user escalation of privileges, and many other protections.

Vulnerability fixes and policies for known and zero day vulnerabilities are provided for major enterprise servers, databases and applications, per the following chart.

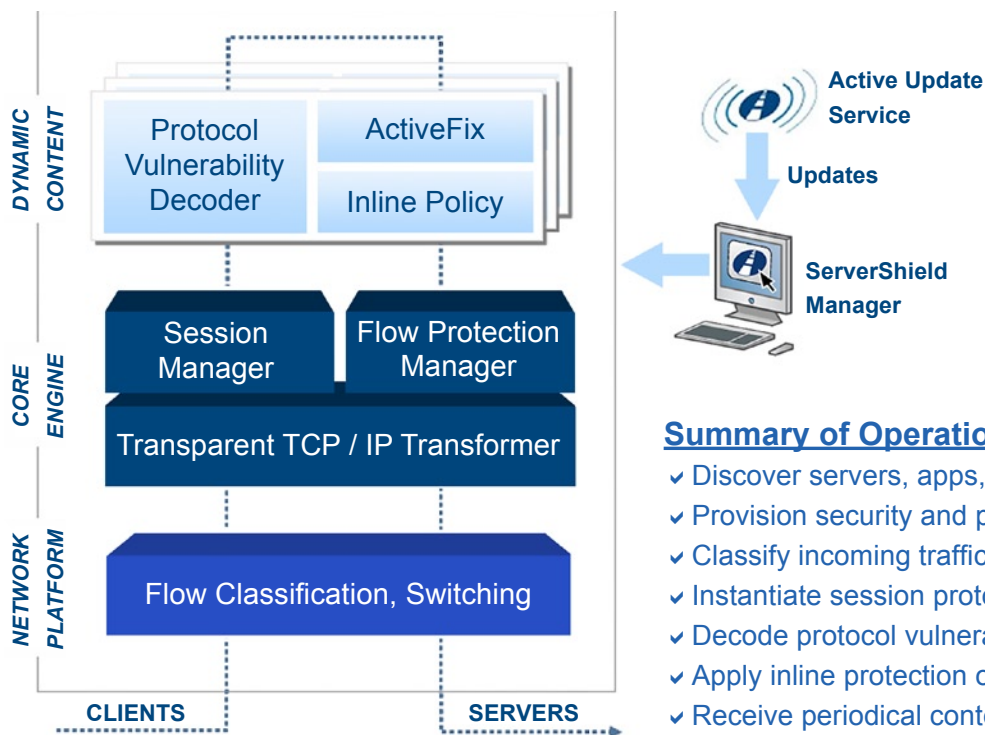
Note that coverage is constantly updated. Please check with Blue Lane for latest coverage information.

OS, Network	Databases	Email	Web	Open Source
Microsoft Windows NT 2000, 2003 solaris OS 7, 8, 9, 10 redhat. EL 2, 3, 4 Novell suse 8, 9, 10 IBM AIX VMware Infrastructure	Microsoft MS SQL 2000 SP0-SP3a MS SQL 2005 ORACLE DBMS 7, 8, 9, 10g AppServer	Microsoft Exchange 5.0,5.5,2003 Courier IMAP 	Microsoft IIS 1.0-6.0 iPlanet e-commerce solutions 6.0/1 SP2, 4, 5 Apache Web Sever 1.3-2.1.3	 Washington University FTP
Covered on the Following Platforms 				

Blue Lane Technology Overview:

Blue Lane's patented architectural approach is significantly different from current signature processing systems; it is based on the following building blocks:

1. In lieu of signature processing, layer 7 protocol decoders are used to detect vulnerabilities.
2. Instead of blocking via connection resets, app-specific corrective action is used.
3. Complete asset discovery and full session state ensure complete context.
4. Dynamic upload & instantiation of content enable instant security without reboots.
5. Protocol-specific inbound/outbound policies provide pro-active server protection.
6. General X86 software, no specialized hardware e.g. regular expression processors are used. This enables re-targeting to latest hardware, virtual environments, and multi-core architectures.



Summary of Operation

- ✓ Discover servers, apps, ports
- ✓ Provision security and policy
- ✓ Classify incoming traffic
- ✓ Instantiate session protocol handler
- ✓ Decode protocol vulnerability
- ✓ Apply inline protection or policy
- ✓ Receive periodical content updates

ServerShield – Summary of Operation

Blue Lane products are deployed inline to intercept client server traffic. Immediately upon deployment, the system discovers servers, their respective operating systems and open ports, the services running on those ports, and the revision/patch levels of these services. The user is presented with this inventory, and through a point-and-click interface can turn on protection on a server, subnet, application or vulnerability basis. The system is now ready for operation.

As traffic flows pass through the shield, based on the inventory information, the respective protocol handler is instantiated. The handler decodes the protocol, including the ability to handle layer 7 fragmentation, and detects vulnerabilities in the flow. Upon finding the vulnerability, the respective vulnerability fix is applied. The vulnerability fix uses the rich set of corrective actions provided by the flow protection engine

to protect against the vulnerability; options include sending client or server application errors, truncating overflows, fixing timing errors, modifying headers, etc. The net result is that the vulnerability is surgically removed from the stream, and harmless traffic is sent to the server. Note that no exploit searches are made; the underlying root cause vulnerabilities are detected and fixed instead.

ServerShields are managed by the Enterprise Manager; the manager polls the Blue Lane Update services on a daily basis, and downloads new vulnerability fixes, or new coverage protocols. New updates are automatically downloaded to the ServerShield or VirtualShield, or if the customer prefers, this can be done manually. Such new updates take immediate effect on new sessions that meet the protocol profile. No tuning is required.

ServerShield – Architecture

There are three critical layers to the architecture of the ServerShield appliance:

1. The network platform, including high-speed switching and flow classification
2. The core engine provides transparent TCP/IP transformation, session management and flow protection engine services
3. The dynamic content layer provides protocol-specific vulnerability decoders, and inline protection and policy

Each of these layers plays a critical part in managing, maintaining and executing the server protection functionality of the ServerShield System.

1. Network Platform

The Network Platform layer provides high-speed layer 2 switching and flow classification functionality. Client-side traffic comes in on the “Unprotected” port, and leaves for the server on the “Protected” port. Incoming traffic is quickly classified as needing protection or not, based on configuration profiles. If the traffic does not require protection, it is immediately switched to the protected port, bypassing the higher layers.

For protected traffic, new sessions are immediately identified and classified, based on destination IP and port, and mapped against the server information table. This results in the appropriate dynamic protocol handler being instantiated to decode this particular flow. Traffic for existing sessions is quickly dispatched to the respective decoder that was instantiated earlier.

This layer also provides fail-open or fail-close bypass capability in the event of hardware or power failure.

2. Core Engine

The core engine consists of three major functional areas:

- the session manager
- flow protection engine
- transparent transport proxy

The session manager provides application-level, end-point awareness to ensure that only relevant transactions are monitored and introduce minimal latency. It maintains complete context for every running session through the system. It is initially responsible for scanning the network to determine all servers behind the appliance, what operating systems run on those servers, their respective open ports, and the services running on the ports, including the revision/patch level. In addition, a continuous scanning mode keeps the server information table up to date. The session manager instantiates appropriate dynamic protocol handler to handle new sessions. For existing sessions, packet pointers are handed off to the respective protocol handler and full session context is maintained. Note that zero copies are made of the packets, as they get handed off to the protocol handlers, resulting in high-speed operation and low latency.

The flow protection engine provides a rich set of corrective actions to the dynamic protocol handlers and their respective inline protection and policy modules. Actions include the ability to intervene at any point within a protocol to truncate overflow data within a string, replace specific characters, convert the encoding of data, insert application layer errors to servers and/or clients. These actions, when invoked, result in high-speed pointer manipulation and reconciliation, working closely with the transport layer. The deep session context and precise, deterministic actions result in low latency (less than 500 micro seconds) and surgical removal of the vulnerability, with no business disruption.

The transparent transport proxy provides the ability to correct vulnerable traffic inline, within the application protocol, while preserving the connection between client and server. This layer maintains all the house-keeping required to preserve TCP state between the client and the server, including TCP sequence number and window size reconciliation. Additionally, it provides security by monitoring flows inline without utilizing an IP or MAC address so that the ServerShield System is invisible to both client and server.

3. Dynamic Content

This layer provides all the vulnerability specific handling that is required to accurately detect, and deterministically remove the vulnerability from, or implement a policy in, the client server protocol.

For each area of coverage, the ServerShield maintains an updated set of protocol handlers, and their associated ActiveFixes and inline policies.

Each protocol handler implements the complete protocol state machine logic required to accurately reach the context of the respective vulnerability. To ensure accuracy, and to avert IPS bypass techniques, decoding includes layer 7 re-assembly as required. For high performance, the protocol handling is exception based, around the context of the vulnerability.

Each vulnerability is mitigated with an ActiveFix. The ActiveFix is complete stateful logic, that lets the associated protocol handler know how to precisely detect the vulnerability, and upon triggering of the vulnerability, has logic to surgically mitigate the vulnerability, by calling upon the rich set of corrective actions available from the Flow Protection Engine.

In addition, for each supported protocol, a set of inline policies are available. These policies are application/protocol specific, and are based on complete knowledge of the user, operation, resource and client/server IP and port per flow. Policies are configurable for both inbound (client to server) and outbound traffic. Examples of powerful policies include: “Deny rdp access to a given server farm”, “Deny insert, delete, select * operations to a set of databases or tables for a given source IP range”, “Alert sql injection for a given set of form fields in a given url”, “Deny all outbound rsh connections”. These policies are



















configurable by users to put in place proactive security to limit protocol access, contain malware propagation, or shield against web coding vulnerabilities.

In place of static signatures that are uploaded by IDS/IPS technologies, Blue Lane uses a high level, hardened “Vulnerability Description Language” (VDL) to upload new protocol handlers, ActiveFixes, and inline policies. New updates can be instantly effected on new sessions, without requiring system upgrades.

The benefits of this approach are compelling:

- Deployable instantly across hundreds of servers to provide immediate protection across even the largest server deployments with zero footprint on the server.
- Promotes uptime and business continuity by performing vulnerability removal inline in an application-friendly manner, without touching servers.
- Provides protection against IPS evasion techniques like exploit morphing, higher layer fragmentation or segmentation, etc.
- High performance because of the precise, exception-based detection mechanism, where processing only proceeds to higher layers if warranted.
- Scales well, and is not subject to performance degradation due to signature explosion.

Comparing Blue Lane against current IPS technologies

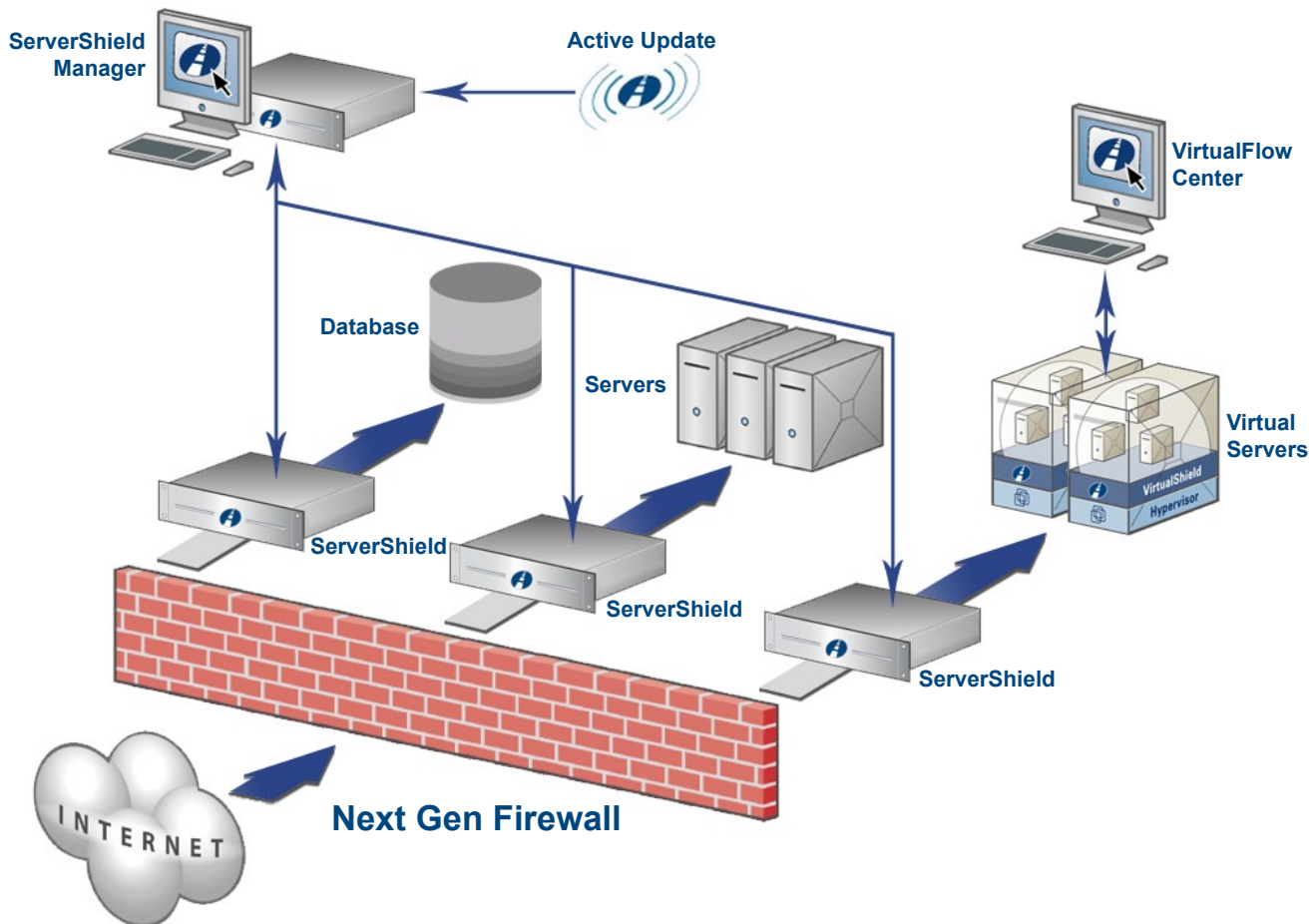
Next Gen IPS Requirements	Current IPS	Blue Lane
Server, database, app coverage		
Accurate vulnerability detection		
Non-disruptive protection		
Resilience to IPS evasion		
Virtualization readiness		
Application control policy		
Operational ease (tuning, etc)		
	Current IPS	NG Firewall
Port scans, DDOS, AV		
Anomaly detection		

Defense-in-depth approach to secure the data center

Blue Lane's next generation IPS technology complements perimeter firewall technology to provide comprehensive protection for servers, databases and applications.

Secure Physical Servers and Databases

Secure Virtual Hosts and VMs



Common use cases for Blue Lane products

Compliance, effective server/database security and virtualization are driving the deployment of Blue Lane products. Following are specific areas where Blue Lane's ServerShield and VirtualShield provide compelling benefits to customers.

- Microsoft environments
 - ◆ Secure immediately, buying time to patch on customer schedule
 - ◆ Secure hard-to-patch servers due to tech, ops, resource constraints
- Oracle environments
 - ◆ Secure and police vulnerable databases while database attacks increase
 - ◆ Audit user operations on database tables & fields; provide policies

- VMware environments
 - ◆ Monitor, secure and control ESX hosts and guest VMs
 - ◆ Provide inter-VM and intra-rack partitioning, protection and visibility
- Web services
 - ◆ Meet compliance requirements (PCI-DSS) for internet facing web services.
 - ◆ Shield web coding vulnerabilities i.e. form field, SQL injection, XSS vulnerabilities
- Specialized high-availability systems
 - ◆ Secure critical high-availability medical devices, manufacturing, FDA validated systems, and other mission critical systems where changes cannot be easily made to the system.

Summary

The Blue Lane ServerShield is a unique solution that allows IT departments to secure servers without compromising uptime. The broad and accurate coverage, as well as the ability to enable the system in full protect mode, provides true server protection from remote threats for all servers and systems in the environment, including those that were previously difficult or impossible to secure. Today with ServerShield and VirtualShield, IT organizations can feel confident that their critical servers, database and applications are secure, and regain control of their operational processes.

Appendix

Following examples showcase the Blue Lane difference. For each showcase example, four areas are covered.

- A. Description of exploit/vulnerability
- B. How current generation IPSes fall short
- C. Blue Lane Vulnerability Detection logic
- D. Blue Lane Vulnerability Protection mechanism

Oracle CPUJuly07 DB02

Vulnerability:

- Stored procedure : dbms_repcat.alter_master_reobject (sname, oname, type)
- Each parameter is of type string.
- 3rd parameter (type) causes buffer overflow if length is more than 1K.
- Fixed by Oracle in one of its CPU (cpu-xxx).

IPS treatment:

Current IPSes “protect” by downloading the following signature:

```
dbms_repcat.alter_master_reobject ((\s* (\x27[\^x27]* | \x22[\^x22]+\x22) \s* ,) {2} ( (\x27[\^x27]{1000,}) | (\x22[\^x22]{1000,}))
```

Translated into english: “look for 2 strings, followed by a string of length > 1000”

Why the IPS protection falls short of meeting the security objective:

This signature is very easy to bypass. Secondly, the protection logic is a simple connection reset, causing db connection pooling or the application to break.

For example, two signature bypass techniques are shown here:

Bypass technique #1: Indirect parameter

```
Declare X ;  
X := “exploit.....< length more than 1K > ”;  
dbms_repcat.alter_master_reobject ( “strA”, “strB”, X);
```

Bypass technique #2: Name => Value style parameter

```
dbms_repcat.alter_master_reobject(sname =>‘strA’, type =>‘<exploit>’,oname => ‘strB’);
```

Blue Lane treatment:

Blue Lane's Vulnerability Detection logic is based on the following:

- An Oracle State machine
- Complete SQL Grammar Parser
- SQL decoded just like an Oracle server would do
- Element tree (next slide) created for SQL statements
- Blue Lane decoder detects the vulnerability

Blue Lane's Vulnerability Protection logic:

- If vulnerable condition is met, a "RAISE APPLICATION ERROR" message is sent to the server, resulting in the server sending an error to the client

RESULT

- Accurate vulnerability detection
- Bypass techniques highlighted above, do not work against Blue Lane
- No impact to any data; method allows graceful close
- No effect on any other application, connection pools, etc

MS05-027

This was also known as SMB max buff vulnerability. It is a very good example of an involved vulnerability where information is drawn from different parts of the protocol which can be apart from each other by a huge amount of data or temporal difference. Here the unpatched server when handling the SMB Trans command could possibly try to write too much data into a kernel buffer when sending its reply causing heap corruption and a way for exploitation.

This example highlights the following important points:

- The detection of the vulnerability involves decoding a lot of different pieces of a complex protocol (SMB).
- All the information that is needed can be separated from each other by a long time interval or large amount of network traffic (meaning all intermediate pieces need to be decoded correctly).
- The logic that determines when the deviation from the unpatched server will occur is complex.
- Blue Lane has the ability to implement the exact logic on the network.
- Blue Lane can mitigate the problem without disrupting the application.

Details:

- The size of the buffer (for sending the reply) that Microsoft's implementation uses is a fixed size buffer (0x1104).
- The client is able to specify the size of it's receive buffer in the max-buff field of the SessionSetup

request. This is done in the initial capability exchange. This can be bigger than the server's send-buffer.

- In the trans request, the client also sends a max-data field, which tells the server the maximum amount that the client wants to receive for that particular request. This request can come much later (for eg, a day later or a multiple Gigs of data has been transferred on that SMB session). The logic that the server uses to determine the actual size it can write for that SMB request is more involved and described a little down.
- The bug is that if the client sets max-buff higher than the size of the buffer the server actually uses, and also sends max-data higher, and the server actually writes more data than will fit in the buffer, an overflow occurs in the kernel heap.
- The problem occurs in a networking layer which is used by a lot of modules like MSRPC, MS SQL server, Content Indexing Service (CIS) etc. and therefore can manifest itself in a lot of different applications. In fact it is possible to cause the problem to occur in scenarios where traffic is not malicious.
- FIX – The patch fixes the problem by limiting the used max-buff size to the size of the server's buffer (change in srv.sys).

The actual logic on the server which determines the space that is really available to write – the easiest way to express this is using pseudocode!

```
// First, when we see the SMB session request
// The max-buffer should be truncated down to a multiple of 4.
max_buff = (value from the network);
max_buff = (max_buff & ~3);

// When we see the SMB Trans request // A macro to round up to multiple of four (utility function).
#define rd4(x) (((x)+3) & ~3)
max_data = (value from the network);
max_setup = (value from the network);
max_param = (value from the network);

// Now calculate the effective max data
if (is_rpc) {
    effective_max_data = 0x10b8; // due to the way the RPC Bind request is processed
} else {
    effective_max_data = rd4 (max_data);
}

amt_needed = (effective_max_data + rd4 (max_setup*2 + 5)+ rd4 (max_param) + 36);

if ((amt_needed <= max_buff) && (amt_needed > 0x1104)) {
    // Patch will kick in, we need to fix
    set max_param to 0, max_setup to 0
    if (! is_rpc) set max_data to 0x1104 - 36;
} else {
    // The unpatched server handles it correctly
}
```

IPS treatment:

The above detection logic cannot be patterned using regular expression signatures.

Blue Lane treatment:

Blue Lane's ActiveFix for MS05-027 precisely captures the above-stated logic, and upon detection of the vulnerability, removes it, without disruption.

MS06-019**Vulnerability:**

The vulnerability is in the processing of emails, specifically calendar attachments inside emails, by a Microsoft Exchange server. The calendar attachment has several elements. The problem is a buffer overflow in the way the Exchange server processes one of these elements, the X-MICROSOFT-CDO-MODPROPS. This element contains different properties of a calendar event including date, summary etc. The element can appear multiple times in the attachment.

- Server allocates memory on seeing X-MICROSOFT-CDO-MODPROPS element.
- The allocated memory size is limited to number of properties in this instance.
- Subsequent instances of this element re-use the same memory. If number of properties is larger then it causes buffer overflow, and the service crashes.

Microsoft Fix in MS06-019:

Microsoft patched the software to reallocate more memory if a subsequent X-MICROSOFT-CDO-MODPROPS command has more properties than prior instances.

IPS treatment:

One of the better IPS's does the following:

- Basically runs pattern matching/regex on some elements that it creates
- The decoding done is very basic.
- Have a pattern that looks for presence of text/calendar in the smtp-header-line
- Check for one property in X-MICROSOFT-CDO-MODPROPS
- Check for more than one property (presence of ',') in another line
- Reset connection if above is seen.

Why the IPS protection falls short of meeting the security objective:

This signature is very easy to bypass.

```
BEGIN:VCALENDAR
BEGIN:VEVENT
X-MICROSOFT-CDO-MODPROPS:dtstamp, dtstamp
DTSTAMP:
END:VEVENT
BEGIN:VEVENT
X-MICROSOFT-CDO-MODPROPS:summary,summary,summary,summary,summary
END:VEVENT
END:VCALENDAR
```

The above email bypasses the IPS and crashes the server !!

Secondly, the protection logic is a simple connection reset. This means a exploitative email, if detected, in the best case would cause the session between two Exchange relay servers to be reset. This means a single email can cause head of line blocking till the Exchange server decides to take the top email and move it to a separate queue.

A second IPS takes a more simplistic approach!

- Absolutely no decoding
- Plain pattern matching on the TCP stream
- Signatures are updated over time to reflect each new bypass!
- Even the following (non email!) traffic will raise an alert. No headers are present.

```
Foo
BEGIN:VCALENDAR
X-MICROSOFT-CDO-MODPROPS:dtstamp
DTSTAMP:
END:VEVENT
BEGIN:VEVENT
X-MICROSOFT-CDO-MODPROPS:summary,summary,summary,summary,summary
END:VEVENT
END:VCALENDAR
```

Why can't an IPS do better:

- Hard to decode more. It requires a system level upgrade.
- Decoding is done irrespective of whether this traffic is sendmail bound.
- Decoding is done irrespective of whether the server is patched (static decoders !!!) – bad performance hit
- Doing complex logic using pattern matching is not possible.

Blue Lane treatment:

Blue Lane's Vulnerability Detection logic is based on the following:

- An Exchange State machine
- Complete SMTP Grammar Parser
- Element tree created for SMTP statements
- Blue Lane decoder detects the vulnerability

Blue Lane Vulnerability Detection logic:

- Use the same logic that the server uses to find the number of properties for a X-MICROSOFT-CDO-MODPROPS.
- Determine the case when memory will be initialized.
- If it finds the case where a buffer overflow occurs, remove the bad VEVENT. No known legitimate email client generates emails so this operation disarms the bad email while not dropping the session between two Exchange relay servers.

RESULT

- Accurate vulnerability detection
- Bypass techniques highlighted above, do not work against Blue Lane
- No impact to any data; method allows graceful continuance

About Blue Lane Technologies

Headquartered in Cupertino, CA., Blue Lane Technologies provides solutions that secure virtual and physical data centers with zero footprint, zero downtime and zero tuning. Since January 2007 Blue Lane has won Best of Interop in security as well as InfoWorld's Technology of the Year, also in security. In 2007 Blue Lane also won a Best of VMworld Finalist award in data protection. Blue Lane has won numerous other awards, including the AO 100 Top Private Company Award for 2006 and 2007.

Blue Lane Technologies is privately held. It has alliances with Microsoft, VMware, Oracle, Red Hat and Qualys. Customers include Davidson Hotels, WesCorp, The Metropolitan Transportation Authority, Wyeth, service providers Ornis and Artful and some of the world's top consumer, healthcare, financial, government and technology organizations.

To find out more about Blue Lane and its products, please visit www.bluelane.com.

Contact Information:

Email: info@bluelane.com

Blue Lane Technologies Inc.
10450 Bubb Rd
Cupertino, CA 95014

Phone: 408-200-5200
Fax: 408-200-5299