



## **Normalizing Security Data Streams for Queries and Analysis**

**February 2002**

## Executive Summary

Most organizations need to correlate vast amounts of system and business data in order to determine their level of security. The Normalizer product helps them to take full advantage of the security information they already have; it complements existing security and system software without requiring a proprietary agent to be installed. It collects copies of system and application logs using a wide variety of existing mechanisms and then processes the disparate security data to produce a single, standardized output. The resulting information can be queried for simple and complex correlations, summarized in “real language” reports for every level of management, and fed into other security systems. The Normalizer enables an enterprise to obtain a unified view of all its security information.

## Introduction

Security information is typically difficult for an enterprise to understand, process and use because it comes from widely distributed and isolated sources that employ varied platforms, formats and jargons. Some of this information turns out to be valuable only after it is combined with other data. Especially in very large networks, much of it goes unnoticed simply because it is more than any reader can handle. Most security software offerings on the market today prefer to generate their own data using proprietary agents, rather than using the information already on the system; this adds to the confusion rather than relieving it. Moreover, no offerings exist that integrate both internal information system data with business-related information.

Software offerings in the enterprise security space either focus on control of client platforms or are tightly focused on a single platform or system. Deploying a new product on a large scale can be very difficult: system administrators worry about the impact on existing systems; control issues emerge between groups; there is often no budget allocated to the time and effort of testing, piloting and rolling out new software. These reactions - both hesitation to adopt new controls and fear of business impact - are compounded by the universal need that such mechanisms have to install software on the target platform.

For some time, regulations have required many organizations to have a level of knowledge of their information infrastructure that current product offerings do not enable. These regulations range from the European Union Data Directive concerning data privacy to banking secrecy laws in countries such as Singapore and Switzerland. The U.S. is no exception: for example, Section 501 of the Gramm-Leach-Bliley Act (“G-L-B Act”) provides that financial institutions must ensure the security and confidentiality of customer information. The Act requires financial institutions to “coordinate all

## Normalizing Security Data Streams for Queries and Analysis

elements of its information security program.” Dispersed and uncoordinated security information does not comply with these regulations.\*

In short, companies know that they need to understand the state of security and the significant impact that it could have on their business operations. In order to reach an accurate profile of that overall state, they should be able to manage the consolidated security information from their firewalls, intrusion detection systems, access control lists, anti-virus software, vulnerability scanners, mail transfer agents, application logs, routers, servers, and clients. The security information management system (SIM) must be accessible not only to the security staff, but also to upper management, including the CIO and CEO. There have been no current products that provide that combined view and knowledge.

### TABLE OF CONTENTS

Executive Summary .....	2
Introduction.....	2
Perfectway’s Normalizer.....	4
What the Normalizer is not .....	5
Source Input Formats.....	6
Collection.....	6
Processing .....	7
Sanitizing Data .....	9
Securing and Archiving Data .....	10
Using the Output .....	10
Asking Basic Questions .....	11
Simple and Complex Correlations .....	12
Tailoring the Reports .....	13
Displaying the Data.....	14
Summary.....	14
Reading List and Other Resources.....	15
About Perfectway.....	15

---

\* “Where the elements of the program are dispersed throughout the institution, management should be aware of these elements and their locations. If they are not maintained on a consolidated basis, management should have an ability to retrieve the current documents from those responsible for the overall coordination and ongoing evaluation of the program.” 66 Fed. Reg. 8619 (Feb. 2, 2001)

## Perfectway's Normalizer

The Normalizer is a self-contained appliance that sits on a network and receives copies of all other system and application logs, using whatever native transmission methods are both convenient and secure. These logs are then processed to produce a single, standardized output. The Normalized output is then subjected to specific and general queries in order to highlight important security events that otherwise might go unnoticed. From a flow of differing logs, an organization can track the trail of users across workstations, servers, public Internet gateways, and in-house applications. The evidence of these trails does not depend upon any single vendor's operating system, application or protocol.

The Normalizer provides customers with a solution to the problem of scattered and uncoordinated security information getting "lost in the shuffle". It is designed so that the security information most important to each customer can be understood both by information technology professionals and non-technically oriented senior executives of the enterprise.

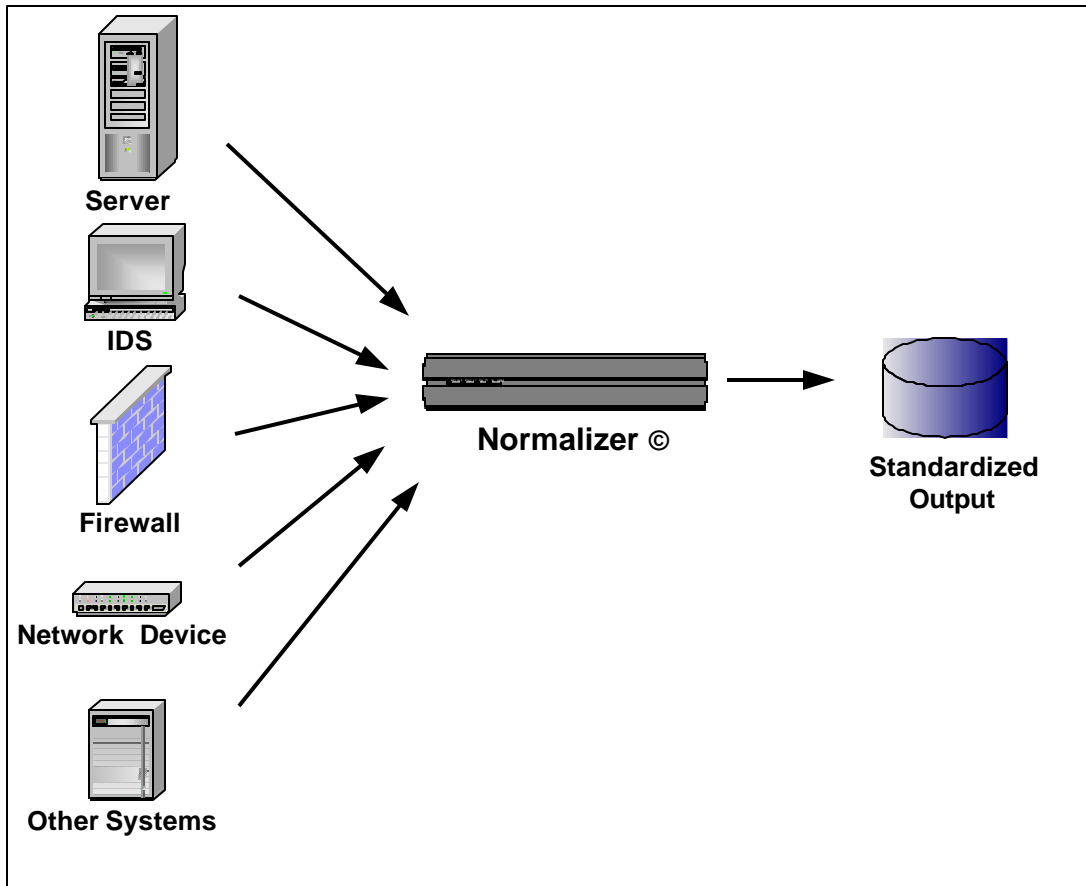


Figure 1

## Normalizing Security Data Streams for Queries and Analysis

This process, illustrated in Figure 1, serves the important function of integrating an organization's disparate security information into one easily readable format. This standardized output is critical for information technology professionals to understand the state of their systems' security. However, to produce a readily understandable picture of an organization's security and business status, particularly for the non-Information Technology professional (i.e., senior managers and executives who work outside the IT area), the process needs to go to the next step – querying the standardized output for significant events.

For example, from the Normalizer we can send email to the head equities trader at a financial institution, notifying that one of the subordinate traders has emailed a large spreadsheet to a competitive firm after hours. We can send a message to an existing network management station (such as HP OpenView), alerting a network operator that someone on the public Internet first scanned a firewall; then logged onto that firewall from the same source on the Internet; and had accessed a vital internal database from that same firewall. In this manner, the Normalizer complements rather than competes with the organization's existing network management and security systems. By neither placing client code on customers' machines nor generating a new application that a customer would need to monitor, we minimize the hurdles for customers to adopt our technologies. Perfectway's Normalizer uses only native log data and delivery mechanisms; therefore deployment of the Normalizer does not impact business as usual, nor does it threaten existing power and control structures in the organization.

By centralizing, standardizing and correlating diverse logs, we can provide a singular, comprehensive and unified view of the entirety of an enterprise's security-related information.

### ***What the Normalizer is not***

The Normalizer is not an intrusion detection system. It can add data to, or process data from an existing IDS. It focuses on standardizing various different streams of data, rather than generating a new one of its own.

The Normalizer is not a security or network management product. It does not try to enter or control anything else. Because the Normalizer does not require software to be placed upon data source machines in order to receive data flow, it is easy to integrate the Normalizer effectively into large networks. The output from the Normalizer process can interface either directly with the customers' existing reporting mechanisms (so that it is not necessary for the customer to introduce a new front end or console), or be queried by the customer using industry standard query tools.

The Normalizer is not a Web analysis tool. It can be used to normalize Web server log files along with many other types, but it does not specialize in analyzing Web statistics in the way that other tools do (such as WebTrends' Log Analyzer).

## **Source Input Formats**

The Normalizer works on raw files in different content formats from many sources. Unix's syslog, for example, contains not only its own operating system log messages, but can also receive log messages written to it by other infrastructure and applications running on the same host, such as email, databases, NIS, and proprietary software (such as a trading application). All of these collected logs can be processed together by the Normalizer.

Other formats understood by the Normalizer include SNMP traps, raw NT event logfiles, CSV formats, various firewall appliances such as Sonicwall and Watchguard, Apache's Common Log Format, and more.

Not only log files can be processed through the Normalizer: all sorts of business information can be standardized and added to the system data to create a much richer picture of the company's activities. Employee lists, spreadsheet contents, names of competitors, market data feeds, vendor lists, online chat transcripts, and other sources can be plumbed for valuable connections to other events and data.

## **Collection**

The Normalizer can receive the inputs in various ways. Some of the most common transmission methods include `syslog`, `SNMP`, `ftp`, `ssh/scp/sftp`, `rdist` ("plain" or over `ssh`), `stunnel`, `SMB` or `NFS` file sharing, and even `http` or `https POST` (although we do not necessarily recommend the last two). Security requirements will dictate whether the Normalizer passively receives a push or executes a pull to obtain the logs. For example, a firewall might send its application, packet filter and configuration files to the Normalizer using `rdist` over `ssh`; the contents of NT event logs might be forwarded as `SNMP` traps. This flexibility allows the Normalizer to use whatever facilities already exist, rather than forcing a new one to be installed.

## Processing

The Normalizer then processes all input data and turns it into a uniform format. Here are some examples of raw logs from various systems:

```
1.2.3.4 - - [25/Apr/2001:13:27:18 -0500] "GET / HTTP/1.0" 403 198
4.3.2.1 - - [25/Apr/2001:13:28:32 -0500] "GET /robots.txt HTTP/1.0"
404 204

[Wed Apr 25 13:27:18 2001] [error] [client 5.6.7.8] Directory index forbidden by rule: /home/httpd/www.emus-r-us.com-80/html/
[Wed Apr 25 13:28:32 2001] [error] [client 9.1.2.3] File does not exist: /home/httpd/www.emus-r-us.com-80/html/robots.txt

01/30/2001-18:24:41:8.2.3.4UDP pkt from 8.2.3.4/137 to 1.2.3.4/137 dropped
01/30/2001-18:24:41:4.9.3.2UDP pkt from 4.9.3.2/137 to 1.2.3.4/137 dropped

***** BEGIN RECEIVED V1 TRAP *****
** DATE: Mon Jul 5 03:00:13 1999
5.4.3.2: Enterprise Specific Trap (1405) Uptime: 37 days, 2:18:47
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.1 ->
INTEGER: 109
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.2 ->
OCTET STRING- (ascii): Error
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.3 ->
OCTET STRING- (ascii): Application
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.4 ->
OCTET STRING- (ascii): ActiveNames
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.5 ->
OCTET STRING- (ascii): testclient
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.6 ->
OCTET STRING- (ascii): The following error occurred Could not start the ActiveNames core due to unknown error.
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.7 ->
OCTET STRING- (hex):
***** END OF RECEIVED V1 TRAP *****

***** BEGIN RECEIVED V1 TRAP *****
** DATE: Mon Jul 5 03:00:17 1999
9.8.7.6: Enterprise Specific Trap (1403) Uptime: 116 days, 15:28:40
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.1 ->
INTEGER: 8007
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.2 ->
OCTET STRING- (ascii): Warning
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.3 ->
OCTET STRING- (ascii): System
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.4 ->
OCTET STRING- (ascii): NwRdr
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.5 ->
OCTET STRING- (ascii): anotherclient
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.6 ->
OCTET STRING- (ascii): The Microsoft Client Service for NetWare redirector has timed out one or more requests to
PWAY_NJ_CS_RESTORE.
Name: .iso.org.dod.internet.private.enterprises.shrdlu.systems.os.winNT.1.1.7 ->
OCTET STRING- (hex):
***** END OF RECEIVED V1 TRAP *****
```

## Normalizing Security Data Streams for Queries and Analysis

The same log information is normalized and reformatted here into a tab-delimited output:

```
agent_format=apache event_host=1.2.3.4 event_message=web request event_proto=HTTP/1.0
event_status=failure
origin_date=2001-04-25 13:27:18 www_arg=/ www_op=GET
www_request=GET / HTTP/1.0 www_result=403 www_server=www.emus-r-us.com
www_size=198
agent_format=apache event_host=4.3.2.1 event_message=web request event_proto=HTTP/1.0
event_status=failure
origin_date=2001-04-25 13:28:32 www_arg=/robots.txt www_op=GET
www_request=GET /robots.txt HTTP/1.0 www_result=404
www_server=www.emus-r-us.com www_size=204

agent_format=apache event_host=1.2.3.4 event_message=apache
server error event_reason=Directory index forbidden by rule: /home/httpd/www.emus-r-us.com-80/html/
event_status=error
origin_date=2001-04-25 13:27:18 www_server=www.emus-r-us.com
agent_format=apache event_host=4.3.2.1 event_message=apache server error event_reason=File
does not exist:
/home/httpd/www.emus-r-us.com-80/html/robots.txt event_status=error origin_date=2001-04-25 13:28:32
www_server= www.emus-r-us.com

agent_format=flowpoint event_host=8.2.3.4
event_message=package filter event_severity=info event_status=success
origin_date=2001-01-30 18:24:41 origin_host=xo pf_action=drop pf_dstip=1.2.3.4 pf_dstport=137
pf_proto=UDP
pf_srcip=8.2.3.4 pf_srcport=137
agent_format=flowpoint event_host=4.9.3.2
event_message=package filter event_severity=info event_status=success
origin_date=2001-01-30 18:24:41 origin_host=xo pf_action=drop pf_dstip=1.2.3.4 pf_dstport=137
pf_proto=UDP
pf_srcip=4.9.3.2 pf_srcport=137

agent_format=snmpv1 agent_timestamp=1999-07-05 03:00:13
event_message=service start event_reason=unknown error
event_service=ActiveNames event_severity=notice event_status=failure
event_type=ActiveNames msg=The following error occurred Could not start the
ActiveNames core due to unknown error. nt_eventid=109
nt_severity=Error origin_host=testclient origin_ip=5.4.3.2
snmp_trapnr=1405 snmp_traptype=Enterprise Specific

agent_format=snmpv1 agent_timestamp=1999-07-05 03:00:17
event_host=PWAY_NJ_CS_RESTORE event_message=timeout event_service=NwRdr
event_severity=info event_status=success event_type=Netware
Redirector msg=The Microsoft Client Service for NetWare redirector has
timed out one or more requests to PWAY_NJ_CS_RESTORE. nt_eventid=8007
nt_severity=Warning origin_host=anotherclient
origin_ip=9.8.7.6 snmp_trapnr=1403
snmp_traptype=Enterprise Specific
```

## Normalizing Security Data Streams for Queries and Analysis

The same log information is normalized and reformatted here into SQL 92 Insert statement output. Note that the insert statements below are oriented toward flat table architecture. The Normalizer does not use flat table architecture internally, by reason of performance, and of simplicity and flexibility of query:

```
INSERT INTO normal
(agent_format,event_host,event_message,event_proto,event_status,origin_date,www_arg,www_op,www_requ
est,www_result,www_server,www_size,agent_format,event_host,event_message,event_proto,event_status,ori
gin_date,www_arg,www_op,www_request,www_result,www_server,www_size) VALUES
('apache','1.2.3.4','web request','HTTP/1.0','failure','2001-04-25 13:27:18','/','GET','GET /
HTTP/1.0','403','www.emus-r-us.com','198','apache','4.3.2.1','web request','HTTP/1.0','failure','2001-04-25
13:28:32','/robots.txt','GET','GET /robots.txt HTTP/1.0','404','www.emus-r-us.com','204');
```

```
INSERT INTO normal
(agent_format,event_host,event_message,event_reason,event_status,origin_date,www_server,agent_format,e
vent_host,event_message,event_reason,event_status,origin_date) VALUES ('apache','1.2.3.4','apache server
error','Directory index forbidden by rule: /home/httpd/www.emus-r-us.com-80/html/','error','2001-04-25
13:27:18','www.emus-r-us.com','apache','4.3.2.1','apache server error','File does not exist:
/home/httpd/www.emus-r-us.com-80/html/robots.txt','error','2001-04-25 13:28:32 www_server');
```

```
INSERT INTO normal
(agent_format,event_host,event_message,event_severity,event_status,origin_date,pf_action,pf_dstip,pf_dstpor
t,pf_proto,pf_srcip,pf_srcport,agent_format,event_host,event_message,event_severity,event_status,origin_date
,origin_host,pf_action,pf_dstip,pf_dstport,pf_proto,pf_srcip,pf_srcport) VALUES ('flowpoint','8.2.3.4','package
filter','info','success','2001-01-30 18:24:41
origin_host','drop','1.2.3.4','137','UDP','8.2.3.4','137','flowpoint','4.9.3.2','package filter','info','success','2001-01-
30 18:24:41','xo','drop','1.2.3.4','137','UDP','4.9.3.2','137');
```

```
INSERT INTO normal
(agent_format,agent_timestamp,event_message,event_reason,event_service,event_severity,event_status,even
t_type,msg,nt_eventid,nt_severity,origin_host,origin_ip,snmp_trapnr,snmp_traptype) VALUES ('snmpv1','2001
1999-07-05 03:00:13','service start','unknown error','ActiveNames','notice','failure','ActiveNames','The following
error occurred Could not start the ActiveNames core due to unknown
error.','109','Error','testclient','5.4.3.2','1405','Enterprise Specific');
```

```
INSERT INTO normal
(agent_format,agent_timestamp,event_host,event_message,event_service,event_severity,event_status,event_t
ype,msg,nt_eventid,nt_severity,origin_host,origin_ip,snmp_trapnr,snmp_traptype) VALUES ('snmpv1','2001
1999-07-05 03:00:17','PWAY_NJ_CS_RESTORE','timeout','NwRdr','info','success','Netware Redirector','The
Microsoft Client Service for NetWare redirector has timed out one or more requests to
PWAY_NJ_CS_RESTORE.','8007','Warning','anotherclient','9.8.7.6','1403','Enterprise Specific');
```

## Sanitizing Data

Not only can the Normalizer reformat logs, but it can sanitize them as well. Some specific content may be confidential to the company, but sometimes an outside vendor needs the log data to diagnose a problem. Login IDs, network IP addresses, hostnames, and application names can all be replaced quickly with generic entries.

## ***Securing and Archiving Data***

The Normalizer is designed to receive and process data as securely as possible. With the proper network placement and configuration, it can do the following:

- Get the data away from the “scene of the crime” as quickly as possible. When an attacker takes control of a machine, the first things to be erased are the log entries showing the break-in. If those entries have already been sent in real-time to another hardened machine, the attacker would have to spend valuable time getting into that one too (assuming s/he notices at all). Many organizations have a requirement to monitor their own system administrators; some of them have created a plausible separation of powers by having system logs sent to another server that the administrators can’t access.\* The Normalizer provides a safe haven for log data.
- Make sure the log server can’t be compromised by the same path it uses to receive logs. The Normalizer can either pull its logs from each target server, or use a transmission method that can’t be hijacked or otherwise exploited.
- Store the data in untouched, raw form somewhere for forensic investigations. The Normalizer saves a raw copy automatically before processing the data.

Once the data has moved off the Normalizer and into unsecured space, it is considered potentially unreliable. There will be many good reasons to pass the normalized data to others, and some display methods necessarily will be open access. But the reliability of that data will only be as good as the security surrounding it.

The Normalizer collection and storage process allows log data to be archived, in various forms and for a set duration. A certain amount of data is usually kept online and readily available, but older logs can be written to tape or CD for on- and off-site storage. Many institutions, such as financial ones, are required by law to keep archives for a certain length of time.

## ***Using the Output***

With a standard format for all log entries, regardless of source, the Normalizer can write the output as a flat text file. This allows the output to be used in a variety of ways: dumped into a spreadsheet, inserted into a database, forwarded to a Web server, queried by text searching utilities, and even passed as an additional input to other security monitoring software.

The Normalizer appliance contains its own database and set of basic queries, which can be used to gather vital information (see **Asking Basic Questions**, below).

---

\* This is often supplemented by the use of a “heartbeat” monitor to raise an alarm if a host suddenly stops transmitting data within a certain time window.

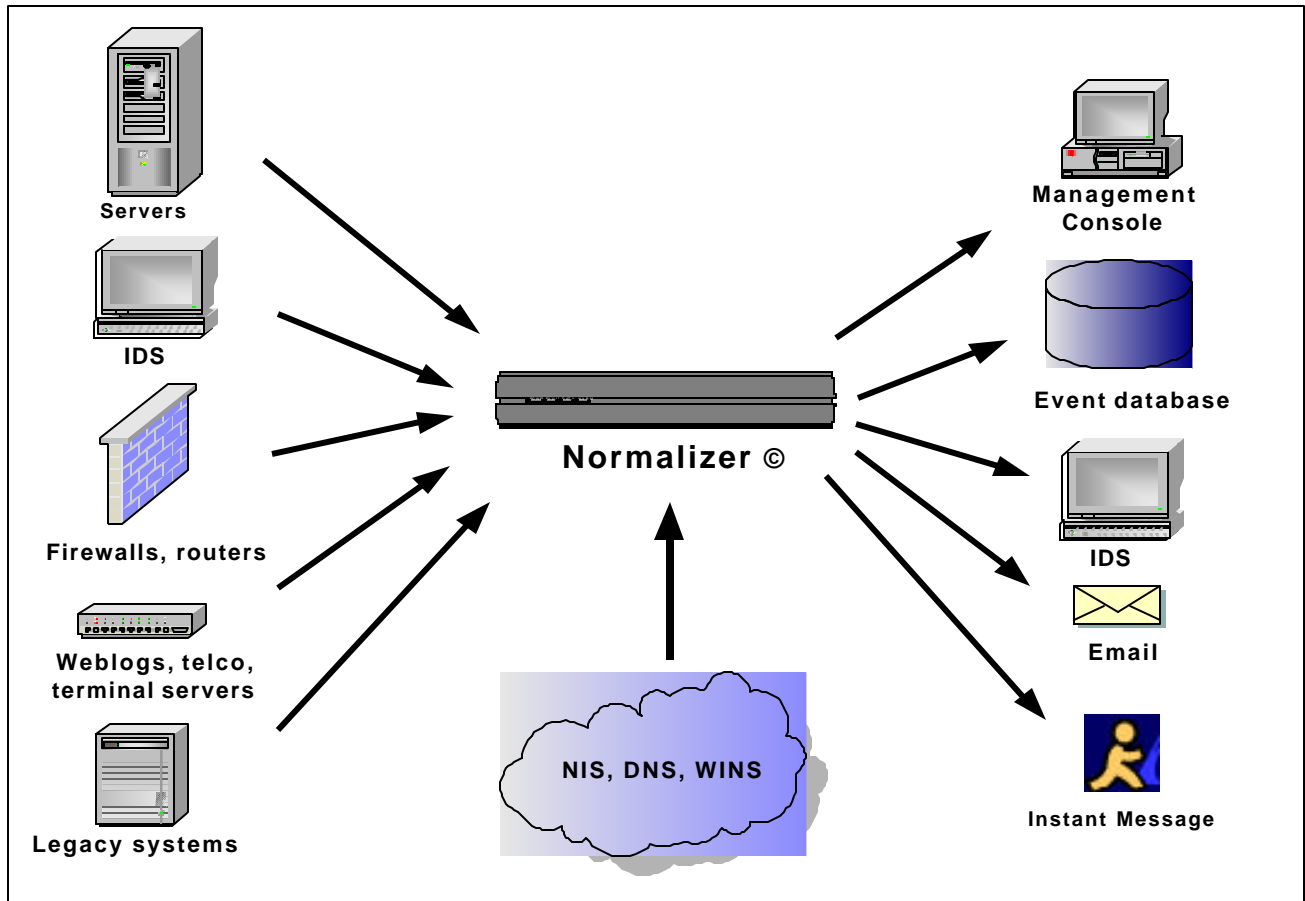


Figure 2

Figure 2, above, is an example of the varied inputs and outputs that can be brought together with the Normalizer. Ranging from database server logs to telecommunications systems to the contents of global network information services, these logs can be combined, normalized for queries and analysis, and sent on to other systems in various ways.

## Asking Basic Questions

By querying a standardized combination of internal system data and business-related data, and real world news items, users can ask and answer questions both basic and complex:

- Is our company under surveillance by an individual, group or entity?
- Have user IDs or passwords been compromised?

## Normalizing Security Data Streams for Queries and Analysis

- Is anyone attempting to hijack our systems in order to attack or hack other systems?
- Who has sent large email attachments, and what MIME-type were they?
- Who has been accessing the system outside normal working hours and for what purpose?
- Have the user patterns of anyone from our staff substantially changed?
- Has someone from outside the company attempted to break into our systems more than once and in different ways?
- Has anyone on our staff sent or received email from a competitor (or headhunter)?
- Have any of our competitors been accessing our web site or attempting to access our internal systems?

Many security events don't really look like classic intrusions; they look like slightly unusual variations in routine. The vast majority of security breaches are internal rather than at a firewalled perimeter. In fact, identifying an event as a security breach sometimes involves a judgment call on the part of the observer. If a help desk employee is found using the CEO's username and password, it all depends upon whether that employee had permission to do so. Turf wars between system administrators from different departments can often take the form of "security squabbles." All these things can be detected with the right combination of Normalizer queries.

### ***Simple and Complex Correlations***

The flexible output created by the Normalizer can provide extensive management of the data. Some ways it can support complex queries:

It can correlate logins by a given user among the desktop, authentication servers, application servers, and Internet access; it can establish several network connections as a standard series of events. An unusual event would be, for example, if the logs showed a user logging into a database server without having first logged into any desktop client. It can also be used to reveal several users working under the same login ID, as opposed to one user of the login carrying out activities on several systems.

It can correlate events on a host in one time zone with possible related events in another time zone. For example, a user might log into one machine at 5.00 am in New York and telnet from there to another host in London at noon local time; these events are actually simultaneous, but they need to be found and correlated to be recognized.

The Normalizer output can be used to match events in different combinations that may or may not be significant when put together. Isolated attempts to log in as an administrator

on one system, which might have been ignored, may indicate something more troubling when it is matched with attempts and successes on other hosts. The path of a security breach is often circuitous; an attacker may need to use one host to gain administrator privileges, use those to make files on another system readable, and then log in to yet another system under a different ID to exploit what was found in the files. Putting these clues together requires querying and sorting of various data, over and over again, to extract the critical events in the proper context.

### ***Tailoring the Reports***

The Normalizer can be used to tailor the output to the audience. A CEO may be more interested in extracting the business-related data, such as the number of hits on an e-commerce website, or the average time it takes a particular order to traverse several department systems. A system administrator might be more concerned with uptime data. A security officer could focus on the statistics for failed logins versus successful ones.

The real power of the Normalizer comes not only from centralization, normalization and correlation but also in the ability to generate "tiered reports". Tiered reports are pyramidal in nature. The Normalizer can be used to answer cogently and succinctly questions by upper management, more thoroughly to IT Management, and in extensive detail to the technical end users. These simplified questions might be:

- What is the state of security? [OK/Bad]
- Is it getting better or worse? It is getting [better/worse] than it was [yesterday, last week, last month, last quarter, last year].

From a technical view these answers are achievable.

When approached logically these questions can be reduced to mathematical summations of explicit choices.

The relative status of overall security in an institution could be derived from various factors such as:

- Sharing of login IDs and passwords: There were fewer(more) than M and changed by less(more) than A percent/std. deviation
- Scans or attacks by unknown parties: There were fewer(more) than N and changed by less(more) than B percent/std. deviation
- Scans or attacks by competitors: There were fewer(more) than O and changed by less(more) than C percent/std. deviation
- Unauthorized accesses to company confidential information: There were fewer(more) than P and changed by less(more) than D percent/std. deviation
- Anonymous uses of an administrator login: There were fewer(more) than Q and changed by less(more) than E percent/std. deviation
- Number of employee accounts closed after termination: There were fewer(more) than R and changed by less(more) than F percent/std. deviation

## Normalizing Security Data Streams for Queries and Analysis

- Number of computer viruses found: There were fewer(more) than S and changed by less(more) than G percent/std. deviation
- Emails to competitors by staff containing spreadsheets/documents: There were fewer(more) than T and changed by less(more) than H percent/std. deviation

The evaluation of the general state improving or getting worse would be determined by a weighted average of the above per period of time.

An upper-level executive interested only in the big picture could receive a report stating plainly: "IT Security is OK and getting better; click here for details." The details, if requested, would be summary charts and figures.

The IT/Security Management would get the overview, plus the chart and figure details.

The technical staff interested in the actual data would get the above two reports, plus access to the data and logs upon which the evaluation was based.

## Displaying the Data

The Normalizer can cast its output into several different formats, including:

- Comma-separated value (CSV)
- Tab-delimited format
- SQL format, for easy incorporation into a database

These outputs can be transferred to other systems in the same ways that the original logs were passed to the Normalizer, including as syslog or SNMP traps. They can be parsed into HTML tables on a website, accessed by a database front end, or pushed into another event monitor such as HP OpenView or a security management console. The normalized output can be sent as input into intrusion detection systems to supplement the data that already exists.

## Summary

The Normalizer is a unique tool for consolidating and correlating data. It enables an enterprise to combine its business and system information to uncover critical events. The Normalizer can be used as a standalone security appliance or as complementary infrastructure with other existing systems. By centralizing, standardizing and correlating diverse logs, it can provide a singular, comprehensive and unified view of the entirety of an enterprise's security-related information.

Copyright © 2002 by Perfectway Corporation.

## Reading List and Other Resources

Go read these other fine papers and books.

**Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**

*Official Journal L 281 , 23/11/1995 p. 0031 - 0050*

[http://europa.eu.int/eur-lex/en/lif/dat/1995/en\\_395L0046.html](http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html)

**What the European Data Privacy Obligations Mean for U.S. Businesses**

<http://www.gigalaw.com/articles/2001/harvey-2001-02-p1.html>

**“Analyzing Event Sequences for Dominants and Deviants”**

CERIAS project, <http://www.cerias.purdue.edu/programs.php#3>

**“Data Mining Approaches for Intrusion Detection”**

USENIX paper, <http://www.cs.columbia.edu/~sal/hpapers/USENIX/usenix.html>

**“Commonly Overlooked Audit Trails on Intrusions”**

<http://mixter.warrior2k.com/logs.txt>

**“Manage Logging and Other Data Collection Mechanisms”**

CERT, <http://www.cert.org/security-improvement/practices/p092.html>

## About Perfectway

Founded in 1999, **Perfectway Corporation** designs, writes, supports and aids in the implementation of enterprise security technology. Perfectway is headquartered in East Brunswick, New Jersey, with operations in Pennsylvania, Illinois, and Florida. More information about Perfectway’s products and services are available at

<http://www.perfectway.com>.