



**SOLEERA**  
NETWORKS

# Negative Day Threat Detection

## *ISSA Utah*

2008-12-09

Joe Levy – CTO, Solera Networks

# Obligatory fear mongering Intro

HIPAA, GLBA, SOX, FISMA, FFIEC,  
SB1386, GRC, FERPA, PCI, CALEA,  
Insider-threats, Data-leakage,  
Identity-theft, Storm/Kraken/Botnets,  
DNS cache poisoning, XSS, CSRF,  
SQL-injection, DNS-rebinding, TJX,  
Heartland Payment, IM/P2P leaks,  
Downadup/Conficker, HR-liability,  
Exfiltration, Deperimeterization

# There is no shortage of “anti-threat” countermeasures

- Firewall, UTM, NG-FW
- IDS/IPS, Gateway Anti-Malware, Anti-Spam
- Host AV, Endpoint security, NAC
- 2FA, Strong Auth/Identity
- Content-filtering, WAF, DLP
- Honeypots, NBAD, Log analysis, SIEM

*Since infinite resources cannot be allocated to countermeasures, the goal should be the mitigation of risk to an acceptable level*

# Yet you can only find what you're looking for

- **Risk** is the probability that some **threat** will exercise a certain **vulnerability** so as to negatively impact an **asset**
- Such events, or exploits, are only detectable by information security controls that have previously classified the events
- The occurrence and impact of an event *today* might not be known for weeks or months

*Is it possible to unobtrusively and completely defend against the unknown, undetectable, and invisible?*

# ...probably not – treat the matter as *when*, not *if*

Enter the total number of affected records here  
(no commas ie., 25000)

Internal Investigation	-20%	Average Cost	+20%
Cybercrime consulting	5520	6900	8280
Attorney fees	5596.8	6996	8395.2
<b>Sum: \$</b>	<b>11117</b>	<b>\$ 13896</b>	<b>\$ 16675</b>
Notification/Crisis Management			
Customer notification (certified mail)	10176	12720	15264
Call center support	7200	9000	10800
Crisis management consulting	4032	5040	6048
Media management	796.8	996	1195.2
<b>Sum: \$</b>	<b>22205</b>	<b>\$ 27756</b>	<b>\$ 33307</b>
Regulatory/Compliance			
Credit monitoring for affected customers	46272	57840	69408
Regulatory investigation defense	17116.8	21396	25675.2
State/Federal fines or fees	36307.2	45384	54460.8
<b>Sum: \$</b>	<b>99696</b>	<b>\$ 124620</b>	<b>\$ 149544</b>
<hr/>			
<b>Total Data Loss Expenses: \$</b>	<b>133018</b>	<b>\$ 166272</b>	<b>\$ 199526</b>

- Countermeasures have practicable limits
- Scare tactics aside, security incidents carry a very real cost
- Big or small, incidents will occur

*The goal then becomes damage assessment and control*

<http://www.tech-404.com/calculator.html>

<http://attrition.org/dataloss/>



# Data Breach Investigations Report (June 2008)

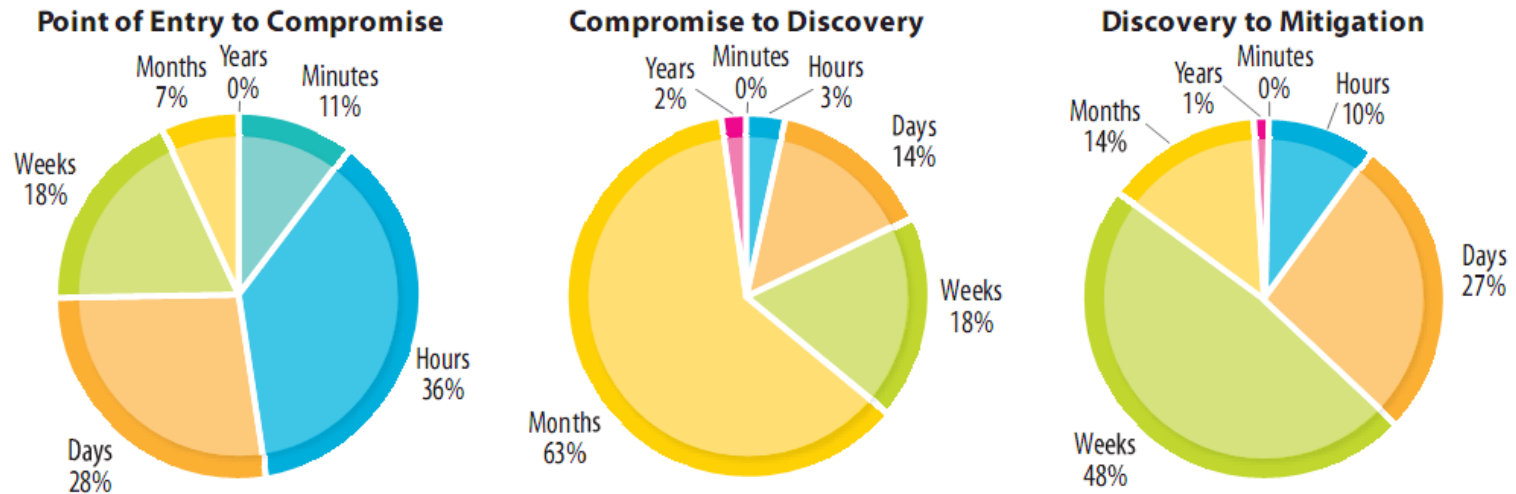
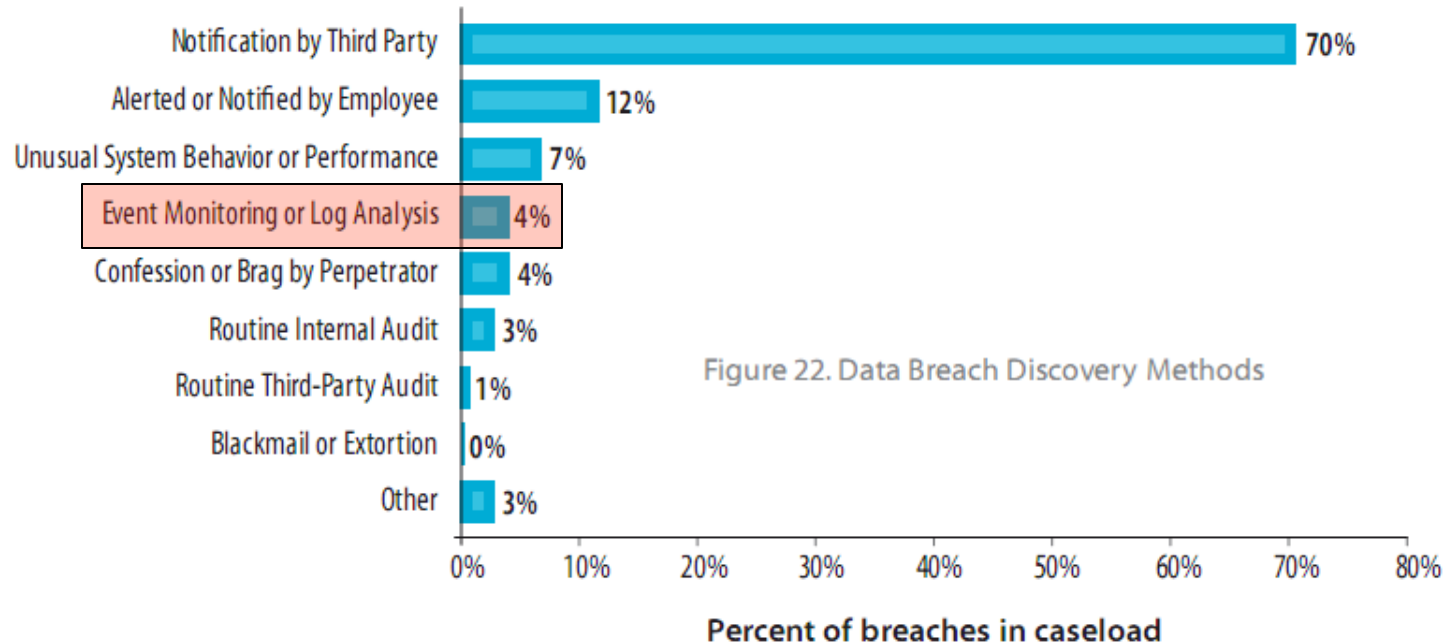


Figure 21. Data Breaches: A Time Span of Events

*“... the main reason for this is that victims do not know how to respond. Many organizations—even those with full-time security resources—either have no incident response plan, or have never vetted it against real-world incident scenarios.”\**

\* <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>

# Data Breach Investigations Report (June 2008)

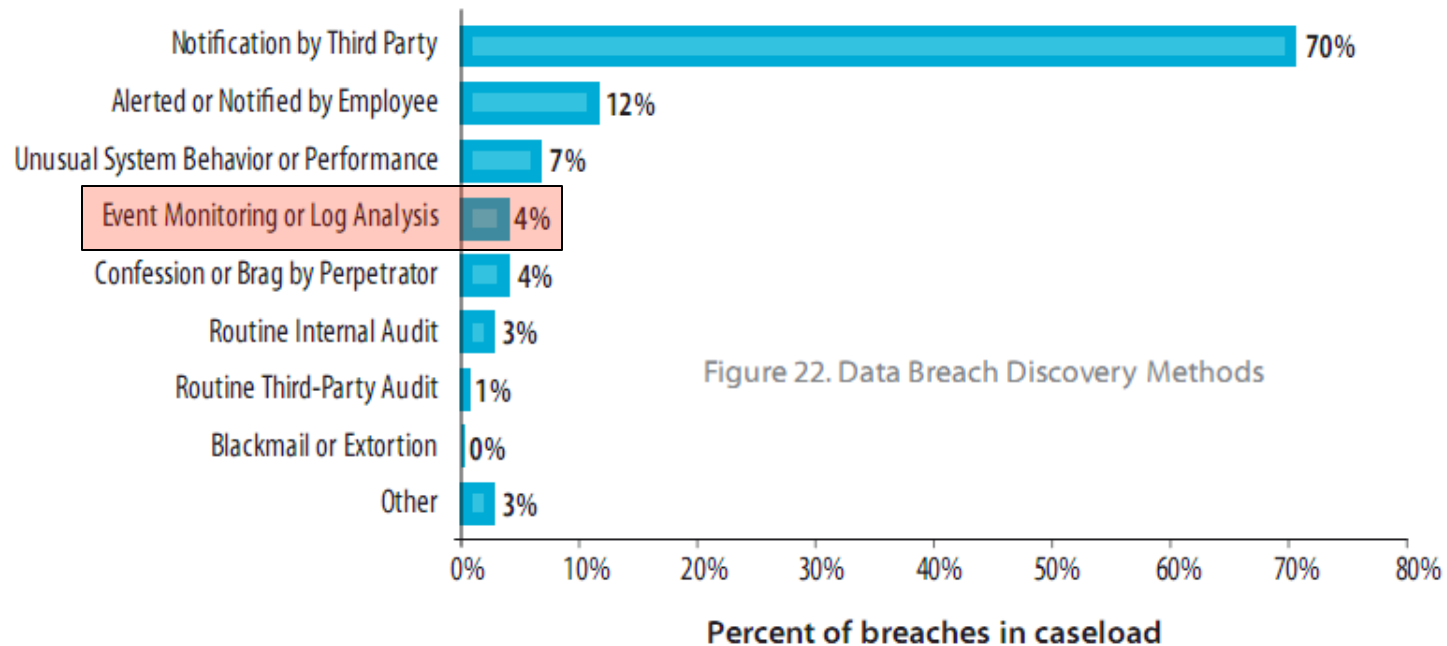


*Whether a failing of people, process, or technology, only 4% of incidents are discovered by existing monitoring or analysis controls*

\* <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>



# Data Breach Investigations Report (June 2008)



*Said another way:  
Event monitoring and analysis tools will fail 96% of the time*

\* <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>



# Incident Response – the basics

1. Contain the damage
  2. Preserve/duplicate the compromised system's state
  3. Contact law enforcement and legal agents
  4. Restore operations of compromised system
  - 5. Determine incident cause**
  6. Document incident and recovery details
  7. Update control agents/implementation details accordingly
  8. Update incident response plan, as needed
- Controls the indirect damage, such as injury to reputation, negative publicity, lost customer confidence, legal repercussions, and other fines or penalties
  - Identifies and resolves the root causes of the incident, determines scope of impact, and helps prevent repeat occurrences

*But the fact that it happened often implies that it was undetectable.  
How do you determine the cause of something after it already  
happened undetected?*

# Digital Forensics

- **Digital evidence** is information of probative value that is stored or transmitted in a binary form<sup>1</sup>
- **Digital forensics** involves the identification, collection, preservation, examination, and analysis of digital evidence
- Preservation and completeness of evidence are foundational to any investigation or incident response
- Forensic sciences are only applicable when there is permanence (a memory) of potential evidentiary artifacts
- Countermeasure: Anti-Forensics (e.g. secure delete, trace erasure, recovery inhibition) tools are becoming commercialized and common
- Counter-Countermeasure: Live response attempts to capture volatile memory, which can persist in the right conditions
- Acquisition must include allocated files, file slack, deleted files, and volatile memory – Total **bit-stream** replication (e.g. dcfldd<sup>2</sup>)

1. Scientific Working Group on Digital Evidence - <http://www.swgde.org>

2. Department of Defense Computer Forensics Lab Data Definition - <http://dcfldd.sourceforge.net>



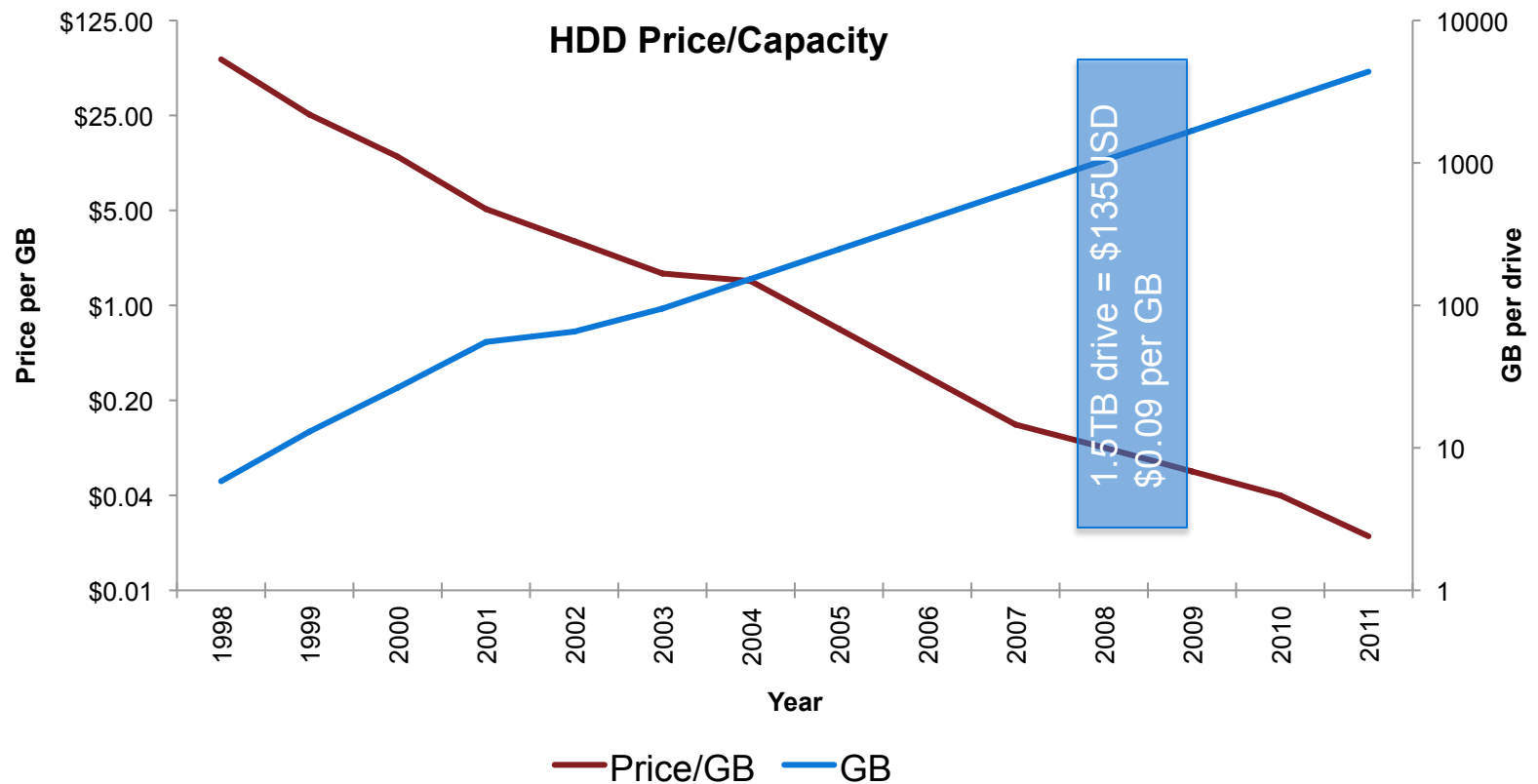
# Network Forensics

- Current attempts at network forensics rely on logs, IDS/IPS events, SIEM analysis, or subject-specific intercept
- Just as it is insufficient to do a standard backup of a hard drive, it is equally inadequate to gather only *what's visible* on the network
- To date, it has been infeasible to capture traffic at rates above Fast Ethernet because at those proportions:
  1. It's hard to pull the packets off the wire
  2. It's hard to lay them down on disk
  3. It's hard to find them once they're there

Speed-Mbps	GB/Hour	TB/Hour	TB/Day
50	21.97	0.02	0.51
100 (FE)	43.95	0.04	1.03
500	219.73	0.21	5.15
1000 (GigE)	439.45	0.43	10.30
5000	2197.27	2.15	51.50
10000 (10GE)	4394.53	4.29	103.00



# Storage trends enable total fidelity



Sources: [http://commons.wikimedia.org/wiki/Image:Hard\\_drive\\_capacity\\_over\\_time.png](http://commons.wikimedia.org/wiki/Image:Hard_drive_capacity_over_time.png)  
<http://www.alts.net/ns1625/winchest.html>



# From Ethernet to Perma-net

- Logging/auditing, IDS/IPS/SIEM ignore the “network slack”
  - Records only meta-data of events
  - Records only what it specifically looks for: the visible
- Consistent improvement in storage technologies and economics enabled DVR
  - Why not leverage for IR and forensics?
- Beyond capacity, the technology must keep pace with the input
  - 100mbit->1GbE->40GbE->100GbE->?
- The full utility of memory comes from efficient and reliable information retrieval
- Storing all the packets is only useful if information can be indexed, searched, and recalled as needed

*What if it were practically viable to replay any event, including the “unknown unknown”, with full fidelity even months after it occurred?*

# Solera Networks Solutions

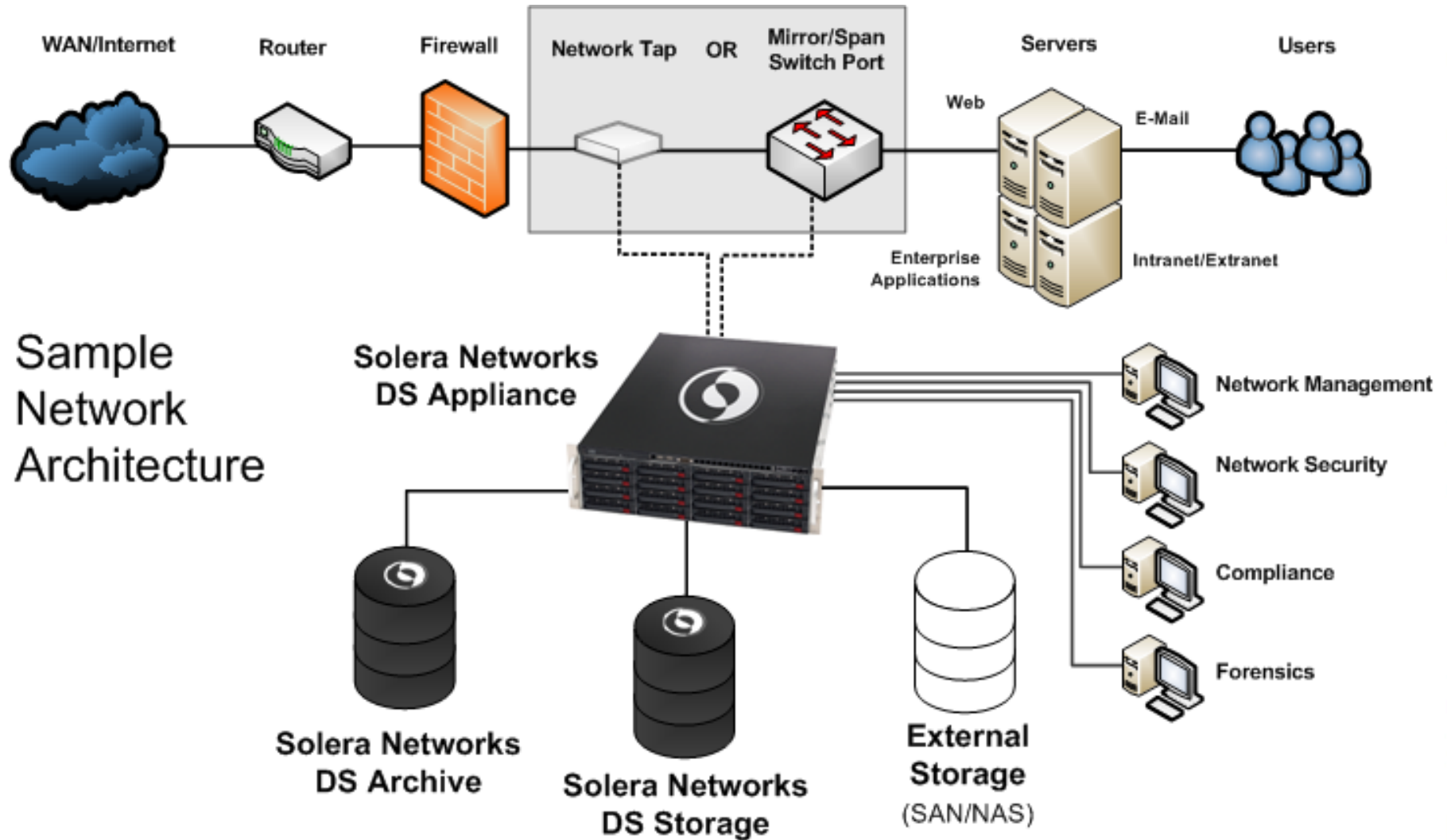


## Full Packet Capture, Stream-to-Storage & Search

- **Software** delivered in multiple form factors: virtual and physical appliances, with **flexibility** to deploy as your needs dictate
- **Passive capture of all traffic** (header and payload) to disk at up to **10Gbps** with no network overhead
- **Easy, contextual search** (e.g. email, web, IM, VoIP, and attachments) of all **data in motion** on the network
- **Up to 16TB onboard storage**, 64bit file system externally expandable to exabytes
- **API access** to storage, and use of **industry standard** formats

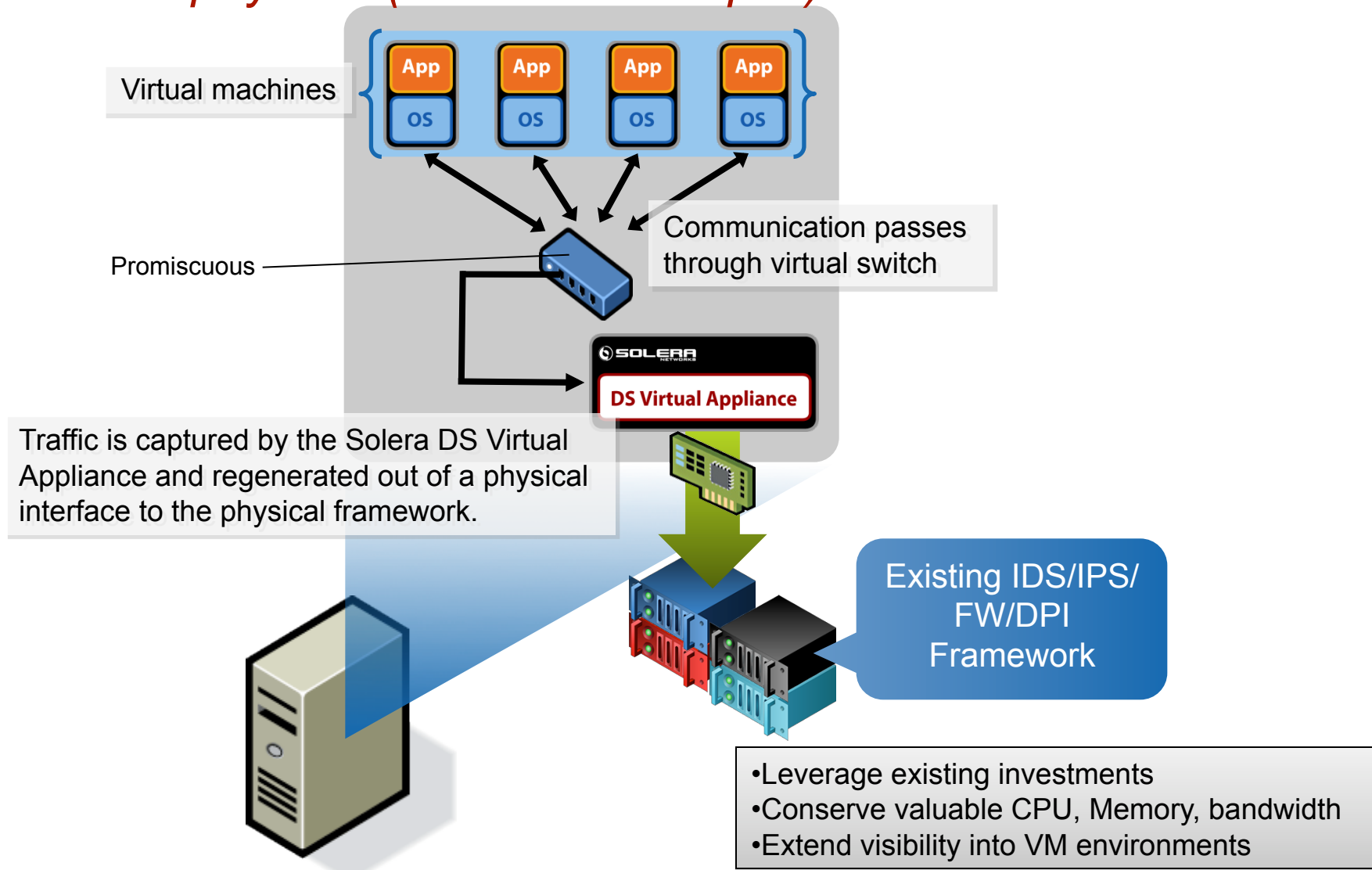


# Functional Deployment

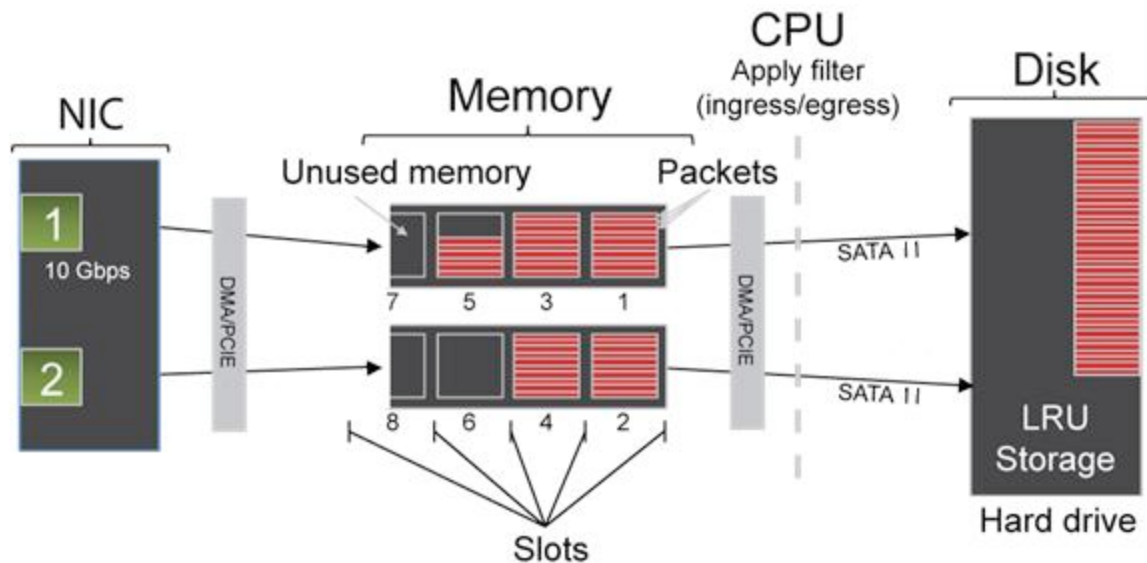


# Secure Virtual Environments

*virtual to physical (Solera V2P Tap™)*



# 10 Gbps Capture



- Custom DSFS created for high-speed capture and playback
- All capture operations in kernel space
- Certified for sustained 10Gbps capture
- Capacity to capture, hours, days, weeks of data

- PCIe 1.1 bus – 250MByte per lane
- PCIe x4 = 1000MB = 8Gbit per slot
- PCIe x8 = 2000MB = 16Gbit per slot
- 10Gbit NIC (PCI x8) and/or multiport 1Gbit NIC (PCIx4)
- 2 x 9650SE-8LPML (PCI x4, SATA II, 700+MB/sec) – 11+Gbit controller throughput capacity
- 16 x SATA-300 drives = 3Gbit per drive (x16) = 48Gbit drive throughput capacity



# DeepSee

- Meta analyzer indexes all packets
- Flows are dynamically reconstructed by query
- Data carver identifies protocols and artifacts
- Artifacts are reassembled and extracted
- Regex searches can be performed on artifacts

Stream of packets crossing the network

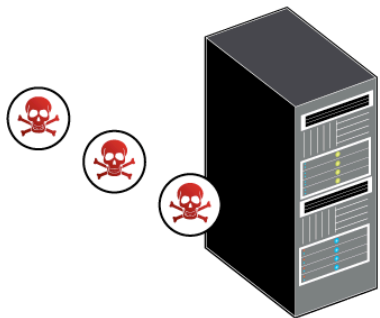


Packets from selected flows are identified and combined

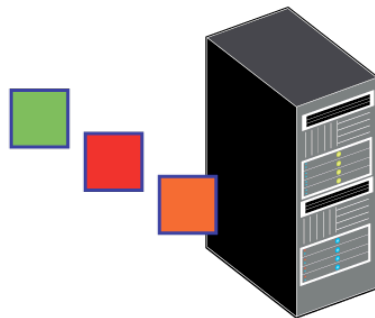
The screenshot displays the DeepSee web interface. At the top, there's a navigation bar with 'Control Center' and 'DeepSee Reports'. Below this is a search bar and a 'Search' button. The main content area is split into two columns. The left column contains a 'Reports' section with a pie chart titled 'Top Applications' and a 'Report Parameters' section with a 'Start Time' slider. The right column shows an 'Advanced Search' section with various filters and search options. At the bottom right, there's a 'Scanner' section displaying a list of detected protocols and artifacts, with one entry highlighted in green.

# Negative Day Threat Detection

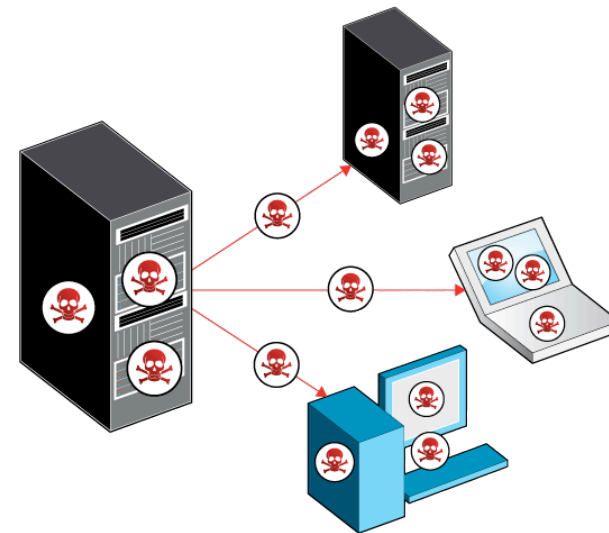
Malware Monday



Patch Tuesday

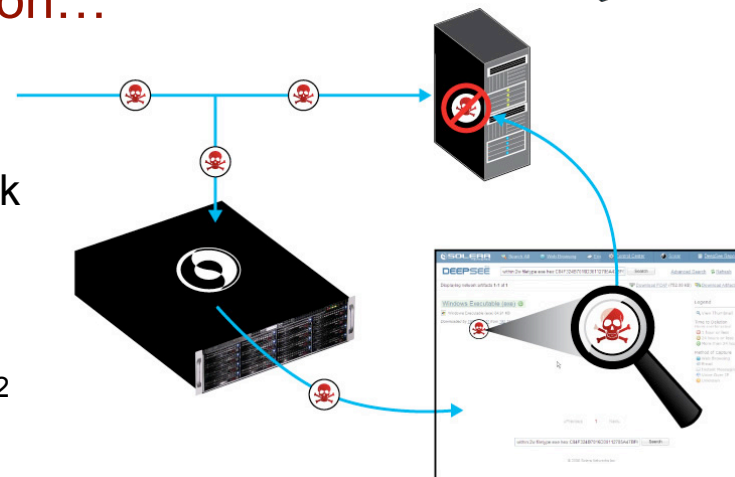


Wake-up Call Wednesday



Events can occur prior to remediation...

1. Microsoft released MS08-067 patch on October 23, 2008<sup>1</sup>
2. Evidence of exploits in the wild (dating back weeks) emerged shortly thereafter
3. Network memory allows a search for all executables containing hex-pattern: C84F324B7016D30112785A47BF6EE188<sup>2</sup>



1. <http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

2. [http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT\\_MS08-067?rev=1.8;content-type=text%2Fplain](http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/EXPLOIT/EXPLOIT_MS08-067?rev=1.8;content-type=text%2Fplain)

# Evolution

- “Attack/Defense Co-evolution” forces Information Security experts to get more sophisticated as attacks increase in strength and number
- With this evolution comes the realization that not all threats can be prevented
- Such enlightenment is creating the urgent need for incident response and network forensics
- Just as we saw the evolution of the firewall from a toolkit to a universal technology, so will we see the same evolution of network forensics
- The sooner forensics technologies become accessible, integrated, and easy-to-use, the sooner can the science of information security become more effective
- Making this feasible are advances in storage technologies and economics - but networks are becoming increasingly deperimeterized, virtualized, and utilized
- It is Solera Network’s mission to stay ahead of these evolutionary forces, advancing the *state-of-the-science* of information security by practically delivering the future of network forensics today





**SOLERA**  
NETWORKS

**Q&A**



**SOLEERA**  
NETWORKS

Thank you

Joe Levy

[jlevy@soleranetworks.com](mailto:jlevy@soleranetworks.com)

**Solera Networks**

See everything. Know everything.

# Ethernet

## Ethernet Constants - IEEE 802.3

	10Mbps	100Mbps	1Gbps	10Gbps	
Bit/time	.1μs	.01μs (10ns)	1ns	.01ns	
Byte/time	.8μs	.08μs (80ns)	8ns	.8ns	
Inter-Pkt Gap	9.6μs	.96μs	96ns	9.6ns	<i>IPG = 96 bits / 12 bytes</i>
Preamble	6.4μs	.64μs	64ns	6.4ns	<i>Preamble = 64 bits / 8 bytes</i>

## Max Pkt per second = #bps / (pkt size + IPG + Preamble) \* 8

	10Mbps	100Mbps	1Gbps	10Gbps
<b>64</b>	14,881	148,810	1,488,095	14,880,952
<b>128</b>	8,446	84,459	844,595	8,445,946
<b>256</b>	4,529	45,290	452,899	4,528,986
<b>512</b>	2,350	23,496	234,962	2,349,624
<b>768</b>	1,586	15,863	158,629	1,586,294
<b>1024</b>	1,197	11,973	119,732	1,197,318
<b>1518</b>	813	8,127	81,274	812,744

## Max Throughput (bits) = Max pkts/sec \* pkt size \* 8

	10Mbps	100Mbps	1Gbps	10Gbps
<b>64</b>	7,619,048	76,190,476	761,904,762	7,619,047,619
<b>128</b>	8,648,649	86,486,486	864,864,865	8,648,648,649
<b>256</b>	9,275,362	92,753,623	927,536,232	9,275,362,319
<b>512</b>	9,624,060	96,240,602	962,406,015	9,624,060,150
<b>768</b>	9,746,193	97,461,929	974,619,289	9,746,192,893
<b>1024</b>	9,808,429	98,084,291	980,842,912	9,808,429,119
<b>1518</b>	9,869,961	98,699,610	986,996,099	9,869,960,988

# Forensic Lab Certifications

- ASCLD Forensics Lab Certification and Accreditation: This program, which has been used by the various law enforcement organizations for some time, was designed to certify forensic labs in scientific disciplines such as DNA and fingerprint analyses. ASCLD now covers digital evidence. Further information on ASCLD can be found on its Web site at [www.ascl-d-lab.org](http://www.ascl-d-lab.org).
- ISO 17025 Forensics Lab Certification and Accreditation: This certification program has the support of the international community, many U.S. organizations and corporations as well as government facilities, and law enforcement agencies. ASCLD is also adopting the ISO 17025 certification process.
- NIST Handbook (HB) 150 Lab Certification: This program is a baseline document that can be used as a foundation for many scientific disciplines such as ASCLD. HB 150 has been used as a foundation to validate various federal government labs.

ASCLD/LAB - American Society of Crime Laboratory Directors Laboratory Accreditation Board

<http://www.ascl-d-lab.org/>

