







UNVEILING THE SECURITY ILLUSION:
THE NEED FOR ACTIVE NETWORK FORENSICS

THE NEED FOR ACTIVE NETWORK FORENSICS

Neither small to large enterprises nor government institutions are immune to the threats that pervade today's security landscape. Leakage of congressional documents, a half million credit card numbers hacked from a leading web host provider, and even a major security vendor falling victim to a website breach are just a few recent headlines that proclaim the costly network threats facing organizations of all types and sizes.

These network threats can typically be classified into four categories: threats coming in, threats invited in, threats already in, and threats going out. Incoming threats typically deal with network perimeter attacks, such as SQL and XSS injections that take advantage of vulnerabilities in an organization's public web portals to get to sensitive data on backend databases or to steal sensitive user information. Threats invited in take on many social and technological forms, from emails phishing for information or inviting users to fall prey to drive-by downloads, as well as online social interactions that make seemingly innocent requests for personal or confidential information.

However, the most dangerous threats are those that are already inside the network. Whether they're compromised systems or renegade users, left unchecked the damage potential of these threats can quickly escalate, since once inside they can do nearly anything they want. The threat of sensitive data going out can often be just as costly, as business viability is put at risk if confidential trade secrets, customer information, or classified national security information leaks out. An often-overlooked aspect of this threat deals with the liabilities and statutory fines that can result if organizations' systems have been infected with active spam-bots that push out bulk email en masse.

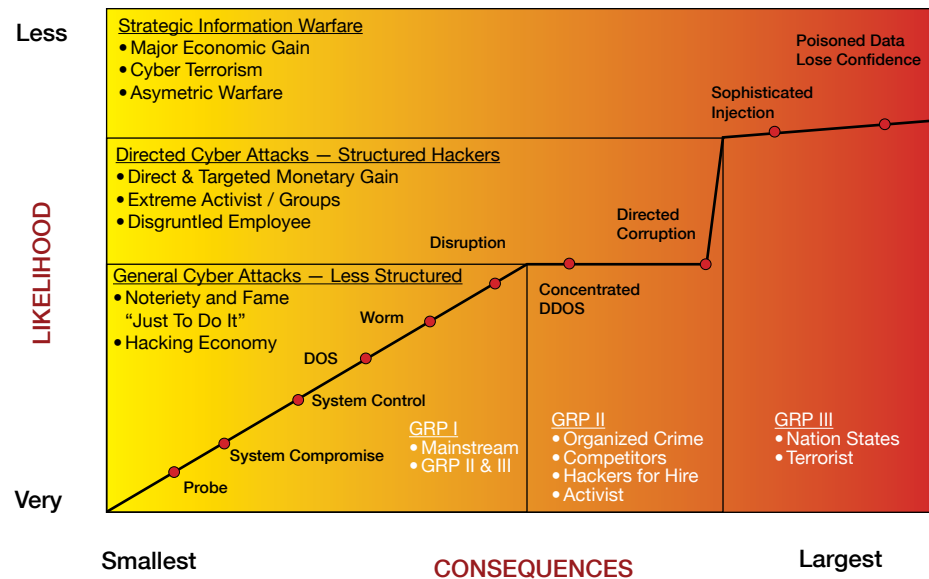
	<p>Congressional Documents Leaked on P2P Service Jaikumar Vijayan — November 1, 2009</p>
	<p>Network Solutions Warns Merchants After Hack 600,000 credit card numbers stolen from Ecommerce Hosting merchants Robert McMillan — July 7, 2009</p>
	<p>First Lady Safehouse Route, Govt. Mafia Trial Info Leaked on P2P Networks Brian Krebs — July 29, 2009</p>
	<p>Kaspersky Hires Expert to Analyze Website Hack Elanor Mills — February 9, 2009</p>

The motivation for attacking a network resource varies greatly between attackers and incidents. However, there is an increasing trend toward more targeted, systematic, and damaging attacks. For example, recent security data suggests that while general attacks motivated by fame or for entertainment ("just to do it") are still present, financially or emotionally motivated attacks directed at specific organizations or individuals (i.e., financial institutions, competing businesses, former employers, and others) are becoming a larger overall percentage of both successful and failed attacks. Additionally, cyber attacks backed by terrorist organizations or foreign nation states that attempt to steal, disrupt, or corrupt strategic information are on the rise and generating great attention in political circles.

While the security industry has taken great strides toward providing an increased level of protection within the constantly expanding threat landscape, it falls short of delivering the complete protection that administrators believe is possible. Although vendors provide a comprehensive array of preventative solutions to help organizations protect against the wide variety of painful and costly threats, their solutions all have an inherent flaw. This flaw, if not appropriately recognized and appreciated, can leave organizations with false confidence and the illusion that they're more secure than they really are.

The inherent flaw in threat protection solutions that makes the promise of a breach inevitable is that traditional methods and industry best-practices for combating attacks rely on known threats or known behavior. For example, deterministic methods create a baseline that first defines and then watches for the fingerprints of known attacks and threats. Other types of preventative solutions employ heuristic measures that look for deviations or anomalies in normal behavior in the usage patterns of a network's users and on their data as it traverses the network. While heuristics are less deterministic in nature, they still require

a pre-classification or administrator training of what's considered acceptable behavior. As a result, they are prone to high "false-positive" mis-detection rates.



Source: INL Training - http://www.inl.gov/scada/training/introductory_scada.shtml

The truth is that no security solution will always know what to look for. It is impossible to accurately determine all possible ways that a future breach can occur. There are simply too many unknowns. For example, the 2009 Data Breach Investigations Report conducted by Verizon Business found a common trend among the breaches it investigated that confirms this point. The report found that 9 out of 10 breaches involved what it referred to as "unknown unknowns," which include unknown data, unknown connections, unknown privileges or unknown systems.

These "unknown unknowns" play an increasing role in more targeted and more strategic attacks. In these cases, rather than making use of publicly known exploits, determined adversaries take a more cunning approach than general attackers. They will likely invent their own special-purpose attacks designed to evade both known deterministic and heuristic protection schemes, or intentionally disabling security intrusion detection systems and event logging infrastructures.

This is why large organizations increasingly accept the fact that while there is much they can do to minimize the effects of known threats, the truth is they know that inevitably they will suffer a breach by an attack that has not yet been classified. In fact, a recent survey of IT and security professionals across the United States revealed that more than 85% had either a major network security incident in the past 36 months or expect to have a major incident in the coming 36 months (Trusted Strategies, Network Forensics Market Survey, September 19, 2009).

However, while most organizations know that breaches will come, what they typically fail to understand is that when attacks happen, they will lack the necessary information to discover not only who did it and how it happened, but what exactly happened as well. The primary problem is the belief that when a breach occurs, existing tools will be able to report on the breach and provide them the remediation information they need. However, the reality is that when network security incidents occur, existing tools report a breach only 6% of the time, necessitating that organizations find out about the breaches in other, possibly embarrassing ways (2009 Data Breach Investigations Report, Verizon Business). This is due in large part because when breaches occur, the majority of the time the tools don't recognize them as known threats. So, not only do they not report on the breach, but they also don't record much, if any, of the information associated with the event.

To make matters worse, if an organization's security solutions aren't consistently telling them when breaches happen, it's very possible that these attacks are ongoing, continually causing more data loss and privacy breaches. Obviously, the longer an attack continues or repeats, the more costly it is for an organization. The faster an organization can discover the source and scope of a breach, stop it and remediate it, the less damage and cost it will accrue. This is the principle reason why organizations need a greater ability to discover and understand the root cause of any network security event. It is also the primary reason why organizations need active network forensics.

ACTIVE NETWORK FORENSICS - A DYNAMIC DEFENSE

Active network forensics makes all past and present network data instantly visible and allows perfect fidelity through replaying past traffic, enabling organizations to detect and understand the full source and scope of any security event so they can protect against further attacks. Active network forensics also enables an organization to validate that the same attack doesn't work again after they've implemented appropriate counter-measures. Combining high-speed data capture, indexed storage, and comprehensive analysis tools, active network forensics is analogous to putting a security camera on a network. Doing so instantly exposes any specific network event, making even the most sophisticated and targeted attacks plainly visible both when they happen, and at any time in the future. Active network forensics dramatically reduces the cost and ongoing exposure of network security incidents by dramatically shortening the time to remediate from days to hours, while eliminating the chance of related follow-up attacks.

In essence, effective network forensics complements and works with traditional security solutions to provide organizations a dynamic defense against breaches through the following characteristics:

- Giving an organization's network a memory
- Capturing, filtering, and indexing all network traffic
- Searching and replaying traffic to uncover the full scope of any network event
- Fixing the problem to mitigate further risk and validating that the fix actually works as intended

THE NEED FOR 24/7 SURVEILLANCE

For a network forensics solution to be effective, it needs to capture 100% of the data stream flowing across the network. Capturing only a subset of the data is not sufficient. The reason is simple: just as with a security camera, if it's not always on and always recording, there's no guarantee that it will capture the events of interest. For example, at a physical crime scene, a forensic team's job is made much easier if they can simply review a video recording that captured in full detail all aspects of what occurred during the crime. Missing video segments or video that doesn't provide a complete picture of everything that occurred result in uncertainty, unanswered questions, and possibly the loss of ability to determine what really happened.

This analogy holds true for network forensics as well. By being able to record, store and index all the data that comes across a network when something of interest occurs, an organization can search, replay, analyze, and even reconstruct those data flows exactly as they occurred. As a result, they can go back to the past at any time to determine what actually took place and what was lost. Additionally, since such a tool provides the complete picture of the event—similar to the surveillance camera—it doesn't take much time or skill to figure out what really happened.

The following illustrate a few key examples for the need to capture 100% of network traffic:

- Stop network hacks and enhance investments in security solutions - A complete historical record – as opposed to snapshots or network traffic samples – reveals the complete context surrounding IDS, IPS and firewall alerts so security managers can see and analyze the actual traffic used to compromise a Web site, database or other critical system. This enables them to be much more effective at pinpointing vulnerable portions of the network and preventing further security breaches.
- Enjoy complete network visibility - With a complete historical record, an organization's network has no more secrets. Every action taken on the network is recorded and stored. Security managers can go back in time to watch network breaches, slow hacks and network slowdowns as they unfold.
- Stop data leakage - A comprehensive record of all data crossing the network lets security managers see what was being viewed, who viewed it, when it was accessed and what was done with it.
- Deny rogue devices access to the network – Organizations can thoroughly monitor network traffic for unauthorized or unsecured network components or access points in order to lock them out.
- Identify security breaches - Specific network traffic can be easily analyzed to verify that only authorized employees are accessing servers and other critical systems.
- Reconstruct incident artifacts (evidence) – By capturing 100% of all network data packets, security managers can completely reconstruct incidents of interest, including viewing the artifacts and other interesting data contained within a network flow; such as documents, image files, executables, instant messaging conversations, etc.
- Validate adherence to compliance mandates – A complete historical record of all electronic communication creates an audit trail to ensure that compliance with regulations (i.e., PCI, Sarbanes-Oxley, HIIIPA, FISMA and others) is strictly observed.

SUCCESS FACTORS FOR NETWORK FORENSICS

An effective network forensics solution must be able to address the following key success factors:

- In incident response, speed equals money
- Quickly ascertaining the scope of a breach limits impact to the business and brand
- Identifying small breaches quickly prevents big incidences later
- Administrators are expensive and busy
- Operators are humans, not machines
- Timely analysis requires familiar search methods for locating and pinpointing desired data (i.e., intuitive search tools, browsable directory trees)
- Effective analysis requires user-friendly tools that help locate the needle in the haystack, since even experienced administrators struggle to read a PCAP (packet capture file)—the raw file that contains the captured network data packets used in forensics analysis

An incomplete record of network traffic is ineffective because:

- Less than 100% capture leads to failure
- Records can become useless without every bit of information
- Critical information can be anywhere and is difficult to trap on today's high-speed networks
- Lack of a full record raises doubt, which can result in the failure to act or the need to remediate well beyond the actual scope of the incident in order to address the maximum potential loss
- Missing data is an effective blind spot that may forever hide an attack and data loss

TECHNICAL CHALLENGES FOR EFFECTIVE NETWORK FORENSICS

When most individuals first learn about networks forensics and its ability to record 100% of network data, their first reaction is often one of amazement or disbelief given the amount of data they believe needs to be recorded. In fact, even though network forensics promises to provide a clear understanding and insight into the full scope of breaches in a fast and efficient manner, until very recently the technical challenges associated with this requirement had stalled the security industry's ability to offer the full array of benefits offered by active network forensics.

- In essence, capturing and managing the amount of data on a typical network has been difficult for a number of reasons, including the following:
- It's difficult to pull packets off the wire fast enough
- It's difficult to put all packets on disk due to storage and speed requirements, as well as other technological limitations
- It's difficult to locate needed packets once on the disk
- It's difficult to provide access to and analysis of packets through well understood search methods

In spite of these difficulties, network forensics has been available in various forms for a number of years. However, the inability to completely overcome these issues has caused past offerings to be too cumbersome or lack the ability to scale. But recently a number of market forces and technology innovations have converged to overcome these obstacles, making active network forensics a viable and effective reality today.

The first of these market and technology forces is the fact that storage capacities nearly double each year, while at the same time their costs drop by nearly half in the same time period. The second breakthrough comes with the ability to now capture and store network packets at 10 Gbps speeds with specialized software and commercial off-the shelf hardware. The final element is the ability to provide a framework that indexes the captured data and then presents it in a way that makes it easy to find, analyze, and drill-down to the details of associated events of interest. While a few solution vendors have developed network forensics solutions that utilize one or both of the first two advances, only Solera Networks combines all three to offer a solution that delivers on all key success factors for effective, active network forensics.

EFFECTIVE, ACTIVE NETWORK FORENSICS FROM SOLERA NETWORKS

Solera Networks has overcome the technical challenges needed to deliver an active network forensics solution. It enables organizations to easily record, search, analyze, and replay all network traffic. As an automated, high-speed network forensics system it enables instant intelligent response that prevents simple security incidents/breaches from becoming catastrophic events. It makes an organization's existing set of security products more effective and valuable by providing instant context for security decisions. It works with and leverages those security investments to provide full contextual information on security issues at near real-time speeds. This reduces the time it takes to uncover and intelligently resolve the real causes of network

events. Solera Networks simplifies network security, providing a dynamic defense against the full array of network threats; including zero-day, unknown, targeted, and strategic warfare attacks.

KEY BENEFITS

By providing in near real-time the complete context for network and security events, active network forensics from Solera Networks provides the following key benefits:

- Prepares you to swiftly respond to zero-day, negative day, and unknown threats
- Enhances the value and effectiveness of other security investments
- Reduces and simplifies the monitoring, reporting, analysis, and remediation time required of a security staff to defend and maintain effective protection
- Facilitates prosecution through forensically complete evidence
- Facilitates a quick understanding of breach root causes to enable swift, intelligent and effective response to prevent catastrophic events and ongoing risk
- Allows for validation of fixes installed after a breach occurred, through the ability to replay a network attack

HOW ACTIVE NETWORK FORENSICS FROM SOLERA NETWORKS WORKS

At a high level, the network forensics platform from Solera Networks can be broken down into the following four key areas:

- Solera OS™ and Packet Capture File System
- Solera Index Layer (SoleraDB™)
- Solera DeepSee Forensics Suite™
- Solera Web Services API

SOLERA OS AND PACKET CAPTURE FILE SYSTEM

The special purpose Solera OS and packet capture file system was specifically designed to automatically capture and store all the data packets that flow across the network, even up to speeds of 10 Gbps and storage partitions up to one petabyte in a single location. As storage capacities expand in the future, the Solera Networks solution will be able to scale to support those higher capacities. At its most basic level, the solution takes network data packets from a network interface card (NIC) and then moves that data to storage in a specialized format that has been optimized for extremely high throughput storage, accuracy, manageability, and security.

Specific to being able to pull packets off the wire at high network speeds, the Solera Networks solution provides the following:

- 10 Gbps packet capture on a single dedicated forensics appliance
- A virtual appliance solution to capture data only seen within a hypervisor

In terms of its ability to stream network packets to disk, the Solera Networks packet capture file system has been designed specifically with the following characteristics:

- High efficiency in writing large segments of network data
- An optimized ring buffer capture methodology specifically designed for network forensics
- Option of ingress and egress filtering
- Multiple data access methods, including PCAP files, regeneration or replay of any time slice
- Resilient, proprietary file system designed to ensure data integrity and un-modifiability
- In addition to enabling organizations to capture 100% of network traffic, the solution also gives complete control over the type of traffic captured. It provides the option to filter network traffic, either during capture or when replaying captured traffic at a later time.

SOLERA INDEX LAYER (SOLERADB)

The SoleraDB index layer is a key differentiating aspect of the Solera Networks forensics platform. Even if a network forensics solution can manage to capture and store 100% of data packets that flow across a network, it has little usefulness unless it provides a way to easily and quickly locate and access specific packets of interest. Trying to find data packets associated with certain events of interest among hundreds or thousands of terabytes of stored data is equivalent to sifting through a giant desert of sand to find a single, specific granule. To simplify searching, SoleraDB provides real-time indexing of every packet,

enabling security managers to quickly search for and locate in a matter of seconds the data they're interested in.

As each packet is captured and stored, SoleraDB creates an entry in its database that includes key identifying attributes relating to the packets and the conversations that the collection of packets make up. These attributes include items such as sending and receiving IP addresses, MAC addresses, ports, protocols, and VLAN identifiers. As it indexes the complete historical record of network traffic, the system identifies specific data flows in a way that is meaningful to both IT professionals and business users to make it even easier for them to search and locate events of interest.

In summary, the real-time indexing of SoleraDB offers the following to enable organizations to quickly find specific network packets stored to disk:

- Mapped index (with metadata) of where important packets and flows are located in the packet capture file system
 - Enables visualization of data index using a directory tree/folder structure
 - Enables rapid retrieval of network flows, data via PCAP, or the use of the DeepSee Forensics suite
 - Scales up to and beyond one petabyte of online storage in a single location
- Performance of more than one million packets per second

SOLERA DEEPSEE FORENSICS SUITE

The Solera DeepSee Forensics Suite consists of a set of integrated applications that guide administrators in their search for and analysis of network data of interest. It provides the keys to unlocking captured network traffic that enable IT and other security professionals to find the real answers to their security concerns. The suite reports on captured data, providing graphical insight and context into that data. It lets users search through captured network traffic just like they would search the web, and to navigate through that traffic the same way they would navigate the files on a computer. It allows them to easily reconstruct network traffic into meaningful flows and conversations, as well as the ability to present network artifacts like web pages, Microsoft Office™ documents, PDF files, instant messenger conversations, or images in the same form that they first existed when originally captured.

The Solera DeepSee Forensics Suite allows organizations to:

- Utilize a web-like interface to search captured and live data in motion
- Rebuild captured network flows into recognizable records
- Search against contents of network records or artifacts, such as PDFs, HTML, and other files
- Search for specific information of interest within captured data
- Perform just-in-time searches
- Leverage an intuitive directory/folder tree metaphor in order to:
 - Quickly browse to and access captured data
 - Drill down into data by timeframe, IP addresses, MAC addresses, source or destination, protocols, ports, and more
- Rapidly and intuitively sift through hundreds of terabytes of data

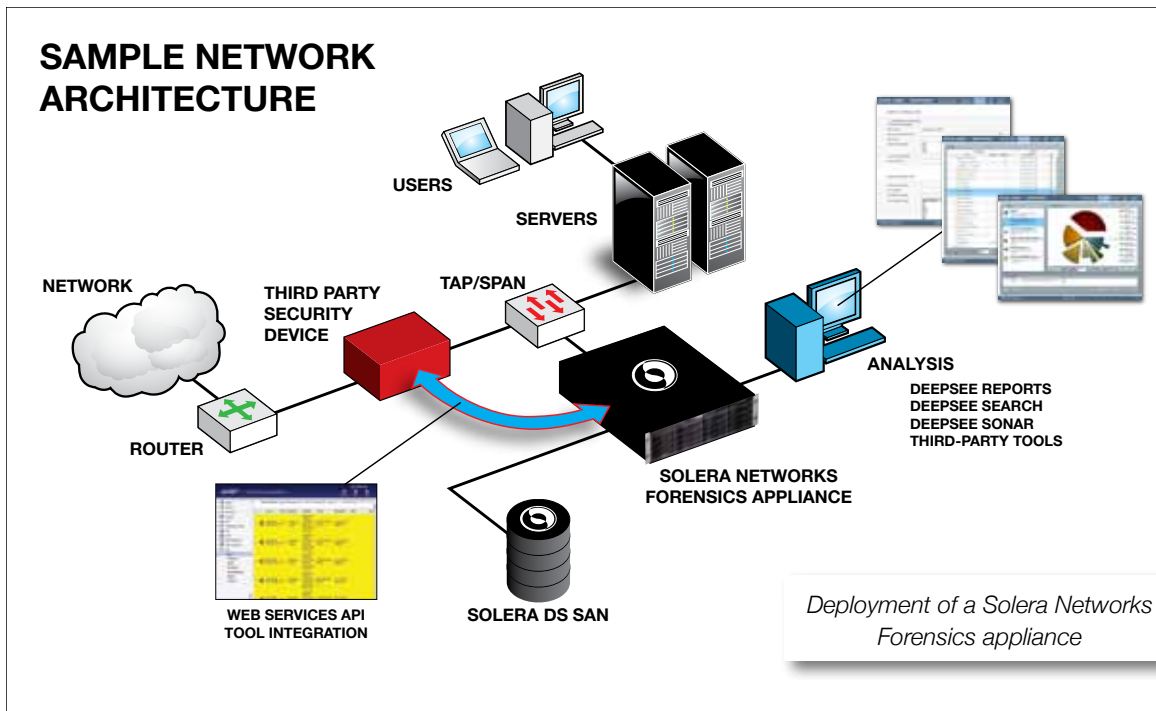
WEB SERVICES API

Through web services APIs, the network forensics solution from Solera Networks enables organizations to better leverage their existing security investments to address the vulnerabilities and security gaps in their network environment. With the web services APIs, a security solution can leverage third-party tools that trigger alerts, thereby adding context to those alerts by providing an accurate record of traffic relevant to the incident.

Additionally, only the Solera Networks solution improves the overall effectiveness of a broad array of network security technologies – including next-generation firewalls, IPS, DLP, SIEM and log management tools – by recording all network traffic at full line rate and then providing those tools access to a complete record of historical network traffic through the solution's open data access methodology. By providing access to a complete record of all traffic, instead of just captured samples, it provides the ability to determine the true scope and context of any network security event.

FLEXIBLE DEPLOYMENT

Active network forensics from Solera Networks can be deployed as a dedicated hardware appliance or a virtual appliance. It can even be deployed inside a virtual network comprised of intercommunicating virtual machines, enabling it to expose their



virtual traffic to external physical security tools for analysis. Regardless of the deployed method, the Solera Networks solution sits passively on the network via an available SPAN port on a switch or a network tap device such that it doesn't interfere with network traffic, remaining essentially invisible and non-detectable from the targeted network segment.

SWIFT, INTELLIGENT RESPONSE

The cost of a major security incident is rarely limited to the direct costs of the attack. Perpetrators often lurk on the network, waiting for the opportunity to strike again. However, without the full source and scope of any breach, organizations are handicapped at best, or blind at worst in their ability to remediate and protect against future attacks. Unfortunately, traditional security solutions can't provide full scope and source since they don't capture 100% of network traffic. This inability to respond in a complete and timely manner not only increases the direct costs of downtime, IT resources, and stolen data, but also increases the indirect costs associated with follow-on incidents, the impact on an organization's brand, and the need to remediate for the maximum potential scope.

Without a complete historical record of an incident, a solution can't typically provide the details needed for 100% remediation and attribution. It might get a response team 80% of the way there, but the last 20% of the unknowns can be costly, perhaps even causing the majority of the loss to the organization. Active network forensics from Solera Networks quickly uncovers those unknowns to enable swift, intelligent response to all security events. Security managers can rapidly determine the full context of what happened and can then rapidly remediate it to stop the threat and prevent any future damages or impact on operations. Finally, once the threat has passed and the security problem has been corrected, the Solera Networks platform replay functionality allows for a validation of the correction.

The difference before and after the deployment of the Solera Networks platform is comparable to the difference between an old-fashioned fire alarm and a modern security control panel with a continuous feed from sensors and cameras throughout an entire building. When an old-fashioned fire alarm goes off in a large building, it doesn't say where the fire is, what caused it, or what should be done about it. This is similarly true when alerts are sent out by traditional security products; such as firewalls, IDS, and UTM solutions. However, with the complete record of all network flows, active network forensics from Solera Networks makes it easy to find the breach, what caused it, and what needs to be done – just as a modern security system in a large building facilitates pinpointing the origins and cause of a fire.

To facilitate the swift, intelligent response needed when an event occurs, network forensics from Solera Networks enables organizations to quickly and accurately discover the cause and scope of what really happened by enabling them to easily:

- Search and find network flows of interest

- Drill down into the details of network flows
- Report on and visualize network flows
- Replay network flows and recreate artifacts
- Analyze network flows and artifacts
- Pinpoint the root causes of incidents and swiftly remediate
- Validate the remediation method by replaying the attack

SEARCH AND FIND NETWORK FLOWS OF INTEREST

Unlike complex analysis and forensic tools that require extensive knowledge of networking protocols and packet analysis

Name	Status	%	Artifacts	Created	Options
All artifacts from John Doe's IP	Finished	100%	129	10/14/2009 11:38:33	[Info] [Search] [Refresh] [Delete]
JPEG images	Finished	100%	723	10/14/2009 11:31:57	[Info] [Search] [Refresh] [Delete]
PDF's from 10.2.3.4	Finished	100%	0	10/14/2009 11:41:31	[Info] [Search] [Refresh] [Delete]
Word Documents	Finished	100%	141	10/14/2009 11:42:39	[Info] [Search] [Refresh] [Delete]

Simple searching and reconstruction of flow artifacts

methods, Solera DeepSee provides searching with web-like simplicity. As a result, anyone can search, locate and view actual network communications in the way they were originally delivered. Quick searches can be performed simply by entering keywords. To narrow results, more advanced searches can be performed by looking for text strings, time parameters, IP address, MAC addresses, TCP ports, VLAN tags, file types, hex values, hashes (MD5 or SHA1), and traffic type.

For example, a search can return all the traffic from a specific IP address for the past few days or weeks. Solera DeepSee can then take the returned collection of packets and reconstruct them into usable network flows that can be analyzed. It can identify any occurrence of well-known file types, (i.e., .jpg, .pdf, .doc, .exe, etc.) and carve them out of the network stream and reconstruct them into their native format. As a result, the file can be analyzed to determine if it contains any threat that might not have been detected by the organization's IPS, firewall or other prevention tools.

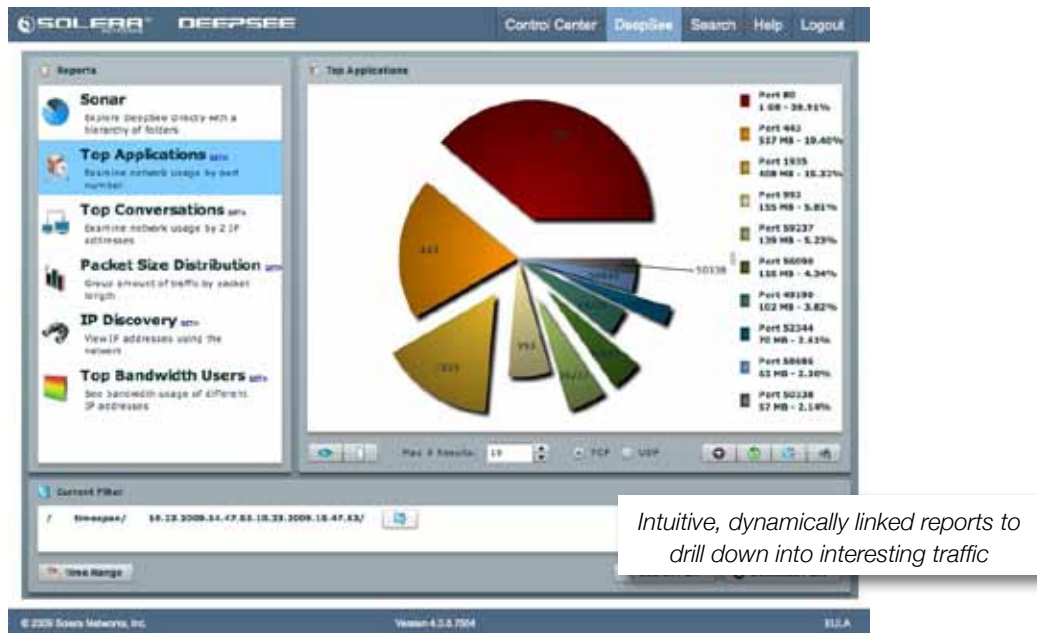
Artifact searches for specific file types can also be conducted. The search can be performed across all captured network traffic or narrowed down to search through a conversation between two specific computers during a specific window of time.

DISCOVER AND VISUALIZE NETWORK FLOWS

To help organizations swiftly and intelligently respond to network events, DeepSee Reports™ provides a variety of visual and

Interactive Graph to visualize captured traffic

highly interactive reports. The Interactive Graph from the solution's basic control center provides a graph-based view of network data patterns over time. It lets IT and security professionals dynamically dig into the peaks and valleys of their captured



network flows. Sections of the graphed network traffic can be highlighted for immediate playback, dragged into the Solera DeepSee Forensics suite for further discovery and analysis, or saved as a PCAP for analysis by other third-party analysis solutions.

In addition to the Interactive Graph, Solera DeepSee has a set of five different reports that let organizations quickly discover what is happening on their network.

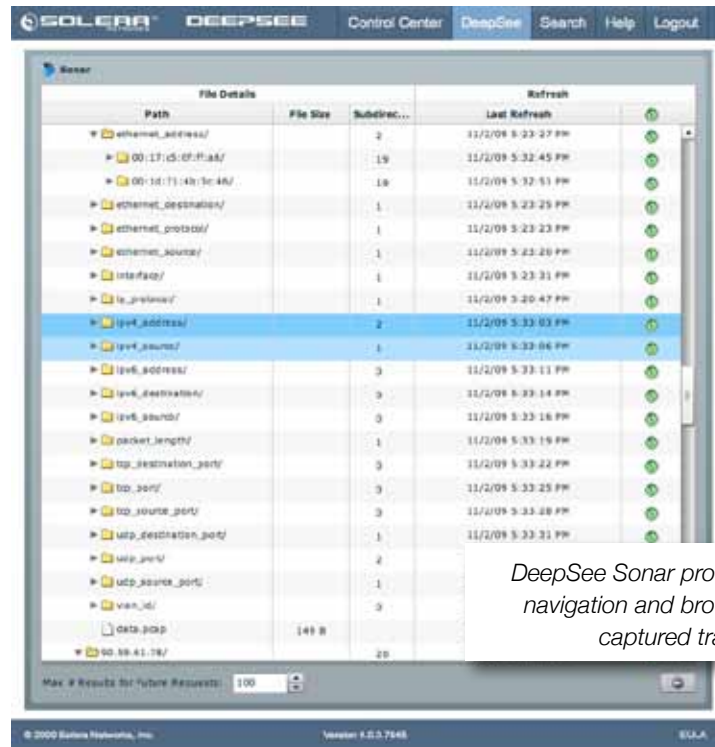
- Top Applications – A pie chart that displays the network services and applications comprising the largest percentage of captured network traffic
- Top Conversations – A pie chart that displays the bidirectional communications (“network conversations”) between two distinct IP addresses with the largest percentage of captured network traffic
- Packet Size Distribution – A bar graph that displays information about the packet sizes traversing the network, to discover anomalous packets crossing the network and help administrators optimize routers and switches to best support the most common types of communications
- IP Discovery – Displays IP address statistics that identify those addresses that consume network bandwidth outside of normal parameters
- Top Bandwidth Users – A line graph that displays the top network traffic producers by IP address to help identify traffic trends, as well as any irregular traffic patterns or spikes in network traffic

Each of these different DeepSee reports can provide a high-level view of events or they can utilize specific filter criteria to display low-level, finite results. Additionally, they can interact with each other to help administrators and managers drill down to the level of detail they need to find exactly what they’re looking for.

DRILL DOWN INTO THE DETAILS OF NETWORK FLOWS

DeepSee Sonar™ provides file-system navigation and granular access to all captured network data, allowing automated folder-based filtering and instant PCAP generation. It allows IT and security professionals to drill down into the captured traffic by a variety of parameters, including IPv4/IPv6 traffic, source or destination IP addresses, protocols, ports, and more. Such browsing is endlessly recursive.

For example, to review all captured traffic from a particular IP address a user simply browses to the appropriate folder for that IP address. To drill down further to more specific types of communication from that IP address to different targets, the user can browse through folders on specific IP addresses, TCP ports, VLANs, etc. Users can continue to browse down into the folder hierarchy until they’ve narrowed it down to the specific desired criteria. That data can then be used to reconstruct



an artifact, pulled into a DeepSee report for further analysis, or saved as a PCAP file to be used by other third-party PCAP analysis tools.

REPLAY NETWORK FLOWS AND RECREATE ARTIFACTS

In addition to using the Solera DeepSee Forensics Suite for discovering suspicious or interesting network flows, the forensics platform allows organizations to playback traffic for review. Traffic can be replayed at variable speeds, merged with other network data streams, or replayed to multiple applications and locations. These options give organizations the flexibility to use their existing network monitoring, data analysis, and forensic applications to conduct in-depth analysis of the flows – an analysis that utilizes a comprehensive record of all network traffic and payload contents, instead of just packet samples or headers. The options also allow organizations to validate that security fixes and other patches indeed resolve issues seen in earlier traffic.

Once the Solera Networks solution has captured a network traffic stream, it becomes immediately available for replay. The stream can be reviewed without impacting network speed or interrupting network performance, and without impacting the ongoing recording of the same network traffic stream. This provides near instantaneous data availability for analysis or forensics with zero impact on the production network.

As mentioned earlier, the solution also lets organizations completely reconstruct any artifacts of interest that they've found within their captured network flows, such as text, spreadsheets, images, PDFs, AVIs, MP3s, instant message conversations, and other files. This ability eliminates the guesswork in determining whether or not a network flow contained a threat. Instead of relying on incomplete information such as a packet's sending IP address, destination, or size, the Solera Networks solution recreates the flow and its artifacts to show exactly what it contained.

ANALYZE NETWORK FLOWS AND ARTIFACTS

The Solera Networks solution lets organizations take any captured network flow or reconstructed artifact and have it seamlessly analyzed using any third-party protocol analyzer, forensics tool or network management solution of their choice that utilizes industry standard formats. As a software-based solution, it doesn't require proprietary hardware, but has extensive flexibility in both portability and integration with existing infrastructure and toolkits. Since all captured data can be accessed through industry standard PCAP files, it is accessible to any application using libpcap or WinPcap. Further integration with third-party applications is available through the solution's web services APIs based on REST (Representational State Transfer).

SEE AN INCIDENT IN FULL CONTEXT AND RESPOND SWIFTLY

Network forensics from Solera Networks provides an unparalleled view of live network traffic and flow dynamics to help organizations pinpoint the root cause of a breach and respond swiftly. It provides a clear picture of what really happened during a security incident, delivering the complete context of events, as well as the complete network evidence needed to take the proper course of action. It includes the needed tools to quickly uncover the true cause of a network intrusion, outage, or data leak.

Solera Networks solutions provide contextual security information needed to reach the right conclusions in terms of:

- Attribution – From where and who is this coming from?
- Methods – How is the attack taking place? What can be done to stop it?
- Intent or motivation – What is the adversary trying to accomplish?
- Scope and impact – How severe is the damage? How much has been taken or compromised? Are seemingly unrelated network conversations actually part of the breach?
- Evidence – Can this information be used successfully in a prosecution?
- Experience and education – What can be learned from this event? How can network security be strengthened?
- Validation – Did a patch or updated IDS signature really close the security breach attack vector?

By capturing and presenting the full extent of an event and its associated damage, Solera Networks enables organizations to take swift and proper action based on facts, rather than guesswork.

BRINGING COMPLETE CONTEXTUAL INTELLIGENCE TO NETWORK SECURITY

Network security is no longer just about prevention. Attacks and breaches have happened, do happen, and will happen. Organizations need to be able to minimize the effects of these attacks through the swift, intelligent response provided by active network forensics from Solera Networks.

Solera Networks fills a critical gap in today's network security landscape. By capturing and indexing 100% of network packets through its active network forensics solution, organizations are provided with the full context needed to swiftly, intelligently and effectively respond to security events and prevent future attacks and ongoing costs, both direct and indirect. It enhances the value and effectiveness of an organization's existing security investments to provide a dynamic defense against unknown threats and to prevent breaches from escalating into costly, catastrophic events. It simplifies the arduous task of protecting information assets and mitigating risk, reducing the overall effort required to respond to new threats and attacks, and provides a way to validate security patches and other remediation through network replay. Solera Networks brings complete, contextual intelligence to network security, enabling organizations to discover what is really happening on their networks in a way that saves them time and money, while enhancing decision-making, responsiveness, and overall network security.

ABOUT SOLERA NETWORKS

Solera Networks' DS Series is a line of high-performance network forensics appliances, including software-only virtual appliances, which capture, record and archive 100% of network traffic at speeds up to 10Gbps. The data is then accessible instantly via Solera Networks' search, alert and archive interfaces, or via any standards-based security, forensics, compliance, analytics or network management application. For more information on Solera Networks, visit <http://www.soleranetworks.com>.