



WHITE PAPER

Negative Day Threat Detection™

Don't ask if or when a breach will occur. Ask: Are we ready to see, identify, stop, & remediate an intrusion?

NEGATIVE DAY THREAT DETECTION

History will repeat itself. This year will bring new attacks that will breach our networks in spite of the security we added last year. Fortunately, Negative Day Threat Detection allows organizations to see backwards in time (post-event identification) to quickly determine the scope of any breach, whether known or novel, allowing for efficient and timely remediation and fortification.

BEST SECURITY PRACTICES CAN DETER - BUT NOT PREVENT BREACHES

Gary McKinnon, an unemployed computer systems administrator from London amassed worldwide attention when he successfully hacked into the Pentagon's computer networks in 2002. Following this and other incidents, the Department of Defense spent billions of dollars upgrading the security of the Pentagon's networks.

However, in spite of the billion dollar security upgrades, the Pentagon's networks have continued to be penetrated. In June 2007 a major network intrusion occurred and a significant amount of sensitive data was stolen. The effected network was shut down for three weeks and the recovery cost was over \$4 million dollars. With the updated and "best practice" security measures in place at the time of the attack, Dennis Clem, the Pentagon's CIO and 25 year IT security veteran, didn't think the Pentagon's network was as vulnerable to attack as it was. "This was something that [I thought] would never happen to me," he said. "Boy, was I wrong".¹

A very significant lesson was learned from the June 2007 attack and the subsequent vulnerability assessments and security strengthening. Even with the best practice security measures in place, information networks will always be vulnerable. "Best practices" are great guidelines, but they don't address the unique circumstances and vulnerabilities every network is bound to have. Clem summed it up with this caution: "Even the best intrusion detection program can't stop all of the network breaches."

These cautionary words from Clem in 2007 proved prophetic. Extraordinary new security countermeasures were implemented in 2008, yet in April 2009 it was revealed that spies had again broken into the Pentagon's networks. This time it was the \$300 billion dollar F-35 Lightning Joint Strike Fighter project, the Defense Department's costliest weapons program ever.² The intruders were able to copy and siphon off several terabytes of data related to the fighter's design and electronic systems. The Defense Department spends \$2 billion a year on computer-network security, but nevertheless remains hugely vulnerable to cyber-attacks, says Deputy Defense Secretary Gordon England.³

¹ Federal Computer Week, *OSD CIO: Network configuration, scanning softened cyberattack blow*, Mar 26 2008

² The Wall Street Journal, *Computer Spies Breach Fighter-Jet Project*, April 21, 2009

³ Washington Pulse, Dec 2006, *US Troops Vulnerable to Enemy Drones*

Of course, it's not just the Pentagon that's penetrated. The Department of Homeland Security reported that federal government agencies experienced 18,050 cybersecurity breaches in fiscal 2008⁴. Even the White House computers have been compromised.⁵

Companies in the public sector with best practice security measures in place are also infiltrated. The number of recent incidents are too numerous to detail here, but two poignant examples illustrate the issue. Hannaford Brothers was breached in March of 2008 and 4.2 million credit card accounts were compromised, even though Hannaford was compliant with PCI DSS (Payment Card Industry Data Security Standards) at the time.⁶ Likewise, Heartland Payment Systems was also PCI DSS compliant, yet it was revealed in Jan 2009 that they were also successfully attacked and financial data from as many as 100 million accounts were stolen.⁷

As these and numerous other cases show, having strong security in place may deter most network attacks, but they will not prevent all of them from succeeding. Organizations that are exhausting huge budgets and paying a lot of attention to security will still fall victim to attack. It's just a matter of time.

HISTORY WILL REPEAT ITSELF

Throughout the history of the Internet and even closed networks, a constantly repeating cycle of *be attacked then react* has been evident. Essentially all large organizations are attacked by a particular category of assaults. Defenses to that category of attacks are then created and installed. This is followed by a different category of attack and the cycle repeats itself. While the categories and specific attack methods change, the cycle does not – it's a constantly repeating sequence of being compromised, and then reacting.

To illustrate this cycle, consider the following. A large, successful, and security conscientious financial organization that asked not to be identified, was successfully attacked by every one of the methods listed below. After each attack, security measures were diligently implemented to resist and hopefully prevent that type of attack from happening again. Not being at liberty to disclose the identity of the company, please substitute the name of any large organization and it will likely be an identical or at least a very similar story.

This is a somewhat simplified list of attack types, and the time periods are general in nature, but you will get the idea. The company was penetrated by every one of these attack categories.

<u>Beginning Time Period</u>	<u>Attack Type or Security Threats</u>
1986	Numerous Traditional Computer Virus Attacks

⁴ The Wall Street Journal, *Computer Spies Breach Fighter-Jet Project*, April 21, 2009

⁵ Fox News, *Chinese Hackers Penetrate White House Computers*, November 07, 2008

⁶ Huliq News, *Does Hannaford Hack Suggest PCI Standards are Flawed?* Feb 9, 2009

⁷ Washington Post, *Payment Processor Breach May Be Largest Ever*, Jan 20, 2009

1988	Worm – The Morris worm, ILoveYou, & others
1996	Employee abuse of external websites
2000	Trojans – Barok, Beast, Optix, Graybird, & others.
2000	Spyware – Thousands of instances
2001	Adware – Thousands of instances
2001	Email SPAM – Ongoing battle
2002	SQL Injection – Multiple instances
2002	Application Level Attacks – Multiple instances
2003	Phishing / whaling – Thousands of instances
2003	Wireless attacks
2004	Insider Data Theft
2005	Instant Messaging Abuse
2006	Botnets – Multiple instances
2007	Virtualization Attacks
2008	XSS Cross-Site Scripting

As shown above, this be attacked and react cycle repeated itself with a different flavor of attacks and reactions, but the cycle and process has been largely the same each time. That cycle is:

1. Update safeguards to defend against as many known threats as is practical
2. Succumb to an attack that hadn't been anticipated
3. Implement safeguards for the new attack
4. Repeat this cycle over and over again

All large organizations will fall victim to some level of attacks, regardless of security measures that are in place. Most midsize organizations will also become victims, and a significant number of small organizations will also experience security breaches.

Most of the attacks at this organization were relatively minor in nature, but a few of them caused extensive damages, with each resulting in tens of millions of dollars in losses.

While it's impossible to know which attacks will succeed in the future, or which ones will be small and which ones will be big or even huge, there is one thing that is certain: history will repeat itself. The next year will bring a new round of attacks and in spite of the security that will have been added to deal with last year's attacks, some of the new attacks will be successful and compromise the network and information systems.

WHY MOST NETWORKS WILL CONTINUE TO BE PENETRATED

Why is it that cyber thieves continue to be successful, even when attacking organizations with the latest and greatest security defenses in place? There are a number of reasons. First of all, large networks may have thousands, if not tens of thousands of vulnerabilities. Network defenders have the task of

strengthening and guarding every one of these weaknesses, many of which are not even visible or known. Intruders on the other hand, only need to find a single vulnerability. With a seemingly endless number of attackers constantly attempting to invade, the defenses are all too often overwhelmed.

Additionally, every new technology, application, or network node that is added exponentially increases the difficulty to secure the system as a whole. Consider the task of supplying an armed guard on flights between two cities – Chicago and New York. This could be achieved by supplying two guards - one on the Chicago to New York plane, and one on the New York to Chicago plane. However if a third city is added, say San Francisco, it will now take 6 guards to secure all possible destinations, not three as one may initially suppose. Add a fourth city and 12 guards are needed. The security requirements increase exponentially when new elements are added. The same is true in the digital world. Security becomes more difficult every year as our networks grow in size and sophistication.

Furthermore, attacks are created and evolve quicker than defense mechanisms. Security countermeasures are written to software engineering standards and must be carefully designed and tested to ensure compatibility and that they have no undesired consequences. Creating a new security product will generally take a year or longer. Not so with malware or other intrusion approaches. Cyber criminals write quick and dirty code.

In today's setting, attackers are driven by incentives that often surpass the salary and compensation available to the IT security community. The rewards offered for breaking into a significant target can raise the status of an impoverished person to that of high society. Foreign governments allegedly pay to educate participants in the latest technical advances. Ironically it's usually done in the best universities and most advanced enterprises in the United States. Organized crime offers cars, homes, and large sums of money for successful hackers. With the dark side compensating on this type of scale, the attackers are keeping pace with, and in too many cases surpassing on the IT security community.

Finally, human weaknesses and mistakes account for a large portion of security incidents. Accidental breach in policy, misconfigurations, and social engineering attacks are all common occurrences. Advances in technology will help some of these human issues, but not all.

A PARADIGM SHIFT – NEGATIVE DAY THREAT DETECTION

Given the cold reality that most organizations will continue to be penetrated by hackers and cyber thieves, it's time to dramatically alter our approach to security. We should not be asking if or when a breach will occur, instead, **we must ask: Are we ready to see, identify, stop, and remediate an inevitable intrusion?** This is a significant paradigm shift from most present day thinking, and the answer to this question is typically some version of: "No. It's difficult to stop and remediate something you can't see or identify."

Certainly we need to continue doing what we have been doing - using anti virus, encryption, strong authentication techniques, firewalls, intrusion detection/preventions systems, patch management, and related products. These are excellent and necessary tools that address *known* vulnerabilities and attack exploits that we can see and understand because they have been classified. But we must also dramatically improve our capabilities to see, identify, stop, and remediate new *unknown vulnerabilities and exploits*. These are the attacks that we don't know to look for until after they have inflicted their initial damage.

This requires moving upstream in the lifecycle of an attack. Doing so focuses on what happens *prior* to day zero, when a vulnerability is first discovered, or prior to the availability of a patch. Performing this *negative day* analysis is critical in order to understand the source, nature, and extent of potential or actual attacks. This approach addresses the *unknown unknowns* rather than continuing to focus solely on technologies dependent on classification of *known* attacks. Examining these "negative days" provide critical information making it much easier to see, identify, remediate, and ultimately fortify against emerging threats.

Like a camera at a bank that captures and records everyone entering the institution, *Negative Day Threat Detection* utilizes digital strategies and technology to continuously record network traffic including packet header and payload. This creates an historical record of all network traffic that transpired over a specified time period. Security analysts can move backwards in time from a given incident or moment and replay and analyze everything that occurred.

The lifecycle of an exploit

To better understand Negative Day Threat Detection, consider the various phases an attack passes through as it is created, launched, and ultimately brought under control. During the first six phases of an exploit's life cycle, organizations are vulnerable to being successfully infiltrated. Unless organizations have the ability to examine what happened during these *negative days*, they have no way of knowing that they have been compromised.

1. Creation phase. Vulnerability discovered by attacker - exploit(s) created and unleashed.
2. Unknown phase. This is a new attack. There are no profiles or signatures to identify it so it slips past existing security measures. The Attack is successfully installed and spreading. It's ready to trigger or begins operating without detection.
3. Discovery phase. At some point suspicious activity is detected. Victims sense something may be wrong. They don't yet understand if this is a false positive that can be ignored or something serious.
4. Analysis phase. Victims realize a serious attack is either underway, or is probably underway. Large organizations under attack begin working to

discover what is wrong. At some point they start getting enough evidence to determine what is going on, or at least have a plausible theory.

5. Solution phase. Security vendors and application or operating system vendors are alerted and become aware of the vulnerability. One or more signatures and patches are developed, tested, announced and distributed.
6. Aftershocks. Other criminals learn of the vulnerabilities from the announcement and patch release. New attacks are created to take advantage of un-patched machines, with each new threat spawning lifecycles of their own.
7. Mitigation phase. Organizations begin to deploy the security patch. The attack stops spreading to systems that have been patched.
8. Uncontested phase. Attacks continue to spread to un-patched systems.
9. Undetected phase. Depending on the sophistication of the attack and the strength of the patch, systems infected before the patch was released may not be detected and could still be under attack for some period of time.
10. Controlled phase. The attack fades over time as the patches and new security measures are applied and maintained.

To see why Negative Day Threat Detection is so powerful, contemplate the following example. One version of Sun Microsystems' implementation of PAM (Pluggable Authentication Module), which is used to provide enhanced user authentication, had a serious security flaw. This severe weakness existed for some time until a patch was available. The flawed PAM module performed insufficient bounds checking of arguments, and a specially crafted logon request would overflow a buffer and allow an unauthorized user to gain root access to the system. Since this vulnerability could be exploited using authorized protocols and methods, an attack would not normally be detected by anti virus technologies, firewalls, authentication systems, intrusion detection systems or other traditional security measures.

With root access an attacker has the highest level of privileges available, and he or she will have unrestricted access to all functions of the operating system. With root privileges, an attacker can create additional privileged user accounts, install Trojans, spyware, botnets, or other malware and modify system logs to cover their tracks.

When this security flaw was discovered, Sun Microsystems immediately created and distributed an update that closed the security hole. Once the patch was applied PAM no longer granted root privileges to attackers.

Now, think about a scenario where a remote cyber criminal exploited this vulnerability and gained root privileges on a number of servers within a large enterprise. Using root authority, a dozen new privileged accounts were created on the compromised servers and a sophisticated system of malware was secretly installed. This network of malware included numerous altered system files that captured credit card data and other sensitive information while transactions were being processed. The stolen data was temporarily stored in

obscure encrypted files that were later retrieved using the company's VPN and one of the user accounts created by the attacker. System files were cleverly altered to hide the various activities.

Additionally, let's imagine a large botnet was established on a different set of compromised servers. This system of botnets utilized user accounts and processes that were completely unrelated to the data theft operation described above. These botnets were part of a large sophisticated SPAM operation involved in illegal activities that would be extremely embarrassing and damaging to the enterprise.

Let's further envision that it was some other organization that discovered the PAM security flaw and reported it to Sun Microsystems.

Here's the scenario that would take place if the enterprise were not performing Negative Day Threat Detection. When they learned of the vulnerability from Sun's announcement and received the patch, the only thing they would know, or even could know, is that prior to applying the patch - their systems were vulnerable to an attack. They would have no idea that they had actually been breached, that multiple systems had been compromised, or that the attacks were still successfully operating. The enterprise would simply apply the patch and move on to other duties. It would be a routine day, no different than what takes place on any other Patch Tuesday. It would take some event, or perhaps multiple events before the enterprise would discover that they had been seriously breached. Because the botnet was not obviously associated with the credit card attack, they would both need to be discovered independently.

However, if the enterprise had the capability of recording and later analyzing all network traffic, they could quickly and effectively analyze historical network traffic and perform Negative Day Threat Detection. In this case a completely different scenario would occur. Upon receipt of the announcement and vulnerability description, the security staff would replay or scan the previously recorded network traffic and see if the logon parameter that caused the security breach ever traversed their network.

Upon running this exercise, the security staff in our example would have immediately seen that they had indeed been attacked by someone exploiting this vulnerability. Armed with this information, they could easily identify the source IP address used by the attacker during the initial assault. The entire session could then be observed and the security staff could watch everything the attacker did. Every character typed, every command he executed, and the security staff would see every process that was started. Within a few minutes, the new accounts setup by the attacker would be known. With this information, the security staff could set filters and replay the network traffic and watch every logon and session in their entirety that used those accounts.

With the data available during the negative day analysis, the security staff would likely have been able to see, identify, stop, and remediate both the credit card attack and the botnets within a few hours. It would have also made it much easier to fortify the network against similar future attacks. Additionally, the available data would make it a great deal simpler to identify the attacker(s) and bring them to justice.

SOLERA NETWORKS – ENABLING NEGATIVE DAY THREAT DETECTION

Solera Networks provides solutions that enable Negative Day Threat Detection and historical network traffic analysis. The company's products can capture and store all network traffic at up to 10Gbps speeds. It's like having a security camera and tape, or DVR for your network except that every channel and every program is recorded, all the time. This data can be later replayed or analyzed, providing complete visibility into what happened in the past.

Solera Networks' flagship product is the DS Series, a line of high-performance network forensics appliances, including software-only virtual appliances that capture, record, search and archive 100% of network traffic at speeds up to 10Gbps. DS appliances sit passively on the network, undetected, and don't impact the performance of the network in any way.

Captured traffic is accessible via Solera Networks' proprietary search, alert and archive interface, or via any standards-based security, forensics, compliance, analytics or network management application - including all open-source tools. These applications can then perform their analysis on either live or captured traffic using Solera Networks' extensive filtering language, all without affecting the production network's performance.

Solera OS is powerful and flexible enough to capture traffic at 10Gbps with microsecond time-stamping granularity, and is capable of addressing very large storage partitions (in excess of 576 TBs). As the hardware capture speeds increase and storage capabilities expand in the future, the Solera OS can scale to take advantage of these improvements. Additionally, the Solera Capture Stack™ provides an open architecture and available web services APIs so any security, management or network analysis tools can automatically gain access to the captured traffic to add context to any alert that may be delivered.

SUMMARY CONCLUSIONS

Prior to the advent of surveillance cameras to protect buildings and physical facilities, criminals could perpetrate their crimes with relative ease. They could scope out a target and study it on the weekend or after hours with little fear of raising suspicion. By simply putting on a pair of gloves they could enter a building, quickly burglarize it, and depart with virtually no trace. An alarm may sound, but this only told the owners that they had already been victimized. Without *eye witnesses*, investigators would have very little to go on and the crime was often unsolved.

Today, surveillance cameras are among the most fundamental and important security devices that can be installed to protect a building or physical facility. Countless burglaries and other crimes are prevented by the very presence of a security camera. When crimes do occur, investigators can study the characters

involved and the procedures they used. This helps solve the crime and protect against similar future episodes.

Until recently, the equivalent of a surveillance camera for our digital networks didn't exist. The technology simply wasn't available to capture network traffic fast enough, or to store it in a cost effective manner. As a result, cyber criminals have been perpetrating their digital crimes with relative ease and leaving little or no trace.

Fortunately, technology and products such as Solera Networks' now make it possible to deploy a digital security camera and capture and replay everything that happens on the network. A twenty-four hour, seven days a week eye witness with perfect eyesight and memory. The benefits of this eyewitness however go well beyond providing testimony in court to convict the attackers. As this technology is deployed and becomes known, it should deter cyber criminals just as a physical security camera discourages crime. Attacks that do occur will be detected earlier and contained faster. Furthermore, everything the attacker does will be known. There will be no guesswork about what was stolen or compromised.

About Solera Networks

Solera Networks develops high-speed network forensics solutions for both physical and virtual networks. These solutions are unmatched in speed and scalability – capturing, indexing, searching, and replaying all network traffic, even in 10Gb environments. The Solera Networks architecture provides open platform interoperability, extensible storage, and portability. These capabilities enable security professionals to quickly identify the source of any attack, remediate, and fortify against further risk.

Solera Networks Headquarters
10713 South Jordan Gateway
Suite 100
South Jordan, Utah 84095

1 877-5SOLERA or 877-576-5372
1+ 801-545-4100
1+ 801-545-4040 fax

Email: info@soleranetworks.com