The Art of Layered Security

Data Protection in a Threatscape of Modern Malware

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

Abstract

Threats to theft of Intellectual Property, financial data, Cardholder Data, and PII (Personally Identifiable Information) are more diverse and increasingly difficult to defend against. The traditional 'internet vandalism' from viruses is still an issue, but the 'threatscape' in 2019 is far more diverse and dangerous than ever before.

Not only is it becoming more difficult to protect your confidential data, but more important too.

Your enterprise is under attack right now and if a breach is successful, you could lose your Intellectual Property, your sensitive company planning and financial data, your market intelligence and with it, your overall competitive edge could be setback by years.

But this could be the best case scenario. If you lose cardholder data or customer personal information, not only would you be left with the costs of financial compensation and system repairs to be paid, but with your brand value and company reputation severely damaged.

The 2019 Threatscape - Modern Malware in 2019

Modern Malware - The Headlines

- ***Ransomware -*** a stable attack vector for cyber criminals, and year after year continues to be the biggest malware threat
- ***Trojans and Viruses*** - are still 'in the wild' and pose a renewed threat when combined with social engineering techniques for distribution - AV systems will never be 100% effective against even known malware whilst 'zero day threats' i.e. previously unknown malware are never ending.
- ***Phishing Attacks -*** bypass firewalls, Intrusion Protection Systems and Anti-Virus by Users unwittingly welcoming in malware.
- ***Vulnerability Exploits -*** year after year when the Top Ten of security breaches is published, straightforward Cross-Site Scripting (XSS) and SQL Injection exploits of Web applications are always at or near the top of the list.
- ***Insider Threats -*** by definition, bypass even the best firewalls, Intrusion Protection Systems and Anti-Virus defenses. Clearly there is a big advantage of being inside the firewall, but when the attacker has Admin rights to key systems, a different approach to data protection is needed.
- ***The Advanced Persistent Threat (APT) -*** the best orchestrated 'professional' attacks play the long game. The classic APT is run as a tactical campaign over a prolonged period of several months as a progressive hack. The APT typically originates with a phishing attack (in the case of the APT, a 'spear phishing' attack, being carefully targeted) or 'Inside Man' to implant spyware, which can then be used as a vector to hack deeper into systems and steal data over a period of months.

Silver Bullets or Magic Bullets for Security?

The truth is that there is no such thing as '***the*** best security defense measure'. The range of threats in terms of sophistication and anatomy used in conjunction with dirty tricks and cunning mean that we also need to similarly harness and blend all security measures at our disposal. Essentially the range of measures can be summarized as

> *In the first quarter of 2018 alone, nearly 2,296,830 new malware types were identified.*

- ***Firewall and IPS*** (Intrusion Protection System) use rules and attack-signature recognition to block attacks
- ***Anti Virus*** uses a dictionary of file signatures to block and remove malware
- ***Best Practice Security Procedures*** such as hardening, change control, user account management, patching, and physical security
- ***DLP*** (Data Leakage Prevention) works by blocking data export functions such as USB ports, DVD writers, and other transfer mechanisms for copying data
- ***Encryption and Tokenization*** render data unusable in different ways - encryption 'scrambles' data to make it unreadable on any device not authorized to use it, while tokenization 'translates' data into a token, with the resulting tokens meaningless unless used in conjunction with the tokenized data store
- ***White listing*** blocks any processes not pre-authorized from running on a system, good for preventing virus and trojan malware
- ***SIEM*** (Security Incident and Event Management) provides analysis and correlation of all system event log activity in order to identify irregular or unusual activity
- ***FIM*** (File Integrity Monitoring) detects any file system activity affecting system/program files, and any configuration changes that may affect security

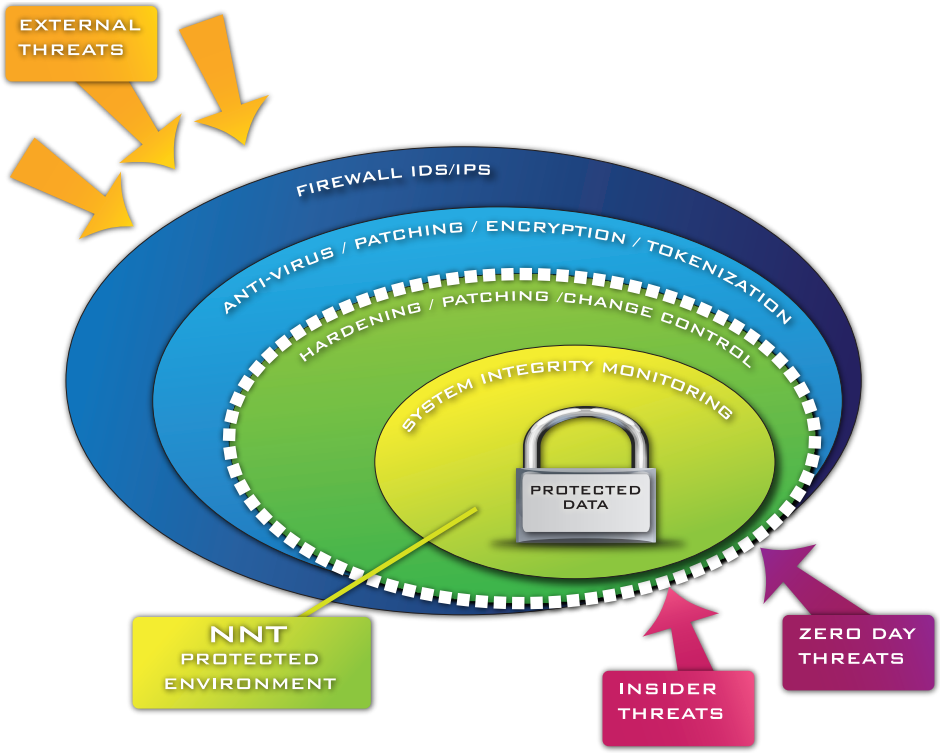

Figure 1: The Art of Layered Security - security measures need to be varied and layered to provide an effective defense to your organization's confidential data

*'But **OUR** Security Isn't Weak?'*

> *The number one threat to security is complacency...*Once you come to terms with the reality that your organization is constantly under threat...you are beginning to practise *The Art of Layered Security*

The multi-billion dollar security technology market is always going to be rife with reassuring claims that 'Appliance X' will 'fully' protect you whilst 'Technology Y' has so much intelligence it can spot a piece of malware within a nanosecond of it hitting your network. They all work well and will defend your data 24/7 - apart from the threats they don't cater for.

For example, there is a new wave in real-time sandbox technology which exploits the higher power processing appliance platforms now available. The concept is sound - assume that all incoming data is potentially unsafe, and before any of it hits your internal network, intercept and analyze its behavior in a safe sandbox environment. It's the equivalent of taking a biopsy and cultivating a culture to see what pathogens exist - but doing it in milliseconds. The theory is good as a way of detecting zero day malware, but you wouldn't stop using anti-virus technology on servers and desktops, because malware can be introduced via other means, not least because laptops leave the corporate network and the protection of the sandbox technology. And what about new generation malware that is able to evade the sandbox, or that is deliberately introduced by an 'Inside Man' with Administrator privileges to do so?

In summary, great idea and great technology implementations are available, but is it the only security measure you'll ever need? Of course not! As we have already highlighted, 'Inside Man' threats exist and any other trusted employee can import malware knowingly (or unknowingly).

The Number One Threat to any Organization's Security?

Complacency - but before you go and check whether your AV package can detect this new polymorphous-worm, we are referring to an organizations' attitude to security rather than any malware. Before you can take action to defend your organization you first need to come to terms with the inescapable fact that it is under constant and unpredictable threats of attack.

There are three key questions to ask yourself on a regular basis:

- ***'What does each of my security measures provide protection for?'***
- ***'Where are the gaps in my security layers?'***

And most crucially if we are to avoid the biggest threat of complacency

- ***'What are my checks and balances? How do I validate that security measures are effective?'***

To get an honest, self-assessment of your organization's security posture can be difficult as the security threatscape is always changing, so getting accurate answers to the first of these two questions is harder than it seems.

If you have a firewall and you have a brand-leader anti-virus package then you have defenses against the large proportion of everyday threats, but as in our opening summary of Modern Malware, these measures alone are only partial defenses, especially when you consider your defenses against Inside Man threats, which may not actually utilize any form of malware.

The Number One Threat to any Organization's Security? Continued

Therefore, the best additional security measure you can implement is to be on your guard. This may sound like a government-sponsored anti-terrorism poster slogan, but when we are trying to defend against threats that can come from any direction, and take any form, then we need to know about anything unusual and irregular happening on our systems that may render the system more prone to attack.

Being vigilant at all times, not just when an audit is due, is a habit that needs to be adopted. Once you come to terms with the reality that your organization is under threat constantly, both from external and internal attacks, and that your technological protection may not always be effective at preventing these, then you are beginning to practice The Art of Layered Security.

The Art of Layered Security

With attacks becoming phased and layered in order to evade malware protection measures in a progressive, step by step iterative attack, we need a security strategy that is also layered.

The Art of Layered Security means combining different security technologies in order that all possible avenues of attack are blocked or, where prevention is not an option, ensuring that threats are always detected.

This approach to security requires technologies to be 'hedged'. The philosophy needed is an assumption that any layer of defense has at least some weaknesses or blindspots. Once weaknesses have been evaluated, other measures can then be selected that will compensate. But this isn't all about buying malware-detection/blocking technology.Bringing us back to the anti-complacency measure, vigilance. Given that we are going to need to be capable of detecting malware and user activities that may be very subtle and trying to avoid detection, we will need to utilize highly sensitive monitoring capabilities. Being highly sensitive will mean lots of false positives, so we will need to deploy the monitoring in a focused manner and make it highly intelligent and automated. Hence the use of the term 'Art' - there is a need to be creative and pragmatic in terms of enforcing security within the context of your organization and its risk of attack.

It will also require our regular activities to become more controlled - for instance, if patches are being applied at any time to any server by anyone, then it will be impossible to distinguish between a legitimate maintenance task and a malware infiltration. This is why change management/change control is such a vital part of any security policy.

The two key metrics to monitor in order to confirm that change control is being observed are file system/configuration file changes and system access. In a well-managed environment with tight change control, there should only be one period of system access and file changes every month during Patch Thursday. At all other times, systems should be isolated and change-free.

Therefore we need an additional two key security layers which combine to give all the checks and balances we need at a forensic level, namely File Integrity Monitoring and System Event Log Analysis.

File Integrity Monitoring and System Event Log/Audit Trail Analysis

These two technologies work together to provide the ultimate forensic-level detail of activities on a server (or laptop, appliance, desktop, firewall etc). File Integrity Monitoring serves to record any changes to the file system i.e. core operating system files or program components, and the systems' configuration settings i.e. user accounts, password policy, services, installed software, management and monitoring functions, etc.

The beauty of FIM as a security measure is two-fold. Firstly, it is utterly comprehensive in detecting any changes to the file system and configuration settings. Secondly, particularly in the case of system or program file changes, it makes no assumptions as to whether the changes are good or bad. This makes it an infallible tool for identifying malware, detecting even the most subtle change to a file (as with a Trojan impersonating a genuine system file, for example). For this reason it brings the need for tight change management procedures to be observed, although of course, change management is a must in order to govern system security anyway.

FIM should be used as a means of verifying that only planned and expected changes are made to devices so that any unplanned change is treated as a potential security threat.Contemporary 'state of the art' FIM technology allows for precise focusing on file types and specific paths to monitor so that only changes to files that shouldn't change are detected. For example, image files on a website may change regularly but pose no potential security risk so can be excluded from the FIM policy.

Figure 2: FIM (File Integrity Monitoring) works closely in conjunction with Event Log Analysis (SIEM) to provide essential 'checks and balances' that security is being maintained, and that critical procedures such as Change and Configuration Management (CCM) are being operated correctly

Similarly, significant configuration file changes need to be recorded in case the security of the component - server, firewall, router, EPoS device etc - is weakened. Unix and Linux platforms are straightforward in that security settings are governed by text-based configuration files. Similarly firewalls and other network appliances will typically expose their configuration settings via a TFTP export or through interrogation via an SSH session. Windows servers pose more of a problem due to security settings being governed by a range of registry keys, Local Security Policy, file system controls, Installed Programs and updates, service startup and running states, and actual processes running on the server. This requires a specialized agent in order to efficiently monitor all these attributes in real-time against a policy.

File Integrity Monitoring and System Event Log/Audit Trail Analysis Continued

System Event Log or Audit Trail analysis provides a further 'check and balance' to record all user activity within the protected IT estate. Again this is ideally used in conjunction with tight change control procedures so that any access to a device outside of a planned change window should be treated as a potential breach. Gathering a full audit trail of user activity also allows for an 'after the event' W5 (who, what, when, where, and why) forensic reconstruction of user activity.

In this way, FIM and Event Log Analysis provide both an advance warning system for any potential security threats, and also a means of deterring Inside Man threats - a System Administrator may well have access rights to some confidential data on the network by virtue of their privileges, but if they know their activities will be detected and recorded then there is no future in data theft.

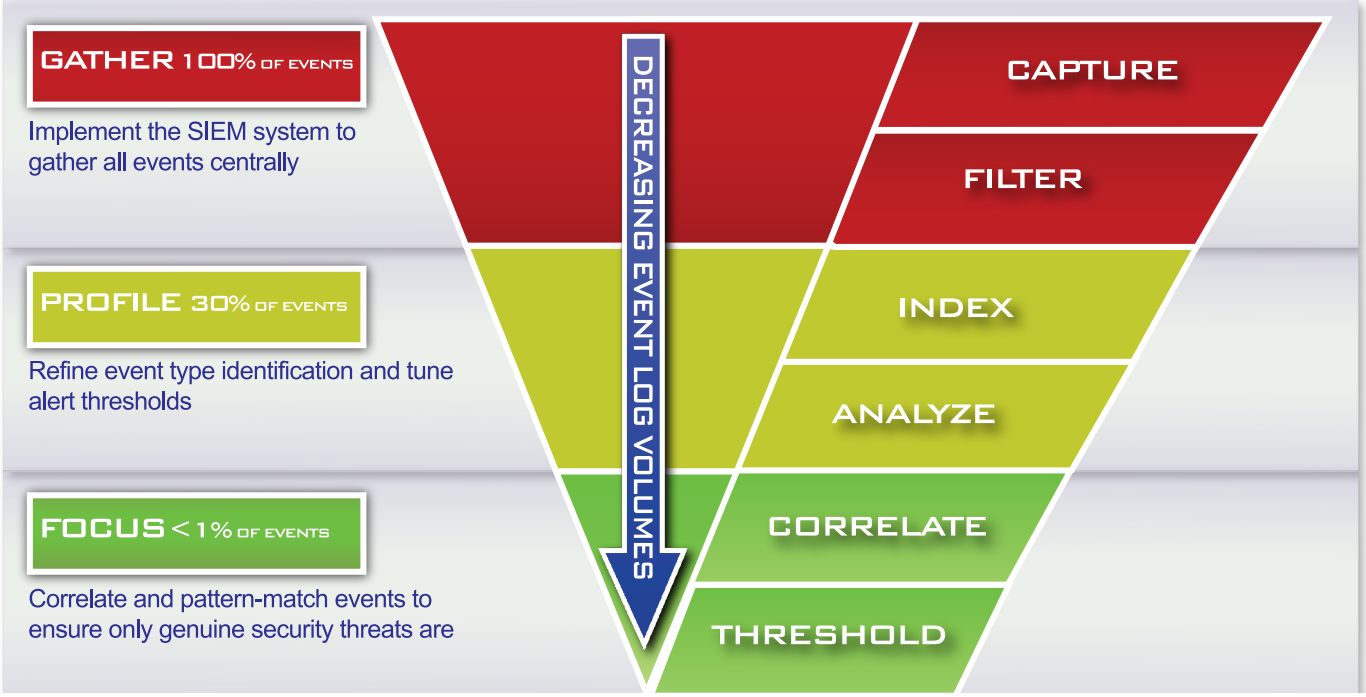

Figure 3: Event Log Analysis (SIEM) must intelligently correlate events from all servers and network security appliances in order to automatically detect unusual or irregular activity symptomatic of potential security breaches

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.