Bloor

White Paper

White Paper by Bloor
Author **Fran Howarth**
Publish date **November 2014**

The need for active response to advanced threats

...passive remediation is insufficient

Today's advanced attacks are increasingly pernicious, with attackers looking to bury deeply into networks so that they can carry out their deeds over long time periods. Organisations need to be proactive in seeking out incidents that have occurred and in actively removing threats.

Author **Fran Howarth**

Executive summary

Security breaches are inevitable. Attackers are becoming ever more sophisticated, using a complex array of tools, techniques and procedures to get past defences.

For any organisation, it is no longer if, but when and how often it will suffer a security breach. The consequences are often far-reaching and highly damaging.

Organisations can no longer rely on outdated methods for protecting themselves, such as ones that can only prevent threats that have previously been seen and for which countermeasures such as static signatures have been published. They need to move from reactive techniques to a more proactive stance of detecting what malicious exploits are on their networks. Then they must move to remediate them in a comprehensive manner.

This means not just containing threats and incidents but actually removing those threats. Given the volume of threats faced, the widespread propagation of attacks across networks and the massive quantity of alerts raised by security incidents, threat removal must be automated. Manual techniques are costly, time consuming and simply insufficient for today's dynamic, pernicious threat landscape.

This document discusses why automation is essential in the fight against sophisticated, relentless attacks. It describes what organisations should look for in selecting a technology platform that can not only ensure all threats are entirely mitigated, but also future-proof their organisation against attacks that are bound to occur.

"This means not just containing threats and incidents but actually removing those threats."

Fast facts

- Organisations need to move from treating incidents in isolation to continuous response to security threats through effective monitoring, big data analysis and detailed threat intelligence capabilities. Automation is essential.
- Security platforms that analyse events captured from throughout the network provide the visibility and actionable intelligence required to detect and mitigate threats.
- Only by automatically removing threats can disruption be minimised, systems returned to good working order and attackers thwarted.
- Yet full automation is a journey. Organisations should look for a vendor that offers policy-based mitigation with built-in checks and full validation of the efficacy of actions taken.

The bottom line

Through a combination of big data analytics, covering data collected from throughout the network, with the latest threat intelligence and an extensive library of indicators of compromise, organisations are better able to determine the extent and criticality of incidents and attacks and therefore can more easily determine the best countermeasures to use.

Rather than just containing threats to limit their effect, which can have the unfortunate outcome of the network being re-infected, a strategy of actually removing the threats is to be preferred.

Through behavioural analysis techniques, security platforms that support automated threat removal are able to automatically configure alerts for new activity that is seen, thus future-proofing the business against similar attacks in the future.

Why continuous response is becoming more important

Assume adversaries will get in

No organisation is an island. To be competitive, any organisation needs to invest in an online presence to reach out to customers, mobile technology to encourage productivity and flexible ways of working, and many make use of cloud-based applications and services for reasons that include cost and efficiency. Yet, these factors mean that networks are increasingly open and the available vectors for attack increase considerably.

Figure 1: Average day in an enterprise organisation

Source: **Check Point**

And those attacks are increasing both in volume and complexity. Opportunistic attacks still occur, launched en masse to impact as many victims as possible. However, attacks are being increasingly targeted against specific organisations and individuals within in them, using carefully crafted threats, often accompanied by social engineering techniques. Verizon's 2013 **Data Breach Investigations Report** found that 95% of such targeted attacks started with a spear phishing message aimed directly at an individual.

Increase in frequency and complexity of attacks

According to the Ponemon Institute, **60%** of organisations say opportunistic attacks are easier to prevent and are not as frequent as targeted attacks. Where advanced targeted attacks are concerned, the research found that 72% of respondents say exploits and malware have evaded their intrusion detection systems and 76% their antivirus controls. Because of factors such as these, FireEye estimates that more than **95%** of companies have been compromised with advanced malware, despite having deployed many layers of traditional defences at their perimeters. According to Proofpoint, **54%** of organisations say that their biggest challenge in thwarting targeted attacks is the increased sophistication of threats.

Traditional technologies no longer effective

Traditional security controls such as anti-virus and intrusion detection tools that are based on signatures are not up to the task of defending against the advanced, sophisticated threats being seen today. Such controls are still important for countering known threats, but they are not by themselves sufficient. They generally also only detect threats at a single point in time, when malware or other exploits first enter the network. Given the methods used by attackers to evade such controls and

then to maintain a hidden presence on the network, they not only fail to detect all malicious incidents, but will also be unable to detect follow-on activity once the attacker has gained a foothold on the network. According to Check Point, the average organisation is hit by 2.2 pieces of unknown malware every hour, which mounts up to 53 per day. It states that even the most responsive anti-virus, anti-bot or intrusion prevention systems face a two to three day window during which unknown malware remains undetected.

Attacks taking longer and getting harder to detect

Breaches are a certainty, but finding them remains problematic, with many remaining undetected for months or even longer. The 2014 **Verizon Data Breach Investigations Report** notes that web application attacks, which it found account for the greatest proportion of breaches at 35%, and cyber-espionage threats, the second most important category at 22% of the total, take the longest to discover. In the case of the latter, 67% of breaches take months or years to discover.

Today's attackers go to great lengths to remain undetected once they have gained a foothold on the network, stealthily moving through the network in search of more valuable targets and using advanced tools and techniques to evade security defences that organisations have in place. The longer they are able to remain undetected, the greater the damage they can cause. According to the **SANS 2014 Survey of Endpoint Intelligence**, whilst 70% of organisations are collecting data from endpoints, just 16% find more than half of their threats through active discovery or hunting.

Breaches getting ever more costly

According to the **Ponemon Cost of Data Breach Survey 2014**, data breaches are getting ever more costly, with the total cost of a data breach having increased 15% to US$3.5 million recently. For US organisations, the average cost is the highest at US$5.4 million—nearly one million more than the previous year.

Several high-profile breaches publicised recently are serving as a wake-up call to organisations owing to the damage they have caused. Many more organisations are starting to realise that such breaches can happen to any organisation, whatever its size or line of business.

The recent breach suffered by Target is case in point. In the weeks following the breach, its sales suffered badly, causing its net income to fall from US$961 million to US$520 million during the essential fourth quarter for the retailer in which the Christmas period falls. This continued into 2014 in terms of both in-store and online sales, with the percentage of US households choosing to shop with Target falling to 33% in January 2014, compared with 43% in January of the previous year.

Another example is eBay, which suffered a data breach in early 2014 in which user names, passwords, phone numbers and physical addresses were taken from its consumer database. According to company reports, the company's profitability was dented in the second quarter by the breach owing to reduced transaction volumes because of disruption caused by customers needing to reset their passwords, resulting in reduced revenue. As a result, eBay has reduced its full-year revenue guidance and has stated that it must bear the cost of significant investments that are aimed at reassuring customers.

Paradigm shift to not if, but when and how often

Factors such as these are leading to a paradigm shift in expectations. Organisations are no longer asking if they are likely to be breached, but rather asking when and how often breaches will occur.

According to the SANS Institute's Endpoint Intelligence Survey, 47% of organisations are operating under the assumption they've been compromised, with another 5% saying they operate under the assumption that if they have not already been compromised, they eventually will be. In reality, more organisations should be working under these assumptions.

Being proactive versus reactive

For many, incident response is seen as a reactive activity, focusing on events that have already occurred. Faced with limited budgets, many organisations feel that

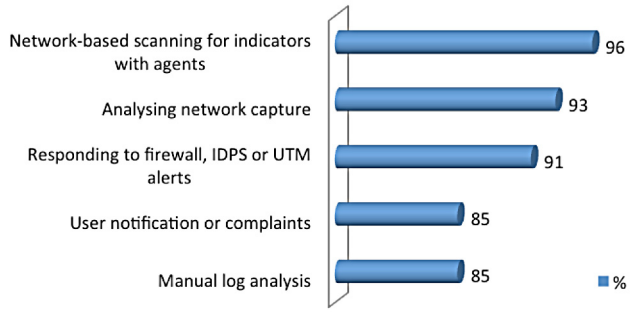
> **While information security risks have evolved and intensified, security strategies—historically compliance-based and perimeter-oriented—have not kept pace. The result? Today, organisations often rely on yesterday's security strategies to fight a largely ineffectual battle against highly skilled adversaries who leverage the threats and technologies of tomorrow.**
>
> *Source: PwC*

their budgets would be better spent on security measures aimed at preventing breaches from occurring in the first place. However, this is not an effective strategy in guarding against today's sophisticated attacks. It is inevitable that some attacks will get through defences and organisations need to be more proactive by making greater investments in detecting and responding to threats that have already infiltrated the network.

According to the SANS Institute, some of the biggest challenges related to incident recovery are connected to lack of visibility and ability to assess damage to endpoints and the network. The top five challenges are:

- Assessing the impact
- Determining the scope of a threat across multiple endpoints
- Determining the scope of compromise on a single endpoint
- Hunting for compromised endpoints
- Losing data inadvertently during a wipe and reimage

Figure 2: Most popular detection tools



Source: SANS Institute

Response needs to shift from incident response to continuous response

The costs of dealing with security incidents go way beyond the direct financial impact. There are hard costs to consider, such as lost revenues, as well as costs that are more difficult to quantify, such as reputational damage and lost productivity owing to the time required for dealing with the fallout and cleaning up the damage. One the other hand, a recent survey by the **EIU** found that 67% of organisations believe that responding to an incident effectively provides an opportunity to enhance the reputation of the company.

According to Check Point, 28% of organisations state that it takes up to ten days of staff time to remediate issues caused by a single attack. It also found that 33% state that each malware attack takes an average of £10,000 (US$16,617) to £50,000 (US$83,084) to remediate. Data such as this shows that it is more effective to adopt a strategy of continuous response rather than trying to battle each incident in isolation.

Automation is essential to continuous response

To shift from responding to individual incidents to a strategy based on continuous response requires the use of next-generation automation tools and techniques for not only detecting security threats, but for enabling efficient investigation of threats encountered so that the most effective countermeasure from a wide spectrum that has been developed can be automatically selected and even the most advanced threats can be removed.

But this is an area in which many organisations are lacking. According to the recent SANS Institute Endpoint Intelligence Survey, 77% of organisations still rely on slow and expensive wiping and reimaging of systems, compared to just 7% who reported using automated workflows for remediating endpoints. It also found that 54% have automated less than 10% of their workflow to manage the remediation process, although more than 60% of those who have not so far automated these processes indicate that they intend to do so in the next 24 months.

SANS cautions that lack of automation causes a remediation lag, during which time the consequences of any breach can increase dramatically. It is also a more expensive option in terms of internal costs. It estimates that, assuming a modest US$50 per man hour, remediating compromised endpoints can easily top US$200 for each infected endpoint being investigated. Estimates such as that underscore the case for more automation.

Another proponent of automation is industry expert Bruce Schneier, who stated recently at Black Hat 2014, "Automated systems and technology are necessary to support incident response." Schneier defines a four-step process that organisations should follow for effective, automated incident response, as shown in Table 1.

Observe	An organisation needs to know what is happening on networks in real time. Log monitoring, log analysis tools and network management tools can help in gathering the necessary information.
Context	Providing context requires information gathering and threat intelligence. An organisation has to know what the latest malware and vulnerabilities being exploited are. Information sources and internal research efforts provide the necessary data to explain the relevancy of network information.
Decide	The decide step requires that organisations prioritise issues and assign responsibility since incident response often breaks down when no knows who has the authority or power to take action. Properly assigning roles and responsibilities, as well as defining an escalation path, means that time is not wasted trying to figure out who needs to weigh in on the decision. Prioritisation is necessary for deciding whether remediation can wait or whether it needs to happen straight away.
Act	The final step involves executing the plan based on decisions made in the prior step.

Table 1: Four-step incident response process

Next-generation approach required to threat response and removal

Advanced automation tools and techniques are essential for keeping up with the volume of security incidents organisations face and for sifting through and making sense of the enormous number of alerts that are generated. According to recent **research** by the Ponemon Institute, some two-thirds of organisations believe that they are constantly inundated with security compromises. This leaves them too bogged down with security event data to be able to prioritise actions or even to undertake the time-intensive process of investigating incidents, which underscores that fact that many attacks go unnoticed for weeks or even months. It found that 61% of organisations state that security products create too many alerts and 85% of respondents believe that their organisations are currently unable to prioritise security incidents.

Because of factors such as these, many organisations feel unable to effectively respond to incidents themselves. According to the EIU report, some 70% of organisations, rising to 80% of large enterprises, rely on specialist organisations as part of their incident response plans, primarily forensic experts or other specialist IT providers, followed by specialist legal firms.

Clearly, a new approach is required for threat investigation and removal—one that is based on automation for the detection and investigation of threats, with the ability to automatically select from a spectrum of countermeasures in order to remove those threats.

However, many organisations are reluctant to embark on automated threat removal over fears that they may inadvertently cause disruption to critical systems, resulting in costly downtime or introducing further risk. To overcome such fears, an automated continuous response system should provide a level of human guidance, with steps built in to ensure that the countermeasure suggested is indeed the right one.

A recent report by the **FactPoint Group** states that the best approach to implementing automated remediation is to take a two-step approach. First, organisations should delve into historical and forensic information in order to minimise false positives. Then, they should allow security professionals to automate those tasks that they feel comfortable automating by setting a policy of what is actually removed, what is detected by software and flagged for a human decision, and what is allowed to remain on the network. Automated threat removal should begin with human oversight of what is being removed and only when the organisation has gained sufficient experience should threat removal be fully automated.

Demystifying remediation

> **Because of the fears that many organisations have regarding automated response and threat removal, many rely on only partial measures.**

Point solutions ineffective

Because of the fears that many organisations have regarding automated response and threat removal, many rely on only partial measures. At the very basic level, organisations will generate help desk tickets for responding to alerts. But, as discussed earlier, the sheer volume of alerts encountered by the average organisation makes this an inefficient, potentially very costly exercise, with each alert investigated in isolation. It relies too heavily on the use of human expertise—which is often thin on the ground—especially if every infected system has to be discovered and remediated separately.

Some organisations use network-level controls, focusing on preventing malicious inbound and outbound communication. For example, IP blocking can be used to prevent communication with malicious IP addresses that have been blacklisted. This can prevent IP-based attacks, but blacklists must be kept up to date and this is an increasingly onerous task, especially with attackers routinely changing domain names, even as often as every few minutes. A recent investigation by **Blue Coat Systems** found that of 660 million unique hostnames analysed, 71% only appeared for a single 24-hour period.

IP blocking can also be used to prevent unwanted outbound communications through egress points to remote command and control channels maintained by attackers. This can prevent sensitive information from leaking out of the organisation by automatically blocking traffic and can also prevent malware that has been programmed to dial out automatically to a command and control server from doing so, so that no additional malicious code can be downloaded. It can be useful for some other purposes, such as compliance with the PCI DSS industry standard, of which one of the requirements is "Do not allow unauthorised outbound traffic from the cardholder data environment to the internet." However, outbound IP blocking is also complex and onerous as it can require extensive configuration and maintenance.

Organisations can also choose to deploy host-based tools that can respond to security incidents by taking automated actions, such as blocking a process from running, quarantining an infected file, or expiring a user's account or credentials to prevent unwanted activity. They can be effective in preventing or remediating threats and incidents on individual host systems, but they are also known to generate a lot of 'noise' in the form of false positives and may block legitimate traffic or processes. Further disadvantages are that the controls generally have to be installed directly on each host being protected, which is a management burden, with extra time and effort required to tune rules for each system.

A major problem with such network- or host-based tools is that they are, in a great many cases, point solutions that solve particular pain points, with separate management systems working in isolation. This means that there is no way to uniformly enforce policies or monitor activities across hosts, the network and virtual instances, some of which will be cloud-based, from a central point.

Greater visibility and intelligence

Start with detection

For reasons such as these, organisations are increasingly looking to security solutions that can tightly integrate controls over all hosts, applications and the network. Such platforms need first to be able to detect threats, gathering log and event data from devices and systems throughout the network to allow threats and security events to be collected in a central data store that can handle both structured and unstructured information so that that incidents and threats can be identified and analysed. It needs to be able to handle extremely big data sets, taking feeds from systems that include data from all endpoints and web interactions, as well as security controls such as firewalls, intrusion detection and prevention systems, and data loss prevention controls.

In order that the security platform can provide timely and actionable intelligence, it must continuously monitor all activity rather than providing a snapshot view at a particular point in time. It should be able to identify all compromised devices and have sophisticated correlation and analysis capabilities so that organisations can identify how malware got onto the network and how it travelled through the network once it had gained a foothold. In order to be able to do this, it must be capable of correlating all activity to identify suspicious behaviour such as abnormal communications, suspect configuration changes caused by malware, anomalous logins and authentication events, or unwanted resource usage to detect all events that are outside of normal baseline behaviour.

Move on to containment

Once suspicious or abnormal events have been detected, including their nature, extent and severity, and alerts sent out, the incident response team needs to decide what course of action to take. This should also take into account the criticality of the assets that have been affected based on assessments that have been made and risk registers that the organisation has developed so that decisions can be taken as to which alerts to prioritise and whether the threat uncovered should be contained, such as by quarantining the infected system, or whether the threat should be removed from the network. In some cases, the organisation may wish to quarantine the threat in order to limit damage, but not remove it completely in order to obtain more information about the incident, such as for legal purposes.

However, a strategy of containment is not always appropriate since that may indicate to an attacker that their attack has been uncovered, which may cause them to hide their tracks and lay dormant on the network in order to recommence the attack once the organisation's response activity has died down.

Automatically remove threats

Even where a security team chooses to contain a threat, that is not always the end game as there is a high chance that the organisation will become re-infected. In cases where it is appropriate, the organisation may wish to completely remove the threat in order to be able to return to normal business operations. As discussed earlier, remediating incidents manually is a complex and expensive chore and there is a high chance that some infected endpoints will be missed.

A far better proposition is to select a security platform that provides tools for automatically removing malware and other exploits. To do this, it must be able to identify the tools, tips and procedures used by adversaries from the traces that they leave as they traverse networks—the so-called indicators of compromise (IOCs)—in a continuous and proactive manner. No matter how hard they try to cover their tracks to avoid detection, forensic artefacts, or IOCs, always remain that indicate that an attack has occurred. Algorithms can then be developed based on identified IOCs to automate the selection of countermeasures for taking action against even the most advanced threats.

Continuous monitoring will provide the necessary information for prioritising remediation activities by showing how

Even where a security team chooses to contain a threat, that is not always the end game as there is a high chance that the organisation will become re-infected.

far the attacker has intruded and what systems have been affected. Coupled with contextual information regarding the criticality of assets that have been affected, countermeasures can then be selected according to the course of action that the organisation wishes to take from a range included within the platform. These countermeasures include taking actions such as removing malware, isolating infected devices, or closing down accounts or expiring user credentials to prevent further access. Expiring credentials can be extremely important as most advanced threats look to gain access to user credentials in order to appear to be acting as much like a normal user as possible. They will then look to gain access to credentials with higher levels of privilege associated with them to get access to more valuable information.

In order to be effective and shrink incident response times, it is essential that the security platform should provide machine-guided incident response automation in line with policies to enable countermeasures to be taken in a semi-automatic or completely automated manner. This will allow organisations to embrace automated threat removal at a pace that they are comfortable with. Even when threat removal is completely automated, there should be a hierarchy of checks built in so that there are no unintended consequences, such as a critical system being shut down.

Once actions have been taken, the organisation should take a number of actions to validate that those actions have been successful (see text box). Once all compromised systems have been remediated and all traces of the attacker removed, it should then ensure that normal business functionality has been returned to its optimal state. By actually removing all threats from the network environment, the attacker's ability to initiate further malicious actions will have been mitigated.

Steps to take to fully mitigate advanced threats

- Stop and kill all active processes
- Remove and save all files installed by the attacked for later investigation
- Separate sensitive data from the network
- Apply necessary patches
- Update/reset all affected logins
- Assess file damage
- Reinstall affected files
- Notify all affected parties
- Disconnect affected hosts
- Perform daily reboot

Source: Hexis Cyber Solutions

Selecting a vendor

The only way to be sure that an advanced threat has been remediated is to ensure that all malware and exploits have been erased.

But caveat emptor: read the small print. There are many vendors claiming to automate the entire threat protection lifecycle, but the vast majority automate many of the steps, but stop short of automated removal. Some solutions will block or contain threats; others claim to provide actionable intelligence that includes proof an infection has occurred, with detailed forensic analysis to aid incident response teams in prioritising and remediating threats; some provide managed services to organisations, conducting investigations on their behalf and suggesting remediation steps. Without automated response capabilities, organisations will find themselves in fire-fighting mode, fighting each new infection in isolation. Such solutions will aid organisations in cutting investigation times by providing greater intelligence and context regarding each security incident, but they stop short of actually ensuring that all threats have been removed.

Instead, those organisations that actually want to ensure that malware infections have been completely resolved should read vendor claims carefully, looking for terms such as 'automated malware removal'. However, since many organisations will not be willing to automate everything, or at least not at first, any solution selected should offer semi-automated processes that give the opportunity to review changes and intervene in the remediation process.

In the early days of intrusion prevention systems, many organisations were reluctant to deploy them in fully active mode, worried that they may cause unwanted errors. However, over time, many organisations have come to be comfortable with active intrusion prevention. The same can be said of the market for security platforms that enable automated malware removal. Many will want to use semi-automated processes, moving to a higher level of automation over time for processes they feel comfortable with and defining policies for where full automation can be safely deployed. This will significantly reduce the time and effort involved in the threat remediation process.

Summary

Today's advanced attacks are increasingly pernicious, with attackers looking to bury deeply into networks so that they can carry out their deeds over long time periods, increasing their chances of garnering a horde of sensitive, valuable information. Those attacks are so widespread that every organisation should consider that it is a victim. It is no longer if, but when and how often an organisation will be attacked. Prevention alone is no longer sufficient.

Rather, organisations need to be proactive in seeking out incidents that have occurred and in actively removing threats. A strategy of containing threats is just a stopgap. Manual investigation and remediation of individual threats—often with the aid of a services organisation, whose mitigation efforts are often not repeatable—must be replaced with automated threat removal. This will allow an organisation not only to recover from security events faster and more efficiently, but will allow it to benefit from the automated learning offered by security platforms that provide effective tools for threat removal, providing it with the ability to better safeguard itself against similar events in the future. In this way, business disruption will be minimised and the organisation will be better able to get on with what it does best.

FURTHER INFORMATION
Further information about this subject is available from
http://www.BloorResearch.com/update/2238

About the author

FRAN HOWARTH
Senior Analyst / Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including ***Silicon***, ***Computer Weekly***, ***Computer Reseller News***, ***IT-Director*** and ***Computing Magazine***. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of ***InfoToday.***

Bloor overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations, and in 2014 celebrates its 25th anniversary. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter 'noise' and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent 25 years distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

Copyright and disclaimer

2nd Floor
145–157 St John Street
LONDON EC1V 4PY
United Kingdom

Tel: **+44 (0)20 7043 9750**
Web: **www.Bloor.eu**
email: **info@Bloor.eu**