256-260 Old Street
London
EC1V 9DD

+44 (0) 207 749 7949
sales@autodata.co.uk
www.autodata.co.uk

CYBER SECURITY WHITEPAPER

Mitigating the risk of a breach with less resource

Contents

1 Introduction

Security professionals are inundated with an unmanageable number of alerts generated by the growing number of security tools in which they have invested. Investigating and connecting individual alerts takes time and resource.

Having a clear understanding of the root cause of a real threat is problem for many security and IT teams and often compounded by the lack of security talent to analyse these threats. Once threats are discovered, the time required to understand the breadth of the attack and ultimately remediate the threat is now measured in months.

"*Many security teams have overinvested in a plethora of tools. As a result, they are also suffering from alert fatigue and multiple console complexity and are facing challenges in recruiting and retaining security operations analysts with the right set of skills and expertise to effectively use all those tools*" - Gartner 2017

The above quote is from 2017 but nothing has changed in the last 7 years, in fact the situation has only got worse. IT teams increasingly struggle to manage the array of security solutions needed to provide visibility into impending threats across their environments. Moreover, the cybersecurity stack has become even more complex and unwieldy, meaning the skillset required to maintain and operate the solutions is beyond the grasp of all but the largest global organisations.

In IBM's Cost of a Data Breach Report 2022, it was reported that it took an average of 277 days for businesses to identify and report a data breach. This is why breaches continue to rise despite increased cybersecurity investments.

A new class of security tools is emerging that promises to greatly improve the effectiveness and efficiency of threat detection and response. Gartner has defined a new solution category that aggregates and correlates telemetry from multiple detection controls and then enriches and automates response actions: **Extended Detection and Response or 'XDR'.**

2 Challenges Faced by Organisations

Threat protection poses numerous challenges for organisations as the landscape of cyber threats continues to evolve.

2.1 The Skills & Staffing Issue

Independent research[1] confirms that high staff turnover is critically undermining cybersecurity capabilities in mid-market organisations. Censuswide recently surveyed mid-market IT professionals finding only 2% manage to retain "excellent" IT talent for over two years. 28% typically lose their top talent within 6 months, a constant churn which severely hinders the development of robust cyber strategies. Limited resources lead companies to neglect basic security practices despite increased investment in training. Over 50% admitted to overlooking fundamental measures like firewalls, antivirus, and regular patching. 47% of respondents develop their strategies in-house yet remain critically exposed with outdated practices.

With every business being a potential target, cybersecurity intelligence, protection, detection, and response are crucial for mitigating risk. The research found that with skill-drain impeding accountability, many mid-market firms operate without expertise, unsure where accountability lies, leaving them vulnerable to unbudgeted remediation costs after an attack.

To make matters worse, Gartner analyst John-David Lovelock recently told CRN[2] that the talent shortage will continue for another five years with the Enterprise IT space suffering from an "unsolvable problem" of labour:

"Enterprises cannot attract, maintain and retain enough IT talent to meet their growing IT needs and are having to turn to consultancies to do the work. That includes managed services to continue to run their ongoing operations."

2.2 Visibility of Threats

Visibility across an organisation's environment and understanding the details of alert data is the first step to stopping a threat. Businesses typically deploy multiple prevention and detection technologies to defend points of entry such as endpoints, networks, users, and data. While these tools generally do a great job in preventing and detecting the vast majority of cyberattacks, they continue to miss the edge cases.

Based on the "dwell time" cited in the IBM study, the real challenge in security today is finding the threats bypassing first-line defences as quickly as possible. Something that may seem benign to one security solution suddenly becomes cause for concern when paired with information from other security solutions. Consolidating prevention and detection technologies into a single solution can coordinate threat signals to paint a more accurate picture of an attack. When various tools share information, security incidents can be identified more quickly and responses can be triggered promptly.

Smaller organisations often face unique struggles due to resource limitations. They often can't afford the different tools required to provide visibility and prevention of security threats and don't have the relevant cyber security talent to manage these risks.

[1] https://www.itpro.com/business/careers-and-training/majority-of-mid-market-firms-struggle-to-retain-it-talent-for-more-than-two-years-research-shows#

[2] https://www.channelweb.co.uk/news/4166432/gartner-talent-unsolvable

2.3 AntiVirus alone is not Enough

Many organisations have turned to Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP) and Next Generation Anti-Virus (NGAV) solutions for enhanced protection beyond the commonly used Anti-Virus (AV) platforms.

The EDR/EPP/NGAV solutions have proven highly valuable in preventing and detecting many forms of endpoint attacks. However, cybercriminals are finding ways to bypass these approaches with increasingly stealthy attacks. These are some of the reason why AV used exclusively might not be as effective:

1. **Limited to Known Threats:** Antivirus software primarily relies on signature-based detection to identify known malware based on predefined patterns and hashes. This means they may struggle to detect new or previously unseen threats.

2. **Behavioural Analysis:** More advanced malware may use techniques that bypass traditional signature-based detection. Behavioural analysis observes the behaviour and patterns of legitimate users to identify malicious activity.

3. **Fileless Malware:** Modern malware operates without leaving traditional file traces making it difficult for antivirus programs to detect. These types of threats can reside in memory and exploit vulnerabilities without leaving traditional files for antivirus to scan.

2.4 The Need for 24/7 Response

Cyber threats don't adhere to a strict schedule. Without continuous monitoring, there may be delays in detecting security incidents, allowing attackers more time to carry out their activities and potentially escalate the impact.

Security teams today spend considerable time investigating false positive alerts. Confirmed threats then require access to multiple controls through multiple consoles to investigate the full breadth of the attack.

Remediating threats also requires far too much effort to plan and coordinate corrective actions across multiple security systems. Security teams are simply overwhelmed by operating and maintaining too many point solutions.

But what happens if there is a security incident outside of working hours?

3 Bringing it all Together with XDR

XDR helps security teams by consolidating and rationalising alerts into actionable incidents and automating investigation with response actions. The primary requirements of an XDR platform are threat visibility, understanding the incident and creating an automated response.

3.1 Seeing the Full Picture

Protection, visibility and detection are the main components that form the foundations of an XDR platform. Combining signals from the different components provides the context and information required to detect the often missed attacks while reducing false positives.

As the components included are part of a unified platform, data and alert information can be easily read and understood. Deciding which prevention and detection components should be included in the XDR platform is critical.

At a minimum, XDR tools should include signals from the following key components:

- **NGAV** - Next Generation Antivirus for basic endpoint malware prevention and detection

- **EPP/EDR -** Endpoint Protection Platform/Endpoint Detection and Response for more advanced endpoint protection, detection, and response

- **UBA Rules** - User Behavioural Analytics Rules

- **NDR** - Network Detection Rules for malicious activity on your network

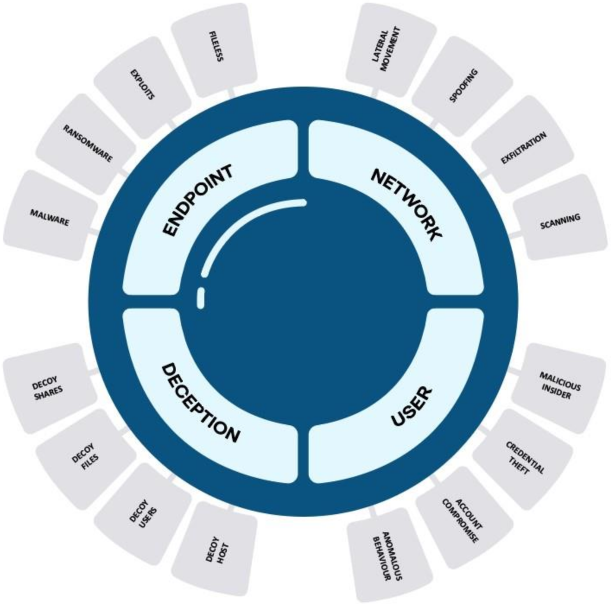
Put together, the signals from these solution categories provide the visibility required to detect the vast majority of attacks across the cyber kill chain.

Other data may supplement this core set, but these components have been shown to provide the best value.

For example, signals from deception technologies that trick successful intruders into exposing their presence before damage can be done can provide highly valuable signals to an XDR platform.

It is also recommended that as many components as possible are native to the XDR platform. This ensures that all signals are visible and accessible in a single pane of glass.

It also eliminates the time and effort required to integrate and continuously maintain tools from multiple vendors.



3.2 Understanding the Cause of the Incident

XDR platforms collect data and alerts from diverse security components such as endpoint detection and response (EDR), network detection and response (NDR), and cloud security tools. By aggregating signals from these different sources, XDR creates a comprehensive view of the security landscape.

Utilising XDR enables the use of advanced analytics and correlation techniques to identify patterns and anomalies across the collected data. By intelligently combining seemingly harmless signals from multiple sources, these platforms can uncover potential threats that may not have been apparent when analysing each source individually.

3.3 Automating the Response

A critical aspect of XDR platforms is their ability to not only detect security incidents but also to respond swiftly and effectively.

Response actions begin with an investigation automatically collecting information associated with the incident, determining the root cause and analysing the impact of the threat. For example, some XDR tools might automatically list running processes associated with an alert, query a windows registry, collect environmental variables, or run an automated script.

While much attention has been paid to the detection part of XDR, the response capabilities of the platform can allow organisations to instantly react to real threats while minimising the burden on their security teams.

Most XDR tools provide some level of automated remediation actions such as deleting malicious files, quarantining infected endpoints or killing rogue processes. More advanced XDR platforms expand remediation across the environment and automate more complex response actions that chain various remediation actions into a single flow that runs automatically when a predefined alert is triggered.

These type of more comprehensive actions are part of Security Orchestration, Automation and Response (SOAR) technology. **XDR platforms with multiple security controls natively built-in have the potential to provide SOAR-like capabilities without the complexity of implementing a full SOAR solution.**

4 The Benefits of XDR

XDR provides a holistic platform that unifies multiple control points to coordinate threat prevention, detection, and response. This approach improves detection accuracy while dramatically reducing the complexity and manual intervention of security teams required for comprehensive threat analysis and protection.

4.1 Visibility

XDR platforms provide a broader view of incoming threats by natively combining prevention and detection controls from the meaningful attack vectors. This holistic view enables XDR platforms to automatically highlight real alerts from noise as well as uncover subtle threat clues that may have gone unnoticed with disparate detection tools. The visibility and intelligence provided by XDR platforms more comprehensive threat detection alerting.

4.2 Reducing False Positives

With XDR platforms, security teams spend far less time chasing after false positive alerts. Many real threats are automatically remediated with no manual intervention required. Confirmed incidents are either automatically investigated and remediated or accompanied by rich data and context to shorten manual investigation and response actions. The time required to integrate, maintain, and operate multiple tools and systems is eliminated enabling.

4.3 Cost Reduction

Consolidating multiple security products into a single XDR platform provides significant cost savings, both in terms of licence and subscription costs and internal support costs. Reducing a large volume of alerts into fewer meaningful incidents along with automating response actions reduces the time security teams would otherwise spend on these tasks.

4.4 24/7 Monitoring & Response

Having an XDR solution managed provides continuous 24/7 monitoring of an organisation's security environment where organisations can call upon the expertise of a SOC team to assist in threat detection, analysis, and response.

Given the skills shortage and the problem of retaining cyber-security talent cited earlier, having a managed XDR solution helps leverage the specialised knowledge of security experts without the need for in-house hiring and training. It also ensures that potential threats are detected and responded to promptly, even during off-hours.