Avecto Whitepaper

Prevention is possible

Why a proactive approach to cyber security pays dividends

Contents

Introduction

It's commonly accepted that prevention is better than the cure, however, when it comes to information security, we often spend valuable time and resource chasing down cures for infections we could have prevented in the first place. This is the digital equivalent of not washing your hands because you have access to antibiotics. It's costly and will ultimately end in failure.

It's time to take a step back from the hype and look at how we can proactively prevent attacks in the real world. There is a wealth of evidence out there showing that implementing a strategy built on proactive security not only provides the best defense, but is also the most cost effective way to implement cyber security.

Just as is the case with antibiotics, detection technology is not dead, but it cannot be relied upon in isolation. Even the latest advances cannot keep pace with a rapidly evolving threat landscape leading to inevitable infection. Adopting a proactive stance allows you to regain control and block, isolate or mitigate the threats at the earliest stage in the attack chain.

In this document we'll walk through the historic pitfalls of security and show why we need to move away from chasing the unknown, to securing the known. We'll then discuss how this shift can be achieved using defense in depth to build secure endpoints, and how this helps us build robust detection and response capabilities on top of secure foundations. This will take us into a discussion around prioritizing solutions and how modern cyber threats are evolving. Finally, we'll walk through the attack chain of some example threats and prove how it's possible to strike first and defeat them.

More than **353 million** infected files exposed to networks each day

McAfee Quarterly Threat Report – March 2016

Historic pitfalls

In the past few decades, we've seen huge technological advances in the enterprise, but despite this we're still failing to learn the lessons laid out by history. The term "computer virus" was coined in 1983 by Dr Fred Cohen, who also stated "there is no algorithm that can perfectly detect all possible computer viruses". Cohen rightly concluded viruses would be able to evade detection by constantly evolving and modifying behaviour when being scanned. Despite these early warnings, the majority of security vendors have spent most of the past 20+ years trying to detect the unknown.

Security products have obviously come a long way since the early days, but even the most advanced solutions, with dynamic analysis environments, are still trying to identify known bad behaviour without false positives. As the technology evolves and introduces more sensors to cover both network and endpoint activity, the complexity and analysis time increases. This means that products are forced to make a compromise between security and performance. Intel Security found a third of organizations disable security features in favor of performance.[1]

Recently, even the vendors seem to be facing the reality that they are fighting a losing battle. Brian Dye, a SVP at Symantec, proclaimed that AV is dead, estimating it can only detect around 45% of attacks. Worryingly, in 2016, an attack does not need to be advanced or highly sophisticated to bypass the majority of enterprise security defenses. It just needs to be unique. We witness this all the time with large organizations being hit with ransomware launched from Word documents. With over 20 years of security innovation why are companies still being brought to their knees by macro attacks?

Is the solution to abandon AV and detection entirely? Of course not. What we need to do is understand that threats will bypass our network and endpoint detection products and start to layer on proactive measures to secure the endpoint. After all, the endpoint is where the user is, where the data is and where the threats are looking to target and exploit.

Total malware by end of 2015 reached nearly **500 million**

McAfee Quarterly Threat Report
March 2016

[1] http://www.mcafee.com/uk/resources/reports/rp-mcafee-security-vs-network-performance.pdf

In actual fact, detection can play a part in refining the security stack over time, but only if it's underpinned by strong proactive security. Take, for example, a typical phishing attack; the user receives a malicious Word document that is not picked up by any email filters or detection solutions. If we apply proactive measures such as preventing access to admin rights, blocking undetectable payloads from executing and isolating the document in a sandbox, then we prevent the attack from succeeding.

We can then use the data from this foiled attack to feedback to other solutions and refine the email and gateway filtering. Because proactive measures were taken to prevent the attack in the first place, the security team were able to use that data to improve other systems, rather than costly and ineffective firefighting while constantly risking being breached.

There were **96,699** phishing scams in 2015

Action Fraud and the National Fraud Intelligence Bureau

The modern threat

The security industry is often awash with scare stories and jargon, confusing organizations into thinking they can never get ahead of threats. With FBI directors stating there are only two types of company "those that have been hacked and those that will be" many worry the battle is already lost.

With free ransomware kits available to would-be attackers and organizations being penetrated by Word document macros, the technical and financial barriers to enter into the cybercrime arena are at an all-time low. The darkweb and bitcoin make attacks and finances hard to trace and shutdown. With low risk and high reward, we're seeing the perfect storm of threats.

As with any thriving industry, cybercriminals are constantly innovating and evolving their offerings to bypass security measures and find new application exploits. The leading exploit kits that offer malware as a commercial service often pride themselves on being undetectable or harnessing a new zero-day vulnerability.

With this threat landscape it's no wonder that security solutions are often obscured by a thick fog of technical language that is designed to spread fear, uncertainty and doubt. Organizations are increasingly becoming confused about what they can do to prevent attackers circumventing their systems. This can lead to losing sight of how to secure the environment; instead attempting to implement products or solutions that are doomed to costly failure. When large retailers invest millions of dollars in the latest solutions and still get breached, faith is lost.

But is this really the case or is there a way to prevent these attacks from occurring in the first place?

APTs and advanced threats

When we look at media headlines surrounding the multitude of large scale data breaches there is a huge focus on Advanced Persistent Threats (APTs) and undetectable attacks. These reports follow hugely costly investigations and often take months to conduct, yet when you drill down to the details it's often the case that an admin account was compromised, a third party was given too much access or simply software was unpatched and vulnerable.

All too often, attacks are dismissed as highly sophisticated and unstoppable, when in reality some straightforward proactive measures could have mitigated them. Take for example a 2015 attack against an international government entity. This attack was attributed to state sponsored actors and was described as highly targeted, containing two zero-day exploits. If we look at the attack chain though, we see that apart from the zero-day exploits, this is a familiar attack pattern:

01 Target clicks a link leading to an infected website
02 Infected page delivers a zero-day Flash exploit CVE-2015-3043
03 Flash exploit launches shellcode dropper on target machine
04 Dropper downloads and runs a malicious executable
05 Executable steals system token using CVE-2015-1701 local privilege escalation vulnerability

> “When someone sends you an email, they are knocking on your door. And when you open the attachment, without looking through the peephole to see who it is, you just opened the door and let a stranger into your life, where everything you care about is.”

James Comey, Director of the Federal Bureau of Investigation

When we break this advanced attack down, what are we actually seeing?

Firstly, the user visits an infected website and the Flash plugin is exploited. This is a common attack vector and therefore to prevent it, we should isolate the browser in a sandbox where possible.

Secondly, some shellcode downloads an unknown executable to disk. As it is not part of the corporate build and not an IT approved application, this should not be allowed to run. In fact, if we apply this within a sandbox environment it's even easier to spot these unknown applications, as we know that only a small handful of applications should be launching within the sandbox.

Finally, we see this attack is ultimately trying to escalate privileges. This is something many organizations just make too easy for attackers when users log in in and check emails using full admin accounts. So of course, least privilege is an essential mitigation technique to build this secure foundation.

Without any detection-based strategy, indicators of compromise or anti-exploit technology, it is possible to prevent this attack. Proactively disrupting the attack chain in this way this would work just the same for a Java exploit, malicious document or any of the common attack vectors.

This idea of proactive measures being able to thwart attacks is a common theme across many breaches. We see headline-grabbing reports talking of sophisticated modular payloads, droppers and undetectable APT threats as if they are an unstoppable tide. In reality, we are facing multiple unknown applications appearing and executing in the environment. A robust whitelist could have stopped each and every stage of this threat.

Nearly **75%** of all legitimate websites have unpatched vulnerabilities

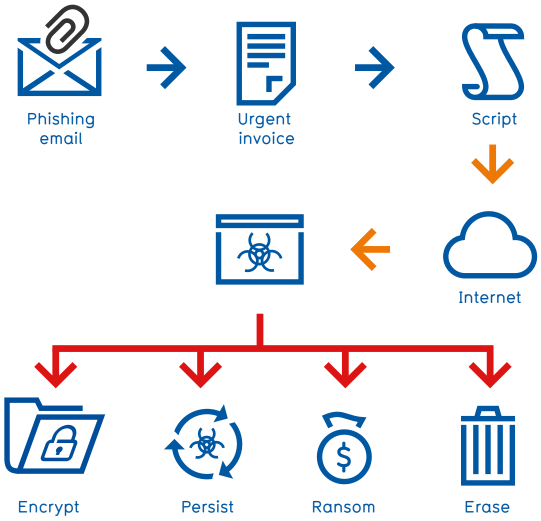
Symantec – Internet Security Threat Report 2016

Ransomware

Ransomware is a hot topic in cyber security at the moment as more and more organizations fall victim to these types of attack, on both Windows and Mac devices. Unlike other attacks, everyone is a target. If you have computer systems and access to data, you are a potential victim. From hospitals to energy companies, a diverse range of organizations have suffered attacks, with files encrypted and ransom demands made in order to get their data back.

Some of the most recent highest profile attacks have come from the Locky strain of ransomware. This is the latest evolution of ransomware, and the threat actors who use it are well versed in how to target enterprises.

Locky attack chain



If we look at the typical Locky attack chain (the steps involved in an attack), we'll see people within an organization have been targeted with a fake invoice. Often the attackers will have researched the business using tools such as LinkedIn or the company website to scope out targets with the most access to data. The fake invoice is usually a Word document, although JavaScript files are also used.

Number of ransomware threats increased by **35%**

Symantec – Internet Security Threat Report 2016

When Avecto conducted research into user awareness of attack vectors, 39% of respondents considered Microsoft Office attachments (.doc, .xls or .ppt) to be safe.[2]

9,515 ransoms are paid each month

Cisco Annual Security Report – 2016

The infected Word document instructs the user to enable macros to view the file. As soon as they do this, the attack begins, a script will download and run the Locky malware on the system. This then encrypts data both locally and on any network shares or connected devices, attempts to delete any local backups, and demands a ransom payment.

The majority of security vendors will tell you that regular backups and better detection are the only ways to try and fight back against ransomware. While backups are essential they are not a defense strategy. They are, as the name suggests, a last resort and fall back option. As for improving detection rates, even with 99% detection you're still going to see threats getting thorough and it only takes one to cause a breach or have all your data encrypted.

If we approach the problem from a proactive prevention perspective, can we regain control and stay ahead of these ransomware threats? As with the previous advanced attack we're seeing untrusted content from the internet being allowed to launch scripts as the logged on user. The first thing we can do is isolate the document in a sandbox and implement least privilege to ensure it cannot access admin rights. This immediately prevents data from being compromised as the isolated sandbox has no access to the logged on user's data.

Phishing email

Urgent invoice

We also see an undetectable payload has been dropped into the user's profile and launched. To a proactive solution this is not undetectable, this is an unknown application that is not on the whitelist so it can simply be blocked. As with the previous case, the sandbox feeds valuable context information to application whitelists, so that applications and scripts dropped by attacks can be clearly differentiated from those deliberately introduced by the user.

[2] https://www.avecto.com/news-and-events/press-releases/41-of-email-users-trust-the-safety-of-email-attachments

This is a unique ability of the Defendpoint solution which provides three powerful modules working in harmony for improved security.

The benefit of this context aware whitelisting comes into play when attacks attempt to exploit built-in system tools such as PowerShell or other scripting engines. These tactics are increasingly being used to bypass security measures as PowerShell is a Microsoft signed application, raises few red flags, and is usually allowed to run. Traditional application control solutions cannot easily distinguish between user behaviour and an attack, so must either block or allow the tools entirely.

With a more pragmatic approach to whitelisting, it's possible to block these attacks without preventing the user from utilizing the tools they need to get the job done. Being able to distinguish real user activity from that of an untrusted document or website attempting to launch a PowerShell script, is made simple given the context of the sandbox.

Now we've shown the benefits of proactive prevention against real world threats, let's take a look at how we actually implement these strategically.

> “To get the most protection, consider layering multiple endpoint tools to limit the attack surface to a manageable level.”
>
> Chris Sherman, Forrester: Prepare For the Post-AV Era Part 1: Five Alternatives To Endpoint Antivirus

Defense in depth

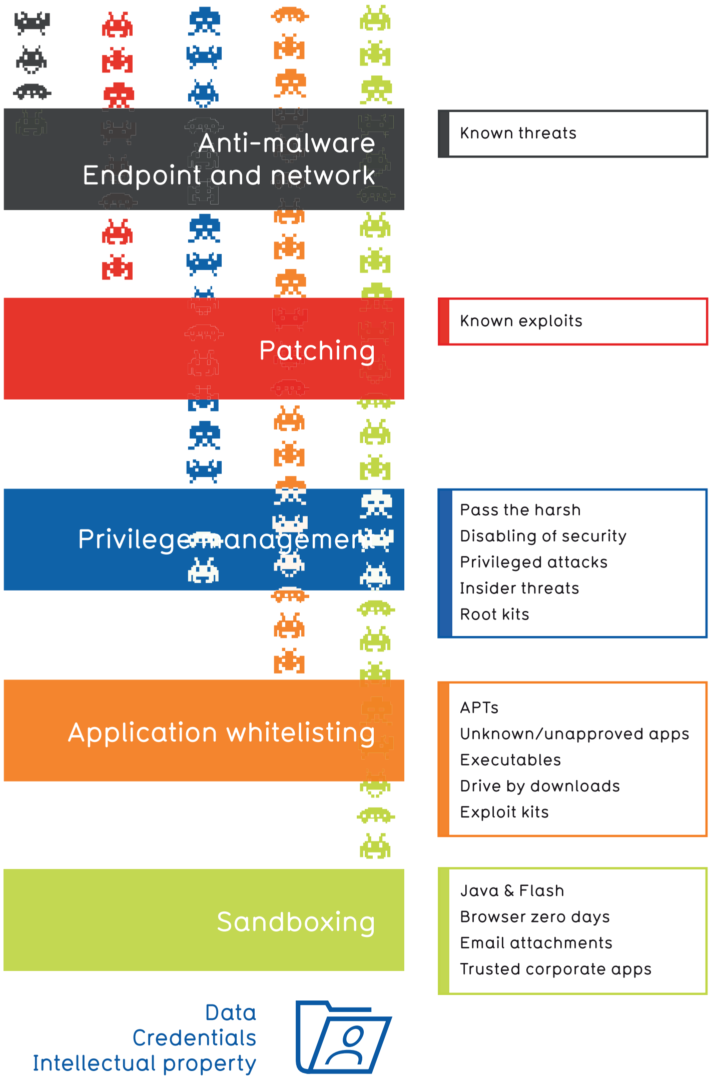
How do we layer on security measures to create a defense in depth strategy? The starting point should be industry best practice and when we look at the research conducted by SANS, Gartner, GCHQ and others, we see a common pattern emerging in the advice:

- Whitelist known good
- Patch business apps and patch the OS
- Least privilege

These are not just token measures, but proven strategies that can prevent real world attacks. In fact, the Australian DoD conducted significant research into cyber intrusions and concluded at least 85% of attacks could have been prevented using these methods alone, as part of a defense in depth strategy.

To illustrate why these measures are so effective at stopping attacks let's look at how the defense in depth approach handles attacks, reducing the attack surface with every layer.

Defense in depth – reduce the attack surface



Anti-malware
Endpoint and network

Known threats

Patching

Known exploits

Privilege management

Pass the harsh
Disabling of security
Privileged attacks
Insider threats
Root kits

Application whitelisting

APTs
Unknown/unapproved apps
Executables
Drive by downloads
Exploit kits

Sandboxing

Java & Flash
Browser zero days
Email attachments
Trusted corporate apps

Data
Credentials
Intellectual property

Antimalware

This is what most organizations have today and comprises of multiple solutions including firewalls, antivirus, network security appliances and threat intelligence feeds. The key point is that even the best antimalware solutions are not 100% effective and can only serve to reduce the number of attacks reaching the endpoint, not prevent them entirely. They rely on being able to detect known bad behaviour and block it.

Patching

Why make life easy for the attackers by running systems that are known to be vulnerable? Where possible, patching should be used to reduce the attack surface and prevent attackers using known public exploits. In some environments this is a challenge, with line of business applications relying on out of date (but compatible) plugins or software to function.

Privilege management

This is where the proactive benefits really start to stack up. If an attacker can gain access to admin rights they have the keys to the kingdom. By implementing least privilege with a privilege management technology, admin rights are assigned only to the tasks that need them and not to the user. This prevents attackers from easily infecting the system, pivoting, stealing credentials and disabling other security measures. It also helps reduce the risk of users making deliberate or accidental mistakes and reduces management costs.

Application control

Whitelisting is the number one defense against cyber threats. Simply put, if you don't know and trust the application, it doesn't get to run. In the past, configuring whitelists has been extremely difficult and costly. However, when used alongside privilege management it becomes easily achievable as the user cannot introduce or alter applications.

> “Application control is the number one strategy to mitigate cyber attacks, as shown by real world data.”

Australian Security Directorate (ASD)

This means the corporate build is whitelisted with just a few simple rules, with exceptions catered for using a variety of flexible options tailored for each type of user. Advanced attacks and APTs that use multiple rapidly evolving modules to evade detection will be blocked as soon as they attempt to launch.

70-90% of malware is unique to an organization

Verizon DBIR 2015

Sandboxing

Even with robust privilege management and application control in place, we still have to allow the user to open high risk applications such as web browsers and document viewers to access potentially dangerous content from the internet. Without admin rights, users still have access to huge volumes of Intellectual Property (IP) and valuable data, both locally and on network shares. So in the event of an application being compromised, so too is the data. We see this tactic being used by ransomware to quickly grab and encrypt data.

Sandboxing isolates these high risk applications from the user account. Even if the browser loads a vulnerable plugin and is attacked, the users account and data are protected from the threat. This is highly effective against increasingly common ransomware and IP theft type attacks.

DiD summary

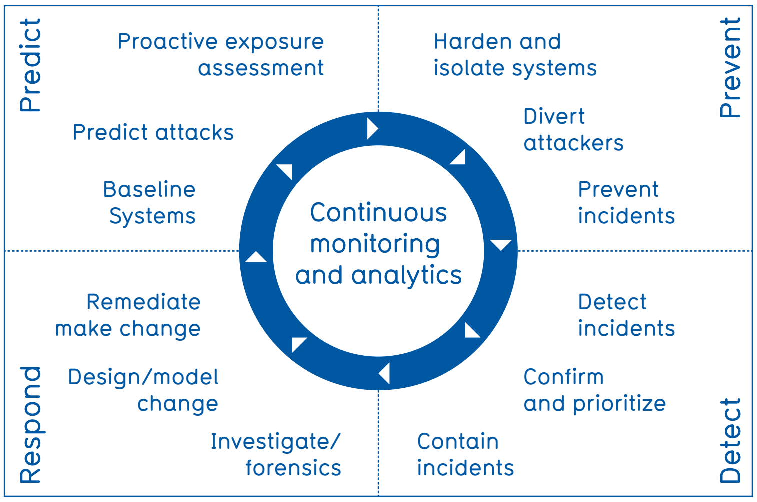
While each layer in this defense in depth stack has clear benefits to offer, it is the combination of these defenses working in harmony that offers the greatest benefit. When we consider that the latter measures outlined are completely agnostic to the threat and have no reliance on detection, we can see they are just as effective against known threats and zero-day attacks. This is why the security stack is proactive – it focuses on reducing the attack surface and breaking the attack chain at the earliest possible stage.

With these defenses in place it is irrelevant how targeted or sophisticated a payload is, or how many vendors failed to detect it. There could be a zero-day attack that drops an undetectable payload to disk, or a fileless malware strain launching scripts from the Registry. Both can be defeated using proactive security measures as part of a defense in depth approach. The attack is stopped, the data is secure, and no costly investigation or remediation is required.

Detection and response

The industry push for organizations to implement detection and response capabilities is huge, with analysts and vendors all driving home the message that this is the best way to handle cyber threats. Organizations often misunderstand detection and response and fail to build these capabilities on top of secure foundations. Failing to do so simply results in the whole architecture being undermined. This is clearly evident in Gartner's Adaptive Security Architecture, where prediction and prevention are key parts of the cycle.

The adaptive security architecture

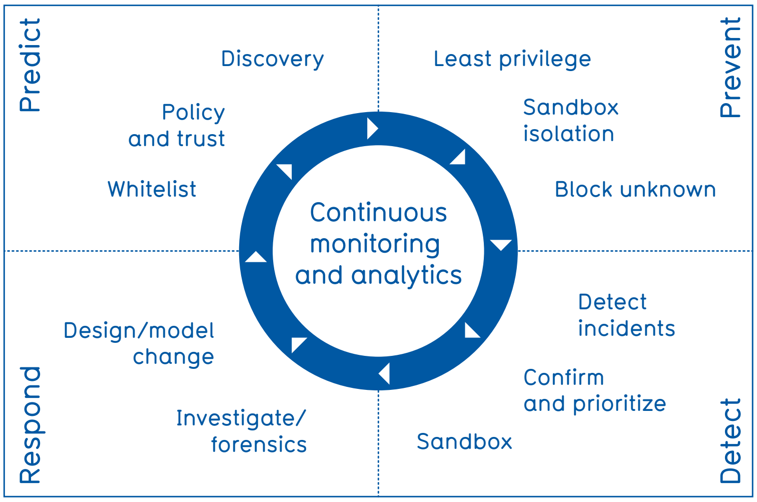


When we look at the Gartner Adaptive Security Architecture model we see two important sections which are often overlooked – Prediction and Prevention. As we have seen time and time again, organizations are often flooded with huge volumes of attacks that exploit known and entirely predictable attack vectors.

The purpose of this cycle is to constantly refine security and ensure it evolves at the same pace as the attacks. What some fail to factor in though is the huge wealth of information available to them already about the best ways to prevent attacks. Instead of leveraging this information for proactive defense, they instead try to layer in more reactive detection on top of vulnerable endpoints.

The end result is that threats can still bypass the detection layers, and malware still exploits the vulnerable endpoints. Security teams become overloaded with information and are unable to spot the attack amongst all the noise, a theme we have seen occurring in some of the biggest data breaches around the globe.

To make detection and response work you must first build secure endpoints and infrastructure based on best practice. This cuts out the majority of common attack vectors allowing you to focus on a select few detected incidents rather than firefighting. In a world of undetectable threats and targeted attacks, we should look to reduce the target and move beyond detection alone.



How does Defendpoint's proactive security let you to regain control and defend against attacks?

Predict and prevent

Defendpoint allows you to harden and isolate systems from threats by reducing the attack surface and containing potential attacks. Running in discovery mode, Defendpoint can quickly allow a baseline of the user's application and privilege requirements to be established, allowing you to accelerate the deployment of policies that reduce their exposure to risk.

The combination of least privilege, whitelisting and sandbox isolation significantly hardens the endpoint by reducing the attack surface; thwarting attackers by isolating potentially malicious content in a separate sandbox environment. This prevents a huge range of attacks, from drive-by downloads, to document exploits and macro attacks.

Defendpoint is designed to work with Windows and the rest of your security stack, not against it, in a lightweight and effective way. This allows you to quickly lock down the common attack vectors without compromising the user experience.

Detection and response

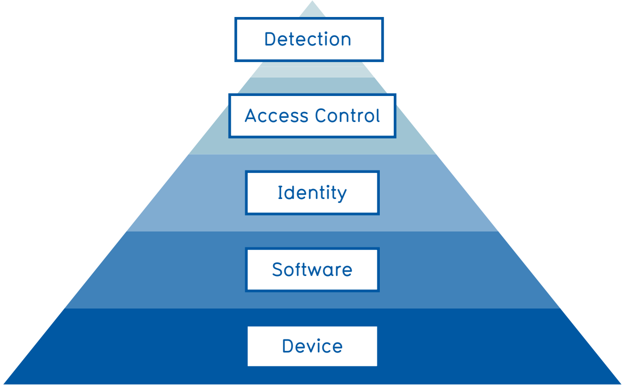
As security is a journey and not a destination, the purpose of Gartner's Adaptive Security Architecture is to evolve defenses as rapidly as the malware. This works as a constant feedback loop, continually improving security. By isolating threats within the sandbox, Defendpoint contains incidents that would otherwise have caused a breach. This allows teams to confirm and prioritize attempted attacks, and gives detection technologies a chance to catch up.

With an attempted attack contained and prevented, it's then possible to leverage the data to respond to future incidents. Defendpoint's simple firewall style rules make updating policy quick and easy, and allows for swift actions such as blocking applications signed with compromized certificates or prompting users to update a vulnerable application.

Hierarchy of Cyber Needs

This strategy is supported by the Microsoft Enterprise Cybersecurity Group's 'Global Incident Response and Recovery' team, who published a blog about building secure foundations. Looking at their "Hierarchy of Cyber Needs" we see that detection (and response) are a part of the stack but require a number of prerequisites before being effectively implemented.

"Use this as a road map to improve your enterprise security as quickly and cost-effectively as possible." —Microsoft TechNet [3]



All too often, organizations are pushed into implementing next generation firewalls or network appliances before they have secured endpoint devices, software, identity and access. The problem with approaching the issue of cyber threats this way is that it does nothing to reduce the attack surface of the target; the endpoint. Because no solution is ever 100% effective, threats can still evade even the most advanced perimeter defense.

If we start security at the endpoint and work outwards, layering on the advanced network detection solutions, then we build on secure foundations and don't risk being totally undermined by an attack.

> “Very often, the endpoint device was the initial point of compromise that allowed for lateral movement into the network, creating additional damage.”

Dr Eric Cole, SANS

[3] https://blogs.technet.microsoft.com/askpfeplat/2016/01/25/the-hierarchy-of-cyber-needs/

The focus on network technologies also fails to address other common attack vectors. With increasingly mobile workforces, what happens when the laptop is taken out of the office? And what about USB sticks with malware on, or an insider attack? If you start by securing the endpoint, you're building the best defense against the broadest range of attacks.

Prevention is possible

In a world full of data breaches and cyber attacks, organizations are often left wondering where to start, and end up implementing technologies without first considering the root cause of their issues. This confusion often results in wasting time and money trying to implement solutions that become costly to maintain, and ultimately fail to prevent a breach. Instead, focus on implementing the strategies in the right order, for maximum effectiveness.

According to research from the Verizon DBIR 2015 report, 70-90% of malware is unique to an organization. The problem is that many organizations are relying on generic detection solutions to handle unique and targeted attacks. When dealing with the modern threat landscape, maintaining blacklists of known malware and bad URLs serves little benefit when others are being exposed to variants you will never see yourself.

From real world attacks to expert advice, it is clear that proactive strategies can improve security, reduce costs and finally allow security teams to work strategically to stay one step ahead of attackers, and prevent as much malware as possible from ever executing on the endpoint.

In doing so, organizations are able to achieve improved security, while maintaining a positive user experience on the endpoint.

Take a proactive approach to security and make prevention possible on the endpoint.

About Avecto

Avecto is an innovator in endpoint security.

Founded in 2008, the company was established to challenge the status quo that effective security leads to user lockdown. This philosophy of security + freedom promotes a positive user experience across every software implementation, allowing organizations to strike just the right balance.

Its unique Defendpoint software makes prevention possible, integrating three proactive technologies to stop malware at the endpoint. This innovative software has been implemented at many of the world's most recognizable brands, with over 8 million licenses deployed.

Attention to detail is paramount, with a team of qualified and experienced technology consultants to guide clients through a robust implementation methodology. This consultative approach provides clients with a clearly mapped journey against measurable objectives to ensure project success.

The company has placed in the top four of the Deloitte Fast 50 for the last two consecutive years, making it one of the UK's fastest growing software companies as well on the global stage.

Deloitte.
Technology Fast50
UK 2014

UKtech
awards
2015

winner
Cyber Security Awards

intel
Security
Innovation
Alliance

Microsoft Partner
Gold Application Development