How to Mitigate Cyber Threats

Our analysis and solution sets

This document gives a view on how we see customers successfully mitigating cyber threats.
We pay particular attention to Watchguard firewall solutions, vulnerability scanning and other supporting solutions.

Contents

1 Introduction

This document discusses our view of current security threats, and how we leverage multiple solutions and techniques to mitigate these cyber threats. We identify a few of these solutions and outline some of the features we see adding the most value.

2 The current landscape

There is no denying that security is of critical importance today. There are many breaches, exploits, and bad guys, vying for your attention. Perhaps this correlates to the rapid pace of software development and deployment, with things like DevOps, or perhaps it's because systems are becoming increasingly complex, or perhaps it's because doing bad things is easier than it's ever been (with off-the-shelf services like Ransomware as a Service/RaaS). Whatever the reason, or combination, security is something that should not, and must not, be overlooked or underestimated.

And whilst that's easy to say, what does it mean? What does good security look like? As is often the case, the answer will likely depend on each situation; there isn't a one-size-fits-all solution that is right for everyone. And we must be realistic, we know there will always be a balance between cost, and level of protection. Understanding environments, policies, procedures, culture, data, risk, and threats are critical to be able to make that informed decision.

That said, there are common threats and proven techniques that do help mitigate cyber threats. It's also important to realise that a lot of attacks or security events could have been prevented by taking simple security measures. It is these sorts of measures that we focus heavily on, because they are commonly overlooked, and also relatively easy and cheap to implement.

Security protection is multi-layered. Firewalls to protect security boundaries, email filtering, web filtering, endpoint protection, server protection, static analysis, AI/ML analysis, human analysis, physical security, device security, account security (complex passwords, passwordless, multi-factor), application security, encryption. All these layers aim to make it increasingly harder to "get in" or get access to systems or data.

However, the usual pressures still apply. Budgetary constraints, workloads, business priorities, evolving infrastructure and interdependencies all add up to making the obvious and simple, quite hard to achieve.

3 Solution sets to help mitigate cyber threats

3.1 Firewalls – Watchguard

Even in the current world of "Cloud servers" and a "work from anywhere", firewalls still have a significant importance. These have evolved from simply being an allow/deny device, connecting users to services, to now dynamically inspecting traffic for malicious looking activity, blocking threats, performing behavioural analysis and reporting duties. And firewalls aren't just necessary for the permitter of your network. There are still many threats, that can happen from within your network; this isn't necessarily staff members with a grudge. Threats can still make it through your defences, despite all the layers. And when they do, these breaches can be used as beachheads to launch further attacks. For instance, ensuring users can only access the services they need within the network, will limit the "blast-radius", or make it considerably harder for the threat actors. This is analogous to the tried and tested use of DMZs for publicly accessible services.

From our perspective, often we leverage Watchguard firewalls for our customers and for our customer-hosted environments within our Datacentre solutions. These platforms have given us a time-tested reliable solution with the following benefits.

- Available as both physical and virtual appliances
- An intuitive interface for administration, reporting, configuration reviews, and quick to learn for non-specialist staff
- Firewall polices can be saved and reviewed / edited offline
- The WatchGuard management server allows central management / logging of local and remote firewalls over secure VPN tunnels
- An array of security features are available, dependent on packages purchased, but even the basic package has some great protection features included
- According to Duo, at the start of 2019, around 87% of all traffic was encrypted, and this will only increase. WatchGuard devices consistently deliver outstanding throughput when utilising extra security features, compared to similarly priced devices. This is important as customers need to start utilising packet/content inspection to catch the 'nasties' that could slip through in encrypted traffic.
- Cloud Visibility/Dimension can supply summary or 'Executive' reports, which can be set up in a few minutes.
- Good Branch Office VPN compatibility with other vendors
- Upgrade / replacement is easy i.e., configuration of older device / different model can be saved to a new or replacement device
- AuthPoint MFA is great and simple to use addition, giving a well needed extra layer of defence on the VPN (remote access via the SSL VPN is very quick and simple to set up).

- Excellent support experience – when you need to call on support, they are quick to respond and always helpful. This isn't always the experience with manufacturers in the IT sector, more so in recent months.
- Watchguard hit a great price point, for a fully functional firewall solution

3.2 Endpoints – Sophos plus MTR

The endpoint is one of the layers of defence that, if threat actors get to this point, is getting a bit too close to home. Ideally you will stop threat actors as quickly as possible, and not have to rely on this layer. However, once a breach gets this far, it's critical that is it contained. However, attacks at this level can be incredibly varied, not just attacking local files or network shares, but also acting as a beachhead to attack other internal systems, perform reconnaissance, or exploiting other vulnerabilities in other systems.

Another benefit of securing the endpoint is that it doesn't matter where the endpoint is connected; you could be in the office, at home, in a coffee shop, tethered to your phone, or in a foreign country, endpoint protection will still protect your users, devices, data and systems. A strong cloud-managed endpoint security solution is essential to support this. Endpoints must be able to get updates, configuration changes and be able to report their health, no matter where they are connected.

Our preferred endpoint security platform is Sophos, with which we see excellent levels of protection, reliability, and critically, investment in research and product development. It's essential for a company in this space to always be ahead of threat actors, but also not be getting in the way of day-to-day activities.

Along with advanced endpoint protection, through automated detection and remediation, we also strongly recommend the Sophos MTR service (Managed Threat Response). This is a managed service run by a highly skilled and experienced team of engineers that sit alongside the advanced automated process, to ensure that a human element of control and analysis can be applied. The idea is that the Sophos MTR team can act as first responders in the event of a detected threat and apply their collective knowledge from all their data points to your environment to ensure threats are detected and handled as swiftly as possible, utilising all the tools and best practice available within the system.

3.3 Mobile device management – Intune

Mobile device use is expanding, and mobile devices are becoming more advanced, powerful and capable. It may not be too long before your mobile device could become your main computing device, leveraging connectivity to external peripherals, screens, and cloud computing, to bring you your computing platform. However, I've thought that

for a long time now, and it's not quite mainstream just yet, but the likes of Windows365, advancing compute power and standardisation, perhaps it's not too far away!

As the usage of mobile devices continues to advance, and data becomes accessible via a myriad of channels, securing those devices, ensuring they are updated, meet with compliance requirements, and can be tracked, are of increasing importance. A reduction of support effort can also be achieved by ensuring mobile devices meet a standard configuration, and applications are automatically deployed to end users.

Being able to report on the compliance and health of these devices is critical for audit processes.

Our chosen platform in this space is Microsoft's Intune, or Endpoint Manager. The vast majority of our customers are within the Microsoft ecosystem, and often have licences for Intune available within their product bundle. Intune has been developing at a rapid pace within the last 2 years, and is now a very capable MDM, and MAM (mobile application management) platform.

3.4 Patching

If you subscribe to any vulnerability notification services, you will have noticed the explosion of vulnerabilities that get reported each week. As I mentioned previously, it's possible that the rapid pace of software development creates a double-edged sword. On one hand, rapid development allows for progression; features and value can be delivered quickly without waiting for large updates with long-lead times. However, the rapid rate of change also introduces challenges. Whilst continuous integration testing can help in identifying issues, no code or person is infallible, and it seems a lot of coding mistakes still make their way in to code that is released.

For each vulnerability, or collection of vulnerabilities, a patch is usually provided to address the issue. For each patch, you need to understand what the issue is, if it applies to you, what the implication of applying the patch will be, then applying the patch and further testing to ensure it hasn't broken or altered anything. And all of this process needs to happen in a reactive manner, as close to the announcement of the vulnerability as possible. You can't forecast the rate, or size, or effort required to apply these patches.

One thing is certain, you need to keep up to date with patching, and patch early and often.

Unlike a lot of security areas, this is one that doesn't have a strong product offering. We have developed our own patching service, that will ensure your environment is kept up to date and patched. This service is typically customised to customer requirements and

systems, as there are a large number of variables involved. However, this next section is one area that can provide checks-and-balances that this process has been working and spot any areas that need attention.

3.5 Vulnerability scanning and penetration testing

These are two separate but arguably related areas. Following on from the patching section above, vulnerability scanning, broadly speaking, is simulating an attack from within your network. This will probe for known services and vulnerabilities, and test to see whether your systems are susceptible to them. The idea being that this process will identify these issues before the bad guys do! Quite often, we see customers aren't aware of every device that is connected to their network. So, the vulnerability scan can also provide a useful insight into what is connected, as well as giving an understanding if any devices are susceptible to vulnerabilities.

Penetration testing, on the other hand, is useful for testing externally presented services. Ensuring that your "front of house" systems, the one the public can access, are free from bugs or vulnerabilities. Both vulnerability scanning and Penetration testing are specialised areas that often require a customer-specific engagement, particularly with Penetration testing. Penetration testing can be similar to the internal vulnerability scanning, whereby external IP addresses can be scanned for known services, and then checked for known vulnerabilities. However, it can (and should) also go deeper into the application that is being exposed. For instance, a web server may be secure, it may be fully patched, there may be no active/known vulnerabilities. However, if the application code that the web server is serving is full of holes, like buffer overflows, or SQL injection, or just poorly written, then attackers could easily perform malicious and unauthorised activities.

We partner and work closely with our friends and experts at PenTest People for both these services, as well as for Cyber Essentials and Cyber Essentials Plus cyber audits and accreditations.

3.6 Multi factor authentication - AzureAD

Arguably, I've left one of the easiest topics until last. It's still shocking how many attacks take place because either MFA was not setup or had been disabled for some accounts.

The move to Cloud services has enabled advanced features like MFA to be enabled with relative technical ease. Historically, trying to enable additional security features on your on-premise solutions would require significant investment in time, products and training. Cloud services can deploy these to all customers on their platform. MFA has been

available for the likes of Office365 for a considerable time, and with the addition of AzureAD P1 licences, other Cloud or on-premise solutions can leverage Azure AD MFA as well.

There should be very few, if any, excuses for not enabling MFA for your email accounts if they are within the O365 environment. If this has not already been done, it should be investigated as matter of urgency. Microsoft reported that 99% of account compromises could have been prevented with MFA. Extending Azure AD MFA to other systems should also be considered, as a single platform will ease the end user experience i.e. a single MFA app to deploy, or a single authentication mechanism (e.g. SMS or phone call), and a single user enrolment process. A single platform will also aid the IT administration effort needed as well.

4 Summary

This document has been a high-level run through of some of the products and services that we utilise to mitigate cyber threats for our customers. The aim being to highlight some of the quick-wins, or absolute must-haves, along with tried and tested solutions within our portfolio.

By implementing these products and services, your cyber threats will be reduced. This is by no means a guarantee that they will be eradicated, but they will go a long way to securing your environment, users and data.

To learn more about how PAVilion can help support your organisation, please contact info@pav.co.uk

pavilion

Pavilion
Sunny Bank Mills, Farsley,
West Yorkshire, LS28 5UJ

Tel: 01273 834 000
Email: info@pav.co.uk
Url: www.pav.co.uk