BIOS

Be secured. Be assured

Microsoft 365

Data Loss and Security

Understanding Microsoft's obligations and how that impacts your organization

CONTENTS

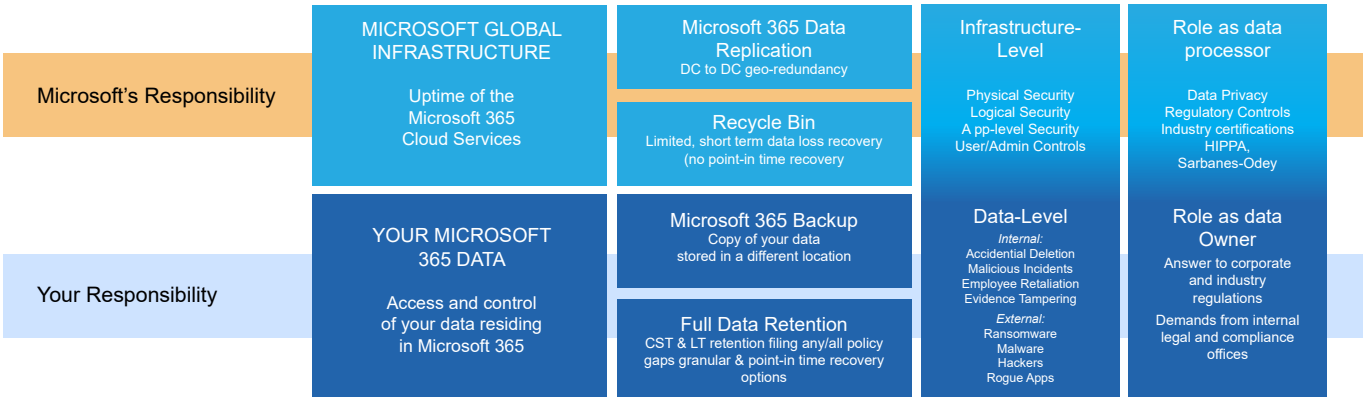
Introduction

There has been mass adoption of Microsoft365 across the region due to the increased drive towards online collaboration. Primarily to support the needs of the post-pandemic workforce such as remote working, online meetings and easy access to corporate files and email anywhere on demand.

M365 has been a great catalyst in that regard, but it has also introduced significant risk to customers, often without their knowledge. Services which used to be hosted in your datacenter are now delivered from a user interface on a SaaS platform. Which is great because all of the controls I need to protect my data and intellectual property on that platform are included as standard. That is the vision that is often sold to customers, the reality is quite different.

Is your data secure on M365?

It is worth searching online and reading up on the Microsoft Shared Responsibility model (below is a graphical representation for reference). In essence when you use the M365 service, Microsoft's obligations are to provide the platform, making sure it is online and available. The responsibility to secure your individual tenant and protect the data lies solely with the customer. Most customers aren't made aware of this when they are sold the license.



This means that companies are putting all their file data on One Drive and SharePoint, capturing critical business meeting data on Teams and storing all their Email on the cloud without proper security or indeed backup.

Take backup for example, when you had email, file storage and SharePoint in your own datacentre, you had a backup that was taken at least every night and kept multiple historical versions as an archive on a separate disk subsystem using a backup software. Sometimes you'd take that backup to tape and store it offsite and/or have a replica to another datacentre for disaster recovery. All of which are controls designed to reduce the risk of data loss and the negative impact that can have on the business.

By comparison the native M365 deployment only provides a Recycle Bin for restore. The Recycle Bin only stores the most recent copy of the data (the version of the file when it was deleted) for a period of 14 days, after which it is wiped from the platform and completely unrecoverable. This means that any email or files that are accidently deleted or overwritten may never be restored. So, a 14-day window to only recover the latest version of a file, with no versioning, no archiving, therefore no legal discovery capability, that represents a huge risk.

Many customers are mis-sold M365 without backup in place, many of whom find out about the recoverability challenges when it is already too late. Thankfully there is an easy solution to remove the risk from your business.

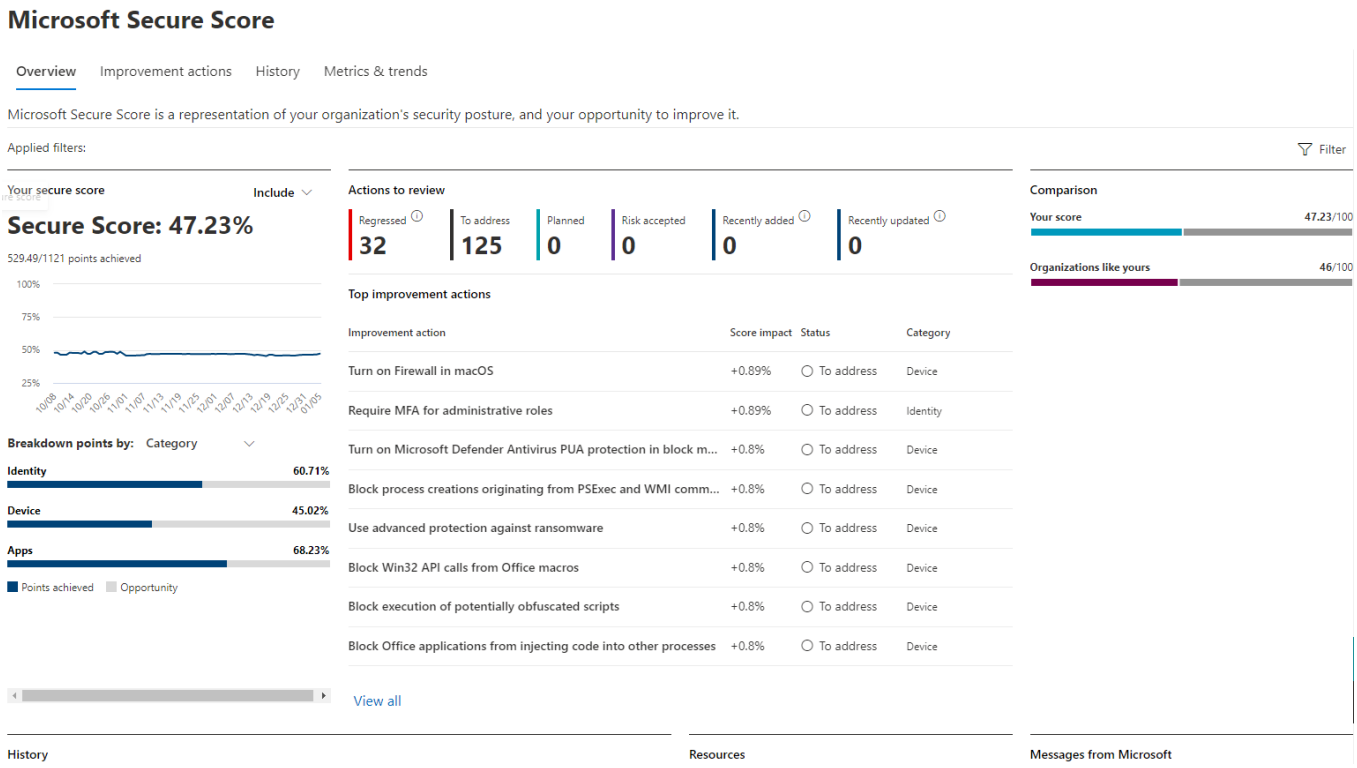
BIOS have a long-standing partnership with Veeam Backup. We use Veeam to protect thousands of virtual machines on CloudHPT across all our datacentres and accordingly they are our vendor of choice for backup on M365.

Our Veeam backup service includes deployment of your own dedicated Veeam server on Azure in UAE. Where we connect it to your M365 tenant and securely backup your data to Azure Blob storage. This provides the most cost-effective solution for data backup. It is then managed on an ongoing basis by BIOS as a service, making sure backups continue to function and the Azure consumption is controlled so costs do not spiral out of control. Also, by using a managed service from BIOS you will receive a more secure model for data protection. We ensure that different admin credentials are required to access the backup server and data. If you are compromised by an attacker, they will not be able to log into the backup server and delete the backups, which is a common tactic deployed.

Other security concerns

In addition to backup there are other controls that should be deployed to ensure you have a secure M365 tenant. Security for M365 is important as it not only is a store of your corporate data online, but it is also linked directly to your users machines and your Active Directory. Any exploit on M365 can easily traverse the entire organization causing immeasurable damage to revenue, brand reputation and customer relationships.

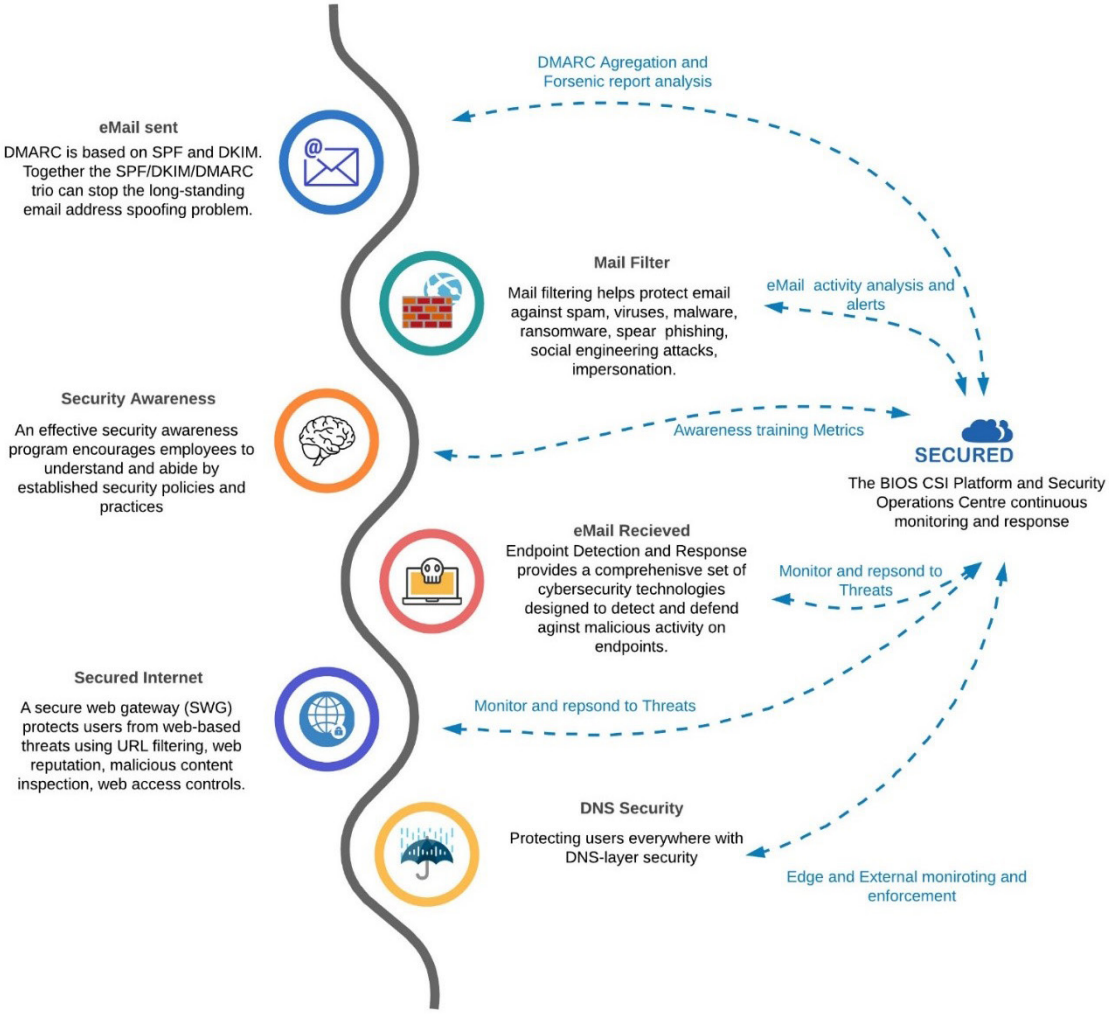
A good starting point is to have your administrator check your secure score.
Log into https://security.microsoft.com/securescore as the M365 admin and you'll be able to see the secure score for your tenant deployment.



The portal details configuration items and features that may not be configured correctly or even enabled. BIOS can undertake this process for you and give you a list of recommendations including additional services that protect your organization from threats which target M365. These recommendations are then mapped to our Security Operations as a Service offering BIOS CSI.

The concept of Continuous Security Improvement (CSI) is to focus on the 'kill chain' or the taxonomy of modern attacks that are borne of email and stolen credentials on M365. Using various controls for blocking, alerting, logging and auditing, data is fed into our NOC&SOC service that provides 24x7 incident management and remediation services.

One of the most common ways customers are compromised is having weak password policies and no multi factor authentication deployed. Imagine a scenario where your M365 admin uses his corporate email address and password to sign up to another service online (we've all done this before right?) and that website gets compromised and the authentication data is stolen. 9 times out of 10 an attacker will try those credentials on M365 log in screen. If they can log in as an administrator then its game over, all your security is bypassed and they can create additional super user accounts so that even if the admin changes his password they still have access. This is how a lot of business email compromise happens, which in 2021 cost the US economy $3bn alone.



**Security Kill Chain for M365*

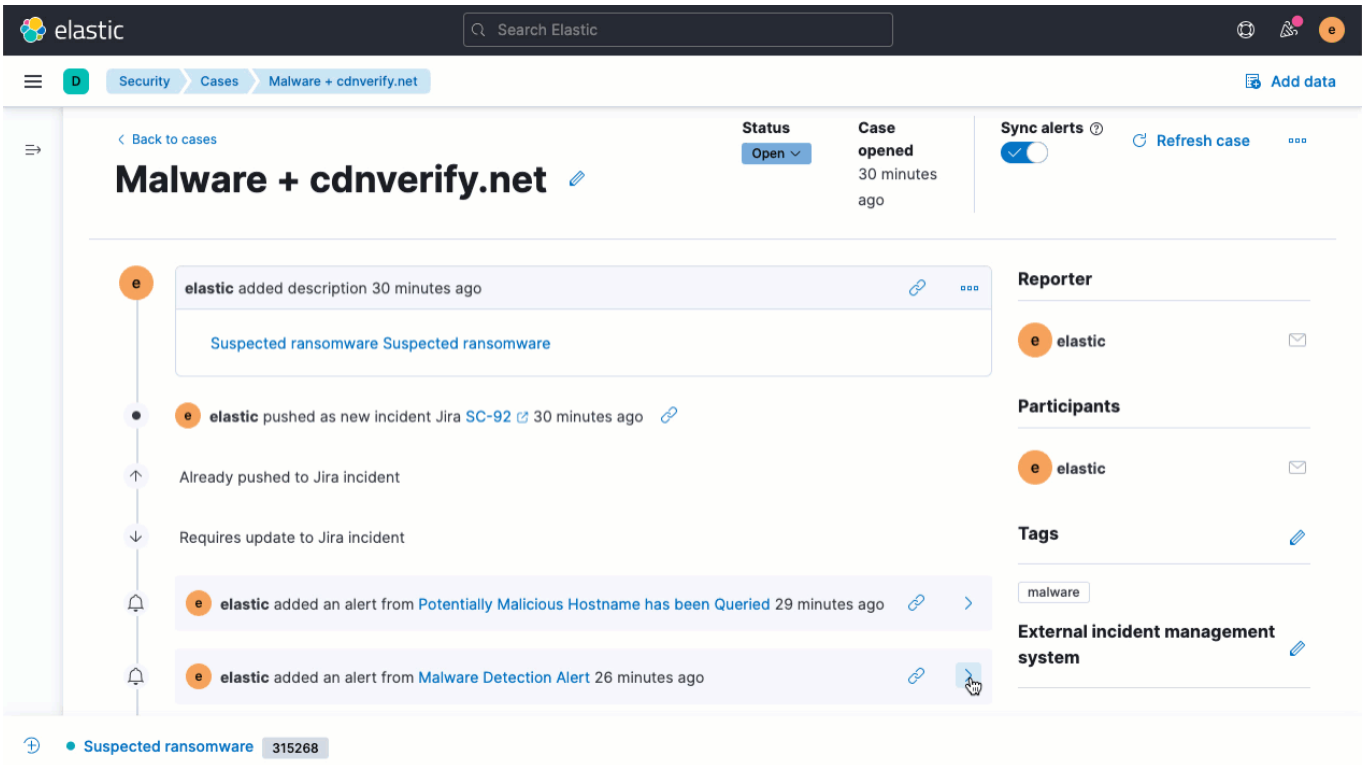
Compromised credentials can be mitigated with MFA, but what about Phishing and other malicious activities? No email security platform is 100% secure, the techniques used to detect spam, phishing and other malicious email rely in part on the user to fill in the gaps. As malicious emails still land in the inbox we need to consider other controls to mitigate late stage threats. These controls broadly fit into 4 solution sets:

1. EDR/XDR
2. MDR
3. DNS Security
4. Active Directory Auditing

EDR/XDR

End Point Detection and Response (EDR) agents will monitor and block malicious and suspicious processes running in memory on the host. BIOS's Elastic XDR (X for extended) provides EDR functions and also sends logs to our SIEM as a Service platform (in CloudHPT) for event correlation against other event sources. Correlation against firewall and active directory logs using machine learning, provides a way to process massive volumes of data to identify patterns/signifiers that a system has been compromised by a more sophisticated attack. Having this data then interpreted by qualified SOC engineers who in turn have access to data across hundreds of customers helps identify areas for improvement through hardening activities across the IT estate.

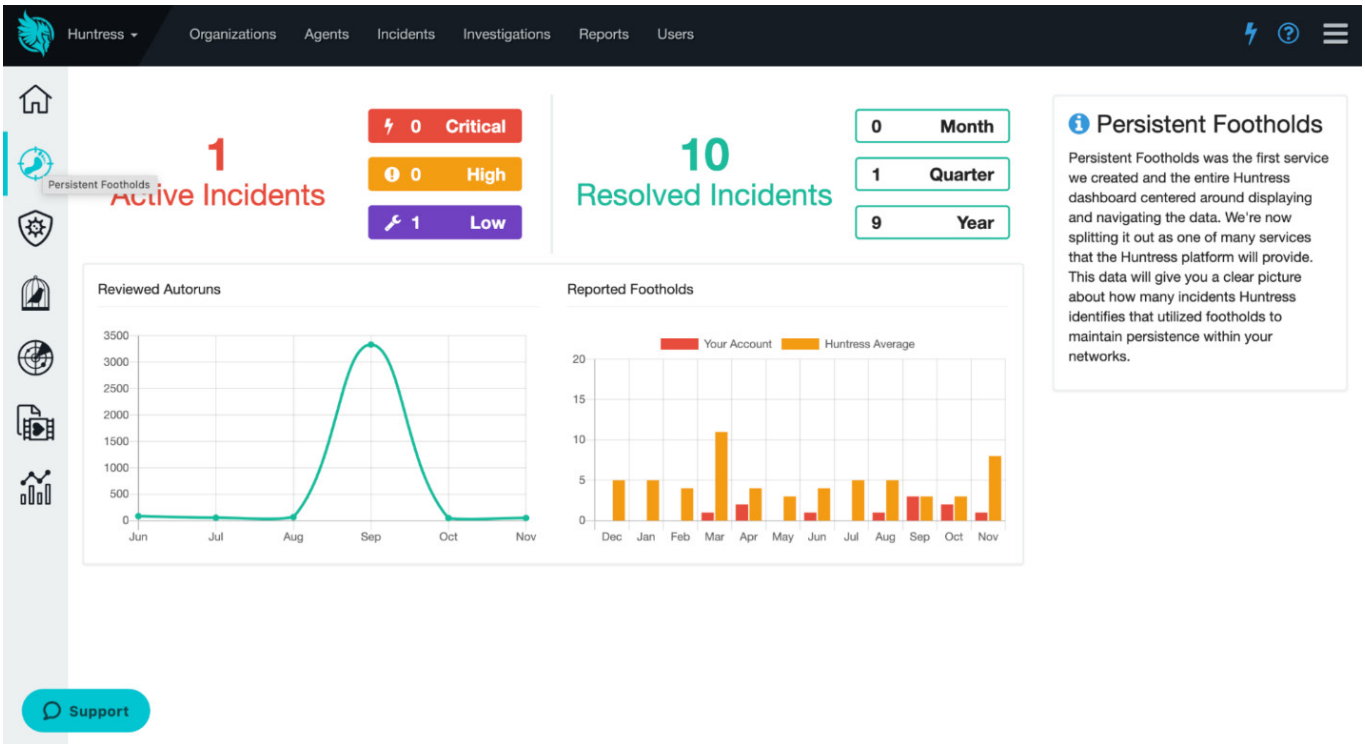
From a compliance standpoint, our XDR provides 12 months log retention in the SIEM giving additional benefit over a standalone EDR platform. Elastic also provides file integrity monitoring, dashboards, reporting and trend analysis.



MDR

Managed Detection and Response (MDR) agents go a step further in detecting Windows OS zero-day attacks. They detect suspicious actions in the operation system through behavioural analysis. Specifically they are looking for Windows signed services that are being used in a potentially suspicious manner. Such activities are sent to an active SOC where human engineers will inspect the logs (a process known as investigation). When a malicious action is detected they send the case to your MSP with the steps for remediation. Some products like Huntress which BIOS rely on, have the ability to perform one click remediation of the steps in the ticket, whereby the system automatically resolves the issue once instructed by the engineer.

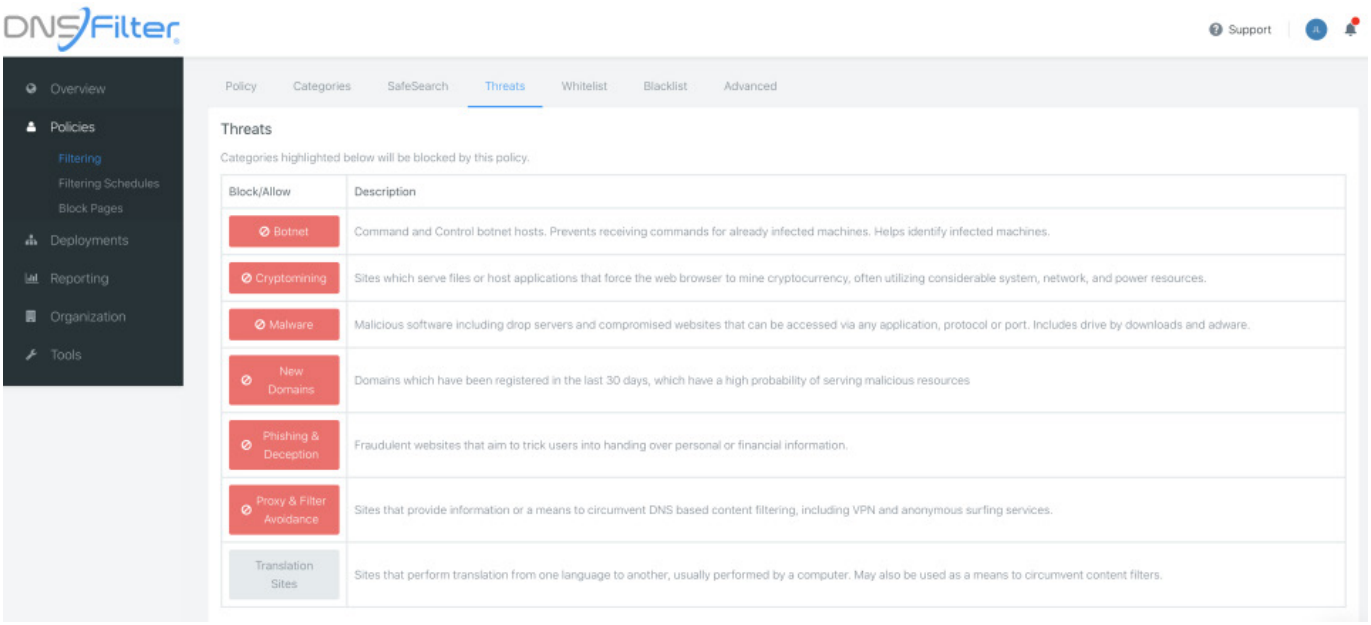
Both MDR and XDR agents are able to isolate machines from the network, allowing only secure access to remediate issues. One-click containment when combined with 24x7 incident response is a powerful tool in remediating issues before they become major security events.



DNS Security

DNS based security compliments email security solutions by adding a last line of defence for user interaction with malicious email and files. A DNS security agent such as DNS Filter will point the DNS resolution of a protected system to the world's largest secure DNS resolution service. This enables policy enforcement based on the reputation of the site, for protection against Botnets, Malware, Phishing, Deception and enforce 'safesearch' on popular search engines.

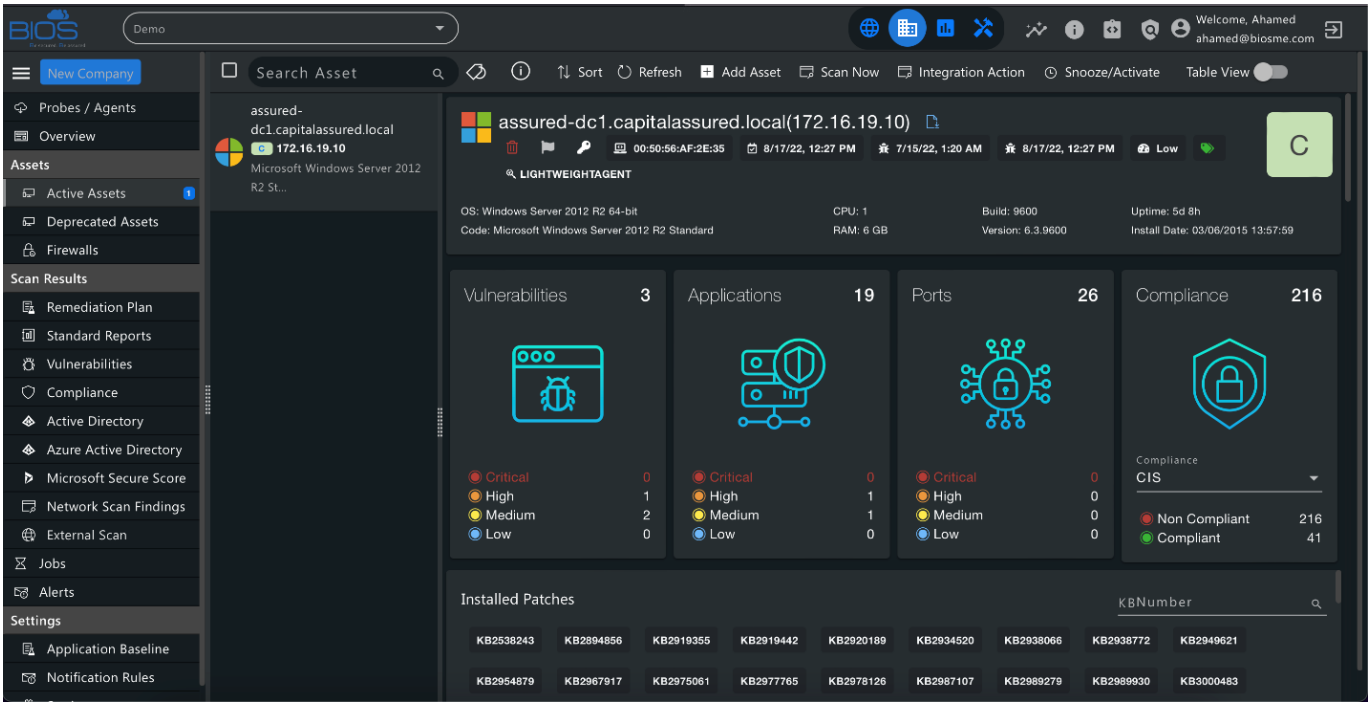
Therefore, if your email user clicks a link or opens and attachment that evaded email security, the DNS policy will prevent resolution of the DNS and protect the end point by blocking the malicious action. Policies can be further customised to block unwanted internet browsing activities such as restriction to gmail or other file sharing platforms.



Continuous Auditing

Adding in continuous auditing to the stack provides visibility about vulnerabilities, shadow IT and changes to permissions in your directory service that may be malicious. Continuous auditing is performed by CyberCNS, through deep asset discovery you are able to perform risk assessments and compliance checks on your active directory and servers/end points. Deep asset discovery checks Windows (WMI, SMB, WinRM), SNPM, UPNP, SSH, ZeroConf and AllJoyn assets to detect vulnerabilities, shadow IT through installed software (whitelist/blacklist) and user behaviour analysis on AD to detect malicious changes.

Continuous scanning provides better visibility of changes in the environment that may be the pre-cursors for attack. By knowing ahead of time the vulnerabilities and risks inherent in the system or suspicious changes that have occurred we are able to proactively remediate through our NOC team. The advantage of having servers on CloudHPT is that we have a 24x7 managed service desk and incident response service already provided to our customers. By adding the data from these various sensors we are able to feed in critical security event data to the operational service to provide SLA backed security incident response.



The combination of these 6 controls into a 24x7 operational security service can greatly enhance your security and reduce your risk of compromise whilst controlling costs.

Contact us today for a free assessment of your backup and security posture on our channels listed.