
8.76
0.11
2.60
6.33
4.72
5.54
4.00
9.66
6.95
2.60
7.49
8.59
1.17
ENCORE

Executive Summary

ENCORE provides a single lens into the organisation's operational security environment. ENCORE covers regulatory and best practice compliance, security control management and action-based reporting, digital foot printing and security infrastructure health monitoring. It accomplishes this by using a combination of innovative toolsets that gather, capture, execute, and visualise data in a logical modular approach.

WHAT IS ENCORE?

ENCORE is a cloud based, secure by design, modular platform that has been custom built from the ground up to address the growing need for operational efficiency and monitoring by visualising information that can be confusing and often overwhelming, providing accurate and action-based reporting and visibility across numerous security controls, through one secure portal.

ENCORE includes the following capabilities:


External Attack Surface


Compliance


Health

ENCORE's capabilities consume and process data from the underlying security controls, custom- built attack capabilities, scripts, and user completed assessments, simplifying a wealth of information so that it can be easily digested by any part of the organisation.

This enables organisations to:

- Speed up their decision-making process with real-time information
- Improve compliance and coverage
- Manage threats and minimise the attack surface
- Create a view into regulatory and audit compliance
- Ensure better ROI from existing investments
- Provide proof and visibility of security

The Capabilities

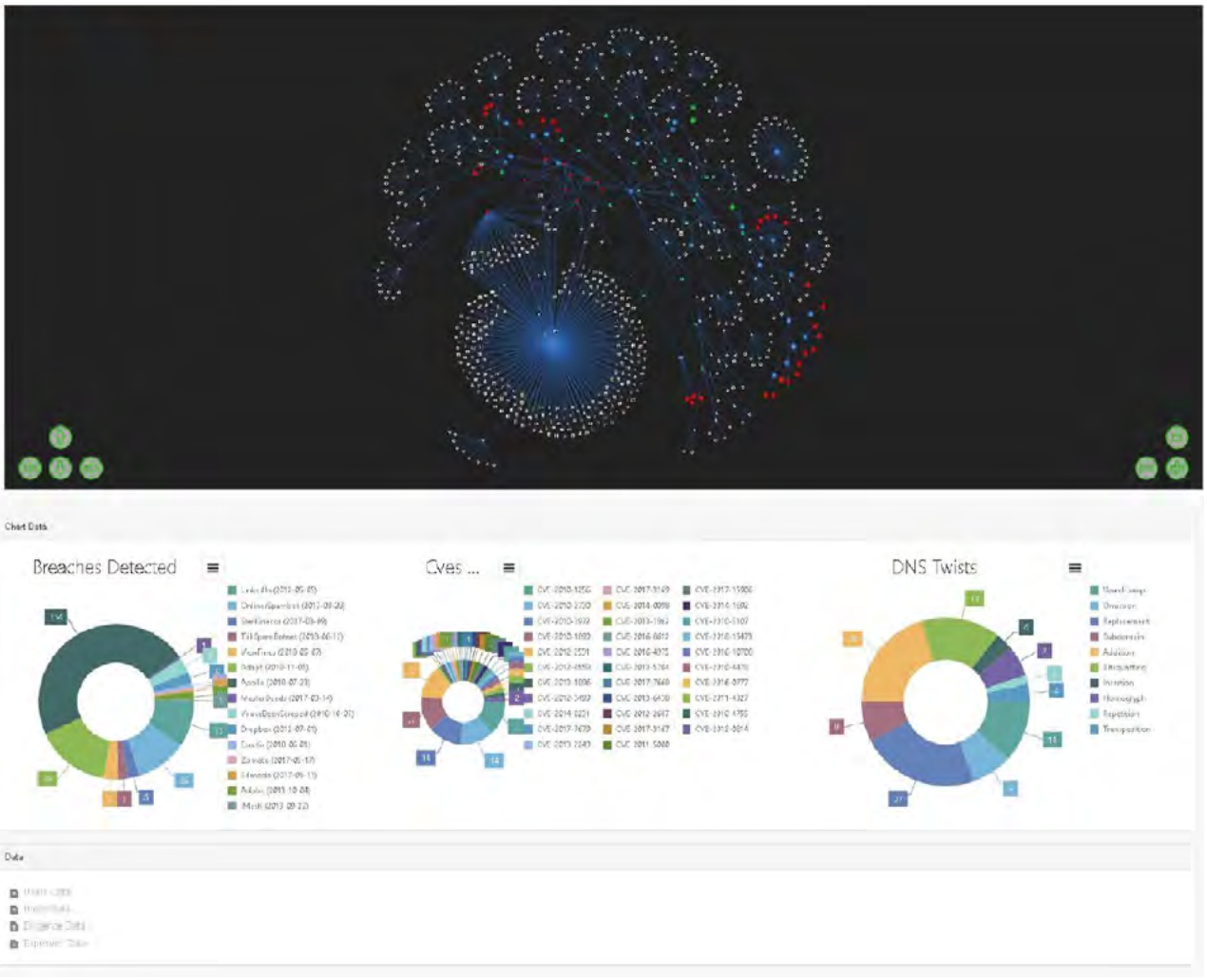
EXTERNAL ATTACK SURFACE

Attack Surface offers the visibility into an organisation's online digital footprint. This is the sensitive data we as humans unknowingly expose ourselves and our companies to. This data an unethical hacker gathers to start their attack on any organisation, regardless of the size.

In many cases attackers are cautious when gathering information in preparation for an attack, avoiding "noisy" vulnerability scanners that can be easily detected by defenders, and instead opting for lower hanging fruits.

The information gathered can be used to combat and mitigate:

- Potential phishing targets
- Potential weak points in online assets
- Potentially leaked credentials of a user that belongs to the business domain, based on data from Have I Been Pawned and data dumps on known breach sharing sites
- The URL's where domain email addresses are listed
- The publicly listed email addresses of the domain
- Potentially linked email addresses of the domain
- Results from cross-referencing gathered email addresses to determine if a user has been involved in a prior data breach
- Publicly available hosts (based on 100-word DNS check) on A records
- Correlated information on each A record
- Pastebin dumps that have links to the domain



COMPLIANCE

The Compliance capability is a single view of an organisation's security controls. This helps reduce the time spent gathering the information from the various dashboards. To gain insight into the current state of the environment which helps give your security team context and assists by providing actionable intelligence.

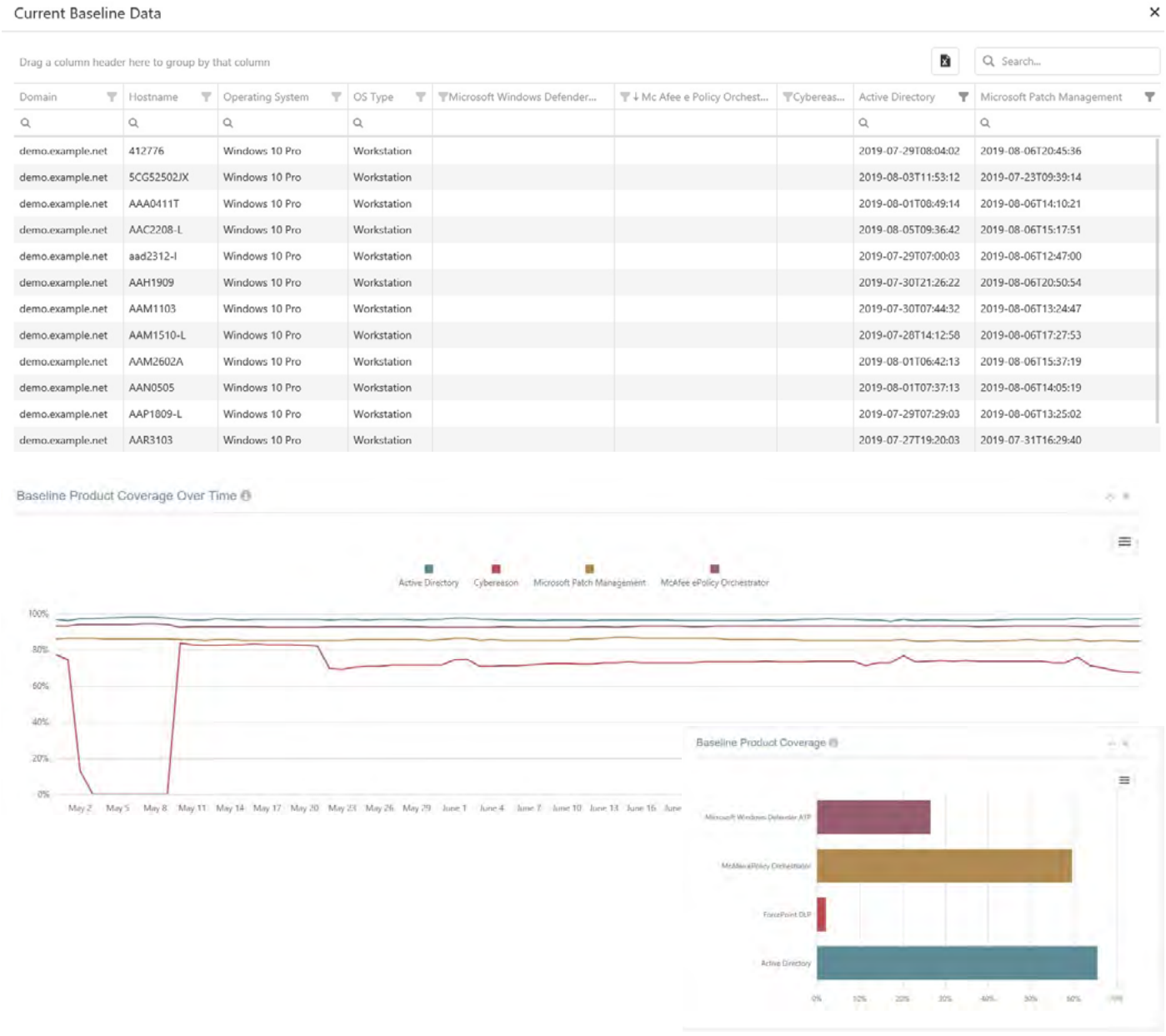
ENCORE has applied deep knowledge and experience in security operations to these lenses allowing for easily consumable reports, metrics, and many features that provide additional context to the security manager, to operations and to the extended business, right up to Board-level.

Operational lenses

Examples of the available dashboards are presented below:

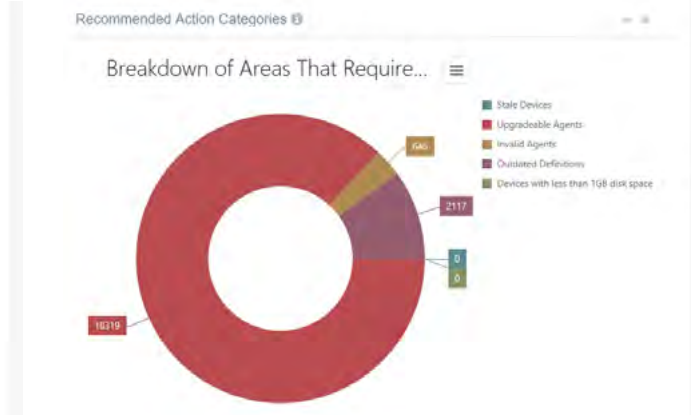
Baseline

This lens is a side-by-side comparison of control coverage, taking data from each security control and correlating it against each other. It provides a view and actionable intelligence of what device is missing what control, while developing an organisational baseline count which coverage can be measured against.



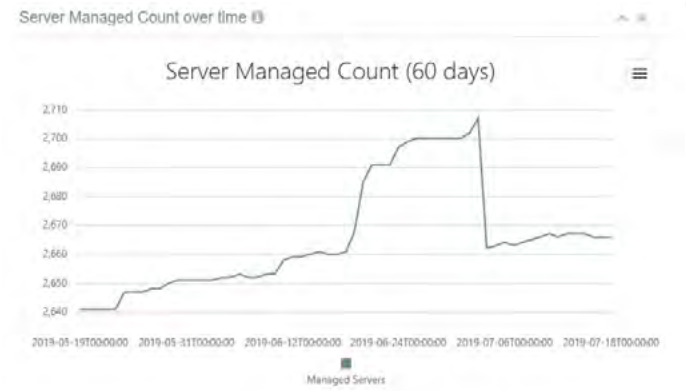
McAfee ePO

The McAfee EPO lens provides an instant, accurate, and consolidated view into operations of the anti-malware suite, offering appropriate measurements, actions and risk views to improve the environment.



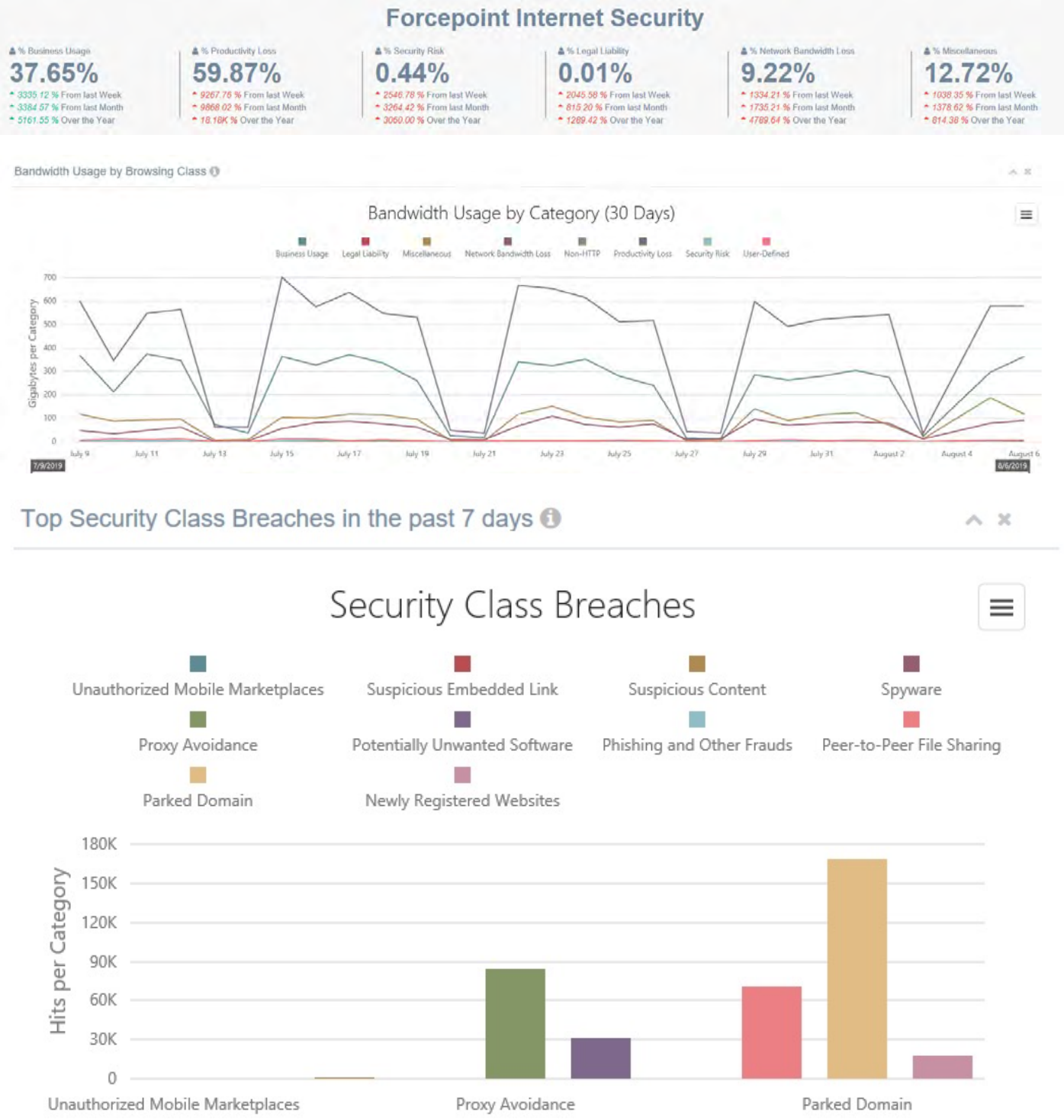
cybereason

The Cybereason lens provides an instant look at the configuration and coverage of the EDR solution within the organisation.



Forcepoint Web Security

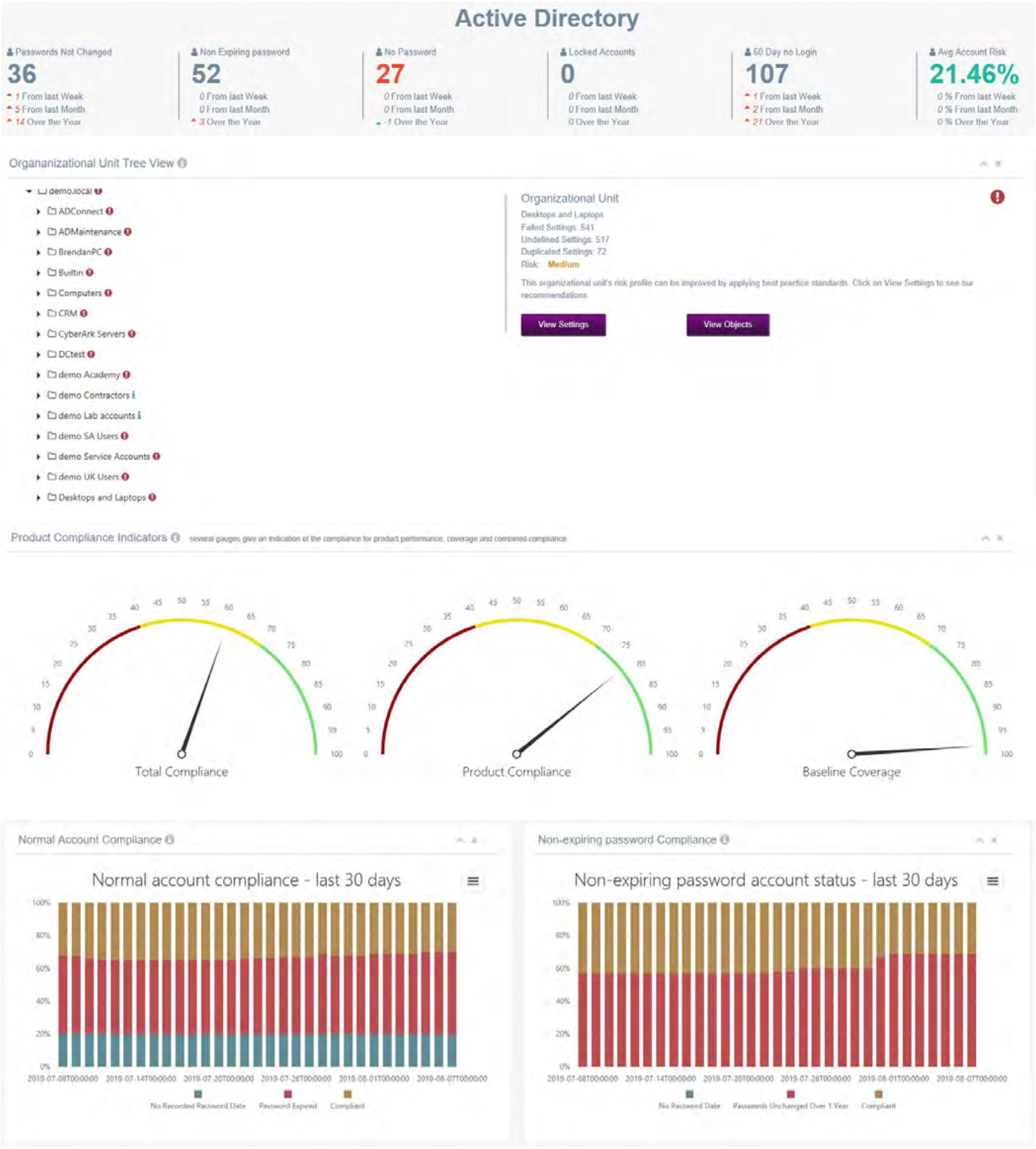
The Forcepoint lens allows visibility into web browsing behaviour and browsing categories, allowing operators to accelerate and enhance reporting and address risky behaviour or legal liability as it happens.



Microsoft Active Directory

The Active Directory lens with built-in security contextualisation provides compliance status, risky account visibility, trending reports, and a weighted risk score. It enables AD administrators to quickly assess the controls and compliance of the domain and to make changes that support security objectives.

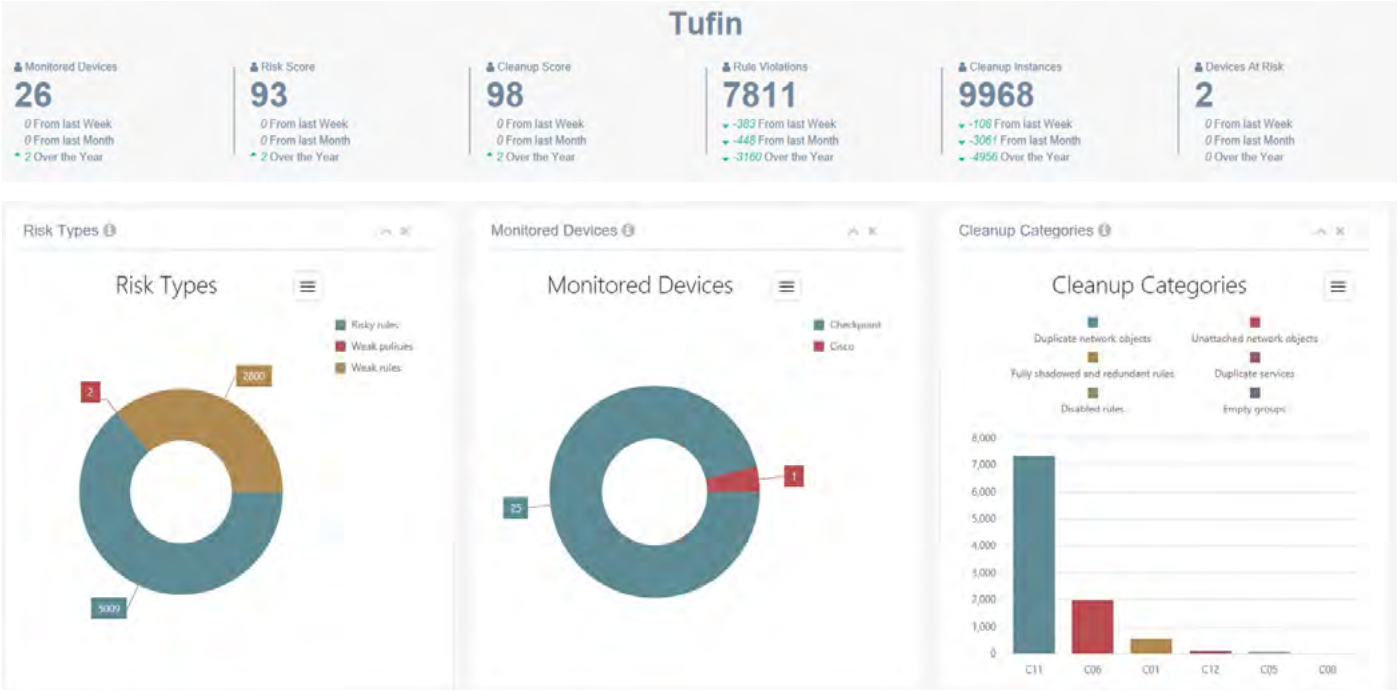
Additional enhancements such as the GPO best practice review and Bloodhound lateral movement add-on make this one of the more powerful lenses within ENCORE.

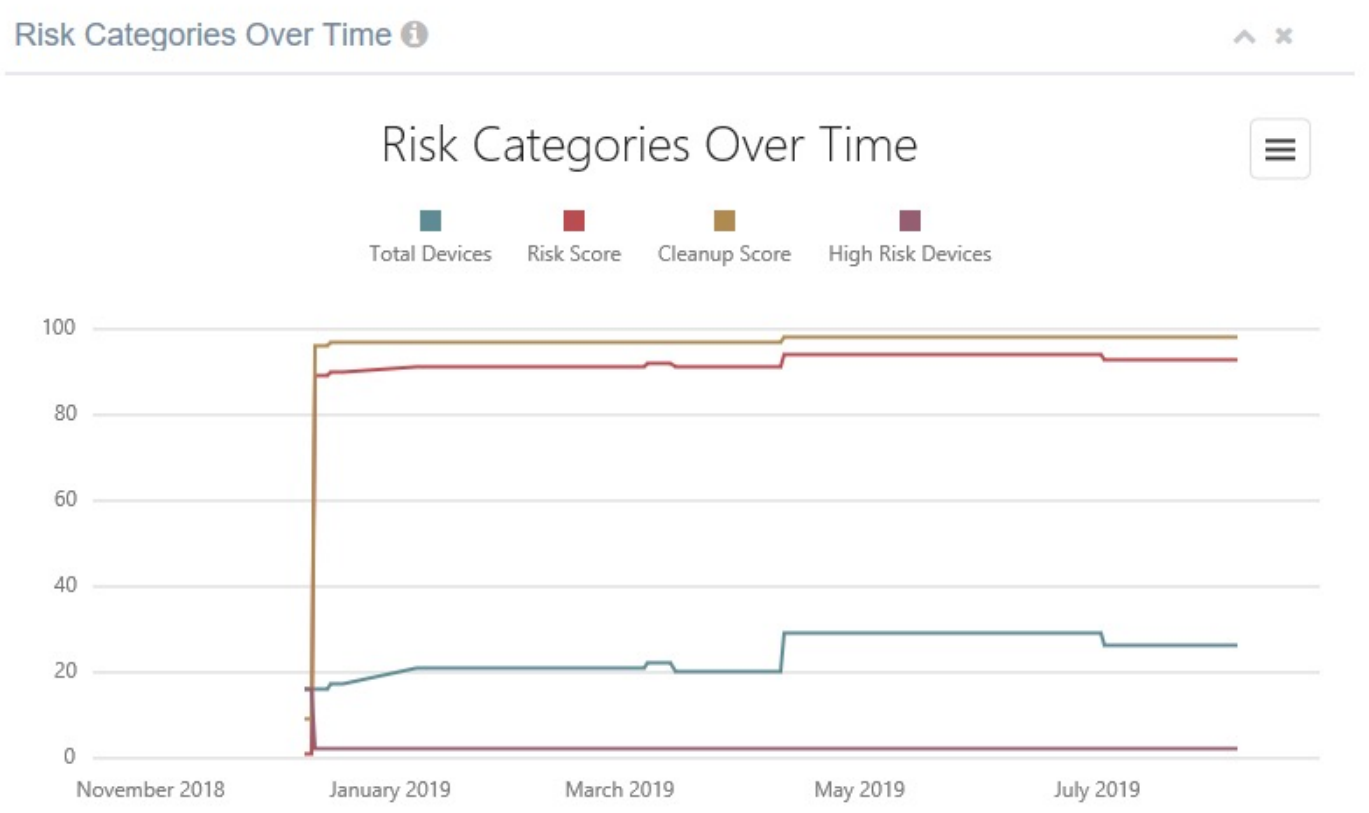


Microsoft System Center

The SCCM/Patching lens provides compliance and risk views of patching cycles, allowing operators to prioritise patches and patch targets by risk exposure.

The Tufin dashboard shows an instant summary of the analysis that Tufin has performed on the monitored devices. This gives an administrator a single visual dashboard that assists in focusing on identified issues, for example risky rules.

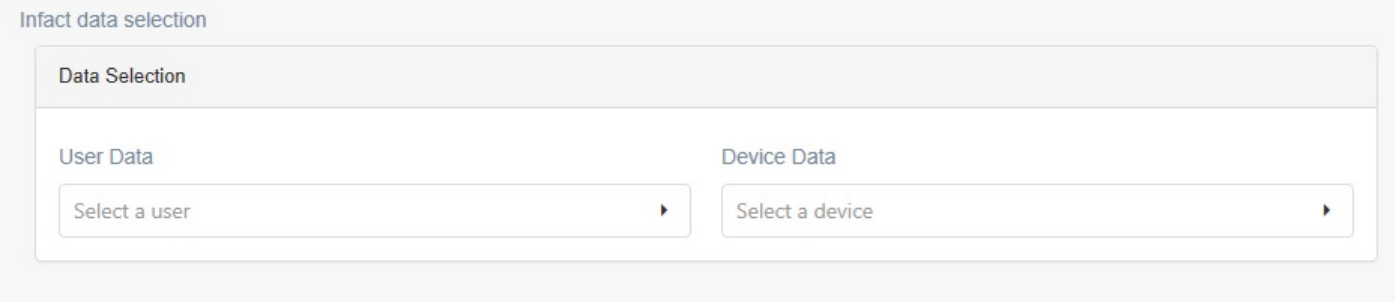


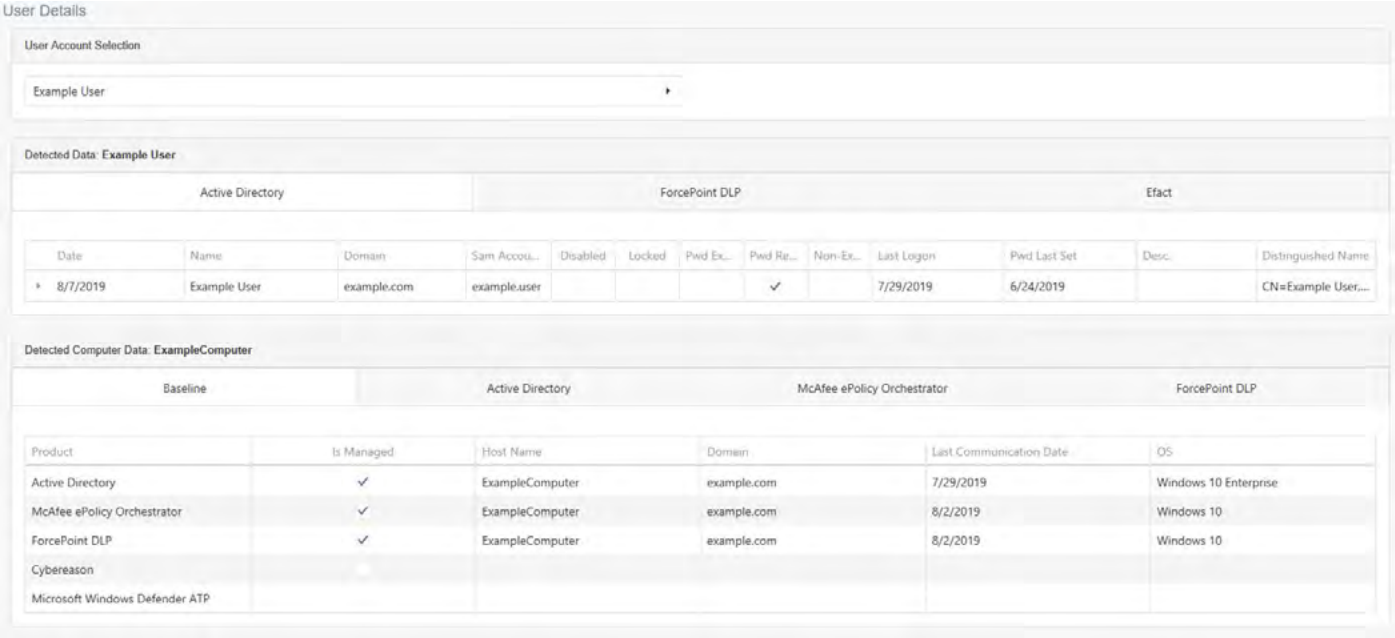


Internal Fast Assessment

ENCORE not only supports macro and micro views per technology control, but also consolidated views of controls per asset or per user, allowing for faster incident response and remediation activities because analysts no longer have to search and correlate data across multiple systems and platforms. This feature enhances incident response activities, and allows a targeted view across all platforms in ENCORE, including the external Attack Surface

The additional advantage of selecting both the Attack Surface (Digital Footprint) and IFA modules is the combination of this data, allowing organisations to quickly identify and match users that have been exposed to breaches, and/or would be likely candidates for targeted phishing, and then matching this external profile to the internal asset and the compliance of that user, thereby allowing targeted risk reduction and awareness campaigns to be performed. This capability is included free of charge, should both ENCORE and External Attack Surface be purchased.





Data Collection – how does it work?

The compliance framework requires read-only access to the systems that support the installed controls or management consoles (if an API is present).

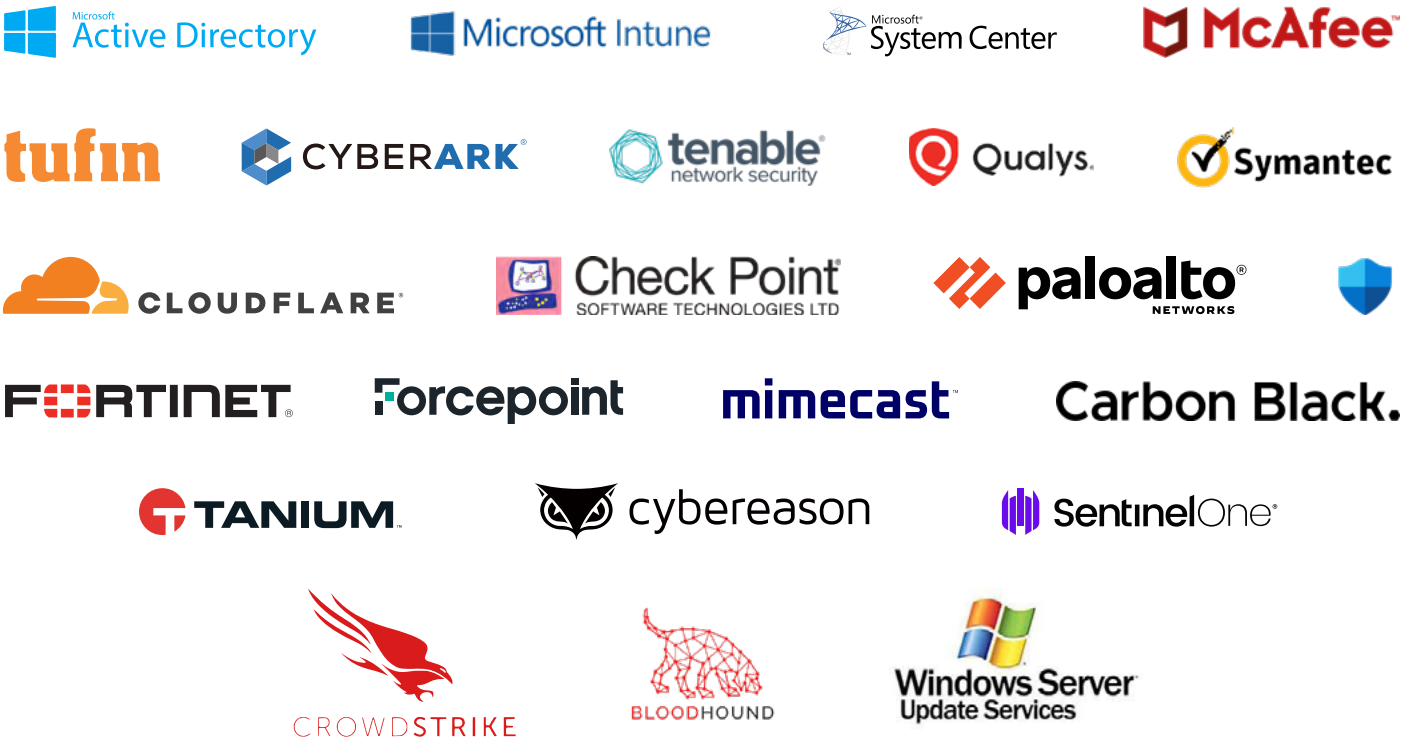
All that is required on the network is our collection agent that runs on a Windows server. The agent uses security keys and other forms of encryption to ensure that all the data is collected and stored in the cloud service safely and reliably.

Supported Products

The examples shown in this document are not exhaustive and product integration work is active and ongoing.

If there is a demand for a new product or feature, there is a team of developers who can tackle the integration.

SUPPORTED TECHNOLOGIES

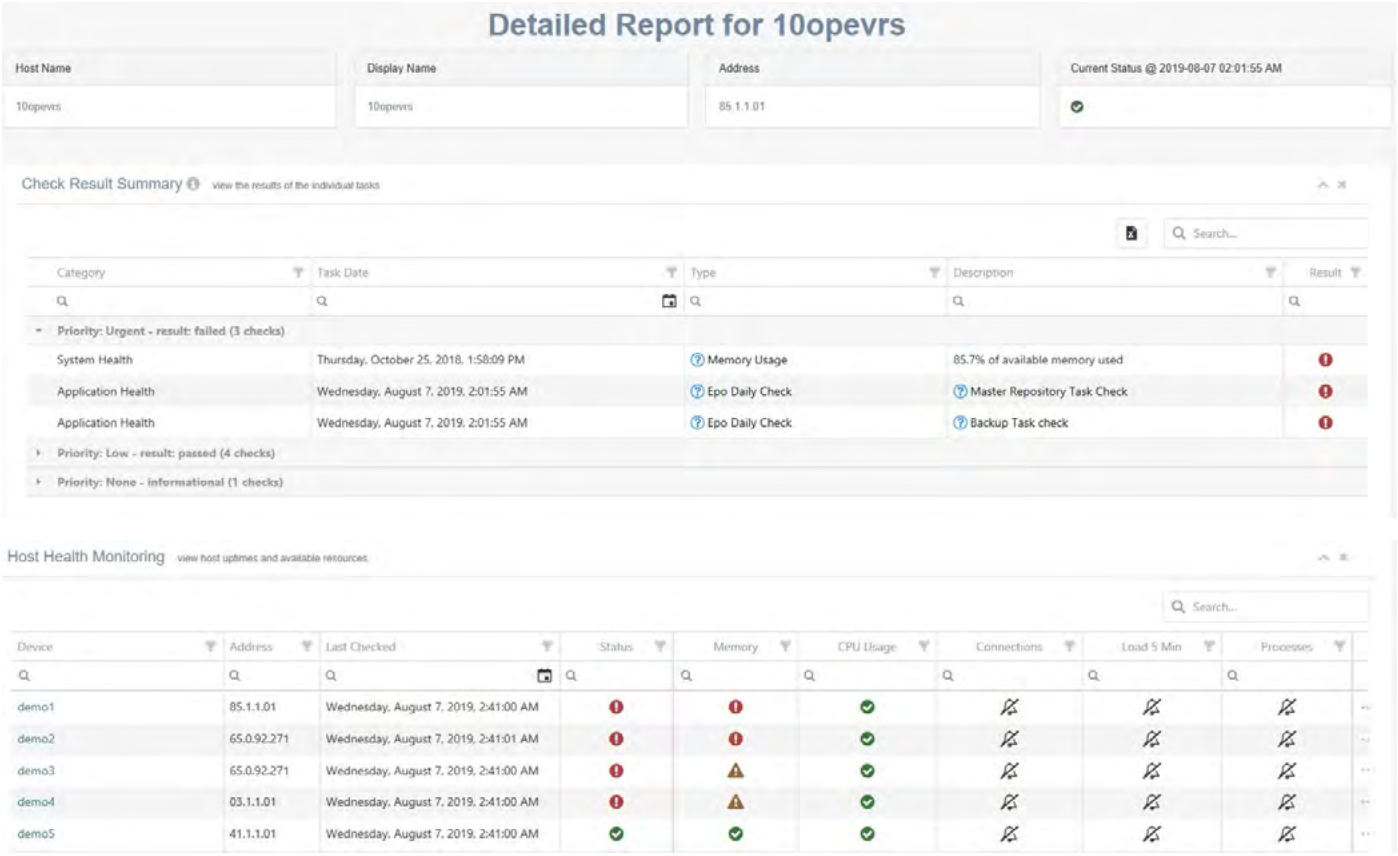


HEALTH

The health framework provides security, network device, server resource utilisation, and threshold alerting, providing SNMP and agent based monitoring across a client's estate, allowing configurable and action-based alert management.

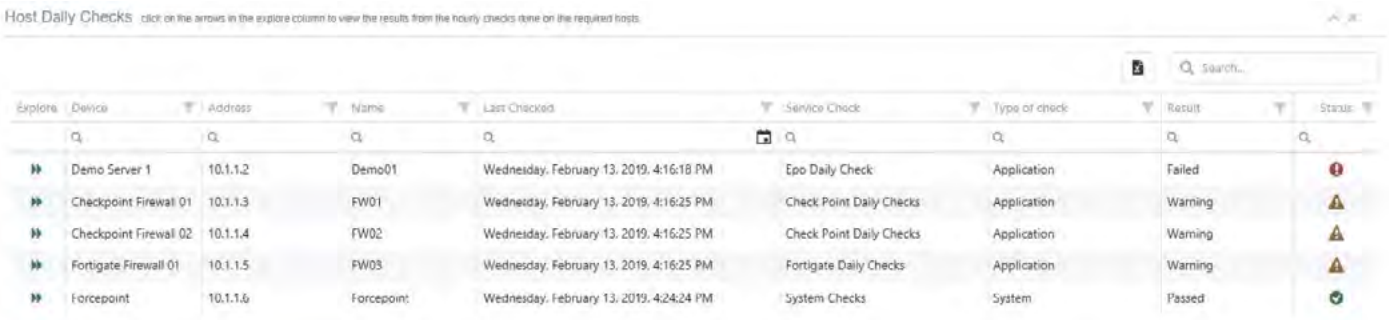
Monitoring

The below shows an example dashboard for the SNMP or Agent based monitoring solution for a single host.



Automated Checks

Ensuring that applications are working correctly goes further than simple availability: ENCORE addresses proper application checks to ensure that the application itself is ready and able to work. The below picture shows an example summary page showing the status of automated checks.



REGULATORY CAPABILITY

The regulatory framework allows clients to quickly complete assessments online, providing visibility into current compliance and measurement against the organisation's industry and recommended compliance levels. All assessments are self-guided, and are easy to use and navigate.

Below a sample report of GDPR compliance:

Controls	Score
Group: Personal Information Management System (Controls: 3)	Score: 5.00
Group: Legal (Controls: 13)	Score: 2.16
Group: Process (Controls: 14)	Score: 2.49
Group: Technical and Technological (Controls: 5)	Score: 3.01
	Total Score: 2.66

Is my data in Encore safe?

The short answer is, yes it is. Some of the features are listed below:

- Separate and isolated database per client
- Role based access control
- Secure login, including Two Factor Authentication (2FA)
- Application behind layers of security including:
    1. Web Application Firewalls
    2. Next Generation Firewalls
    3. Database Activity Monitoring
    4. Encryption of Data In Motion


ENCORE
www.encore.io