



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

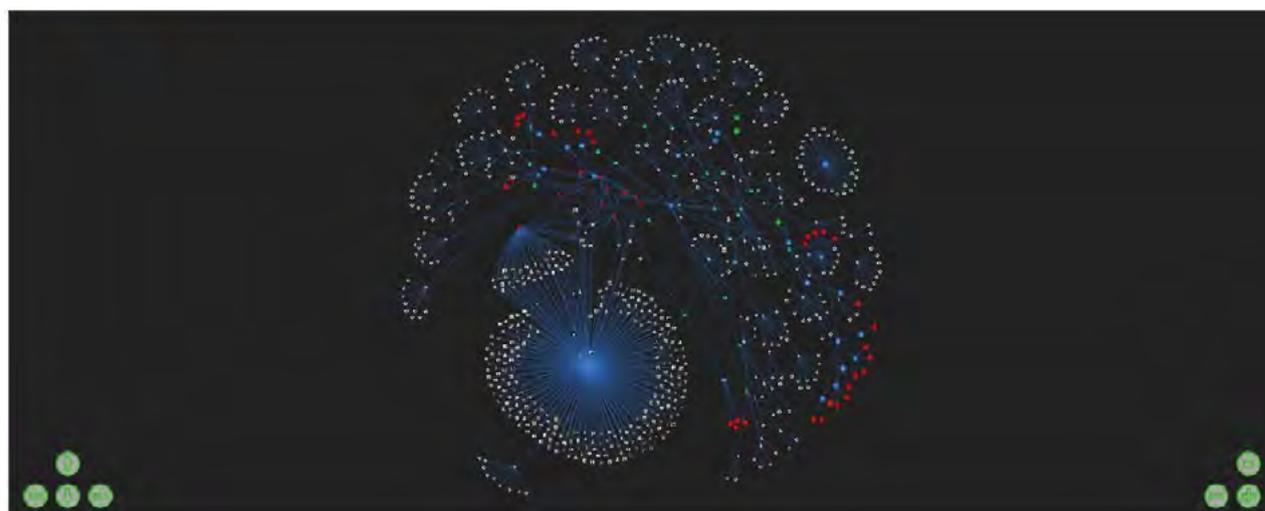
Attack Surface offers the visibility into an organisation's online digital footprint. This is the sensitive data we as humans unknowingly expose ourselves and our companies to. This data an unethical hacker gathers to start their attack on any organisation, regardless of the size.

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 Pwned 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.

Current Baseline Data

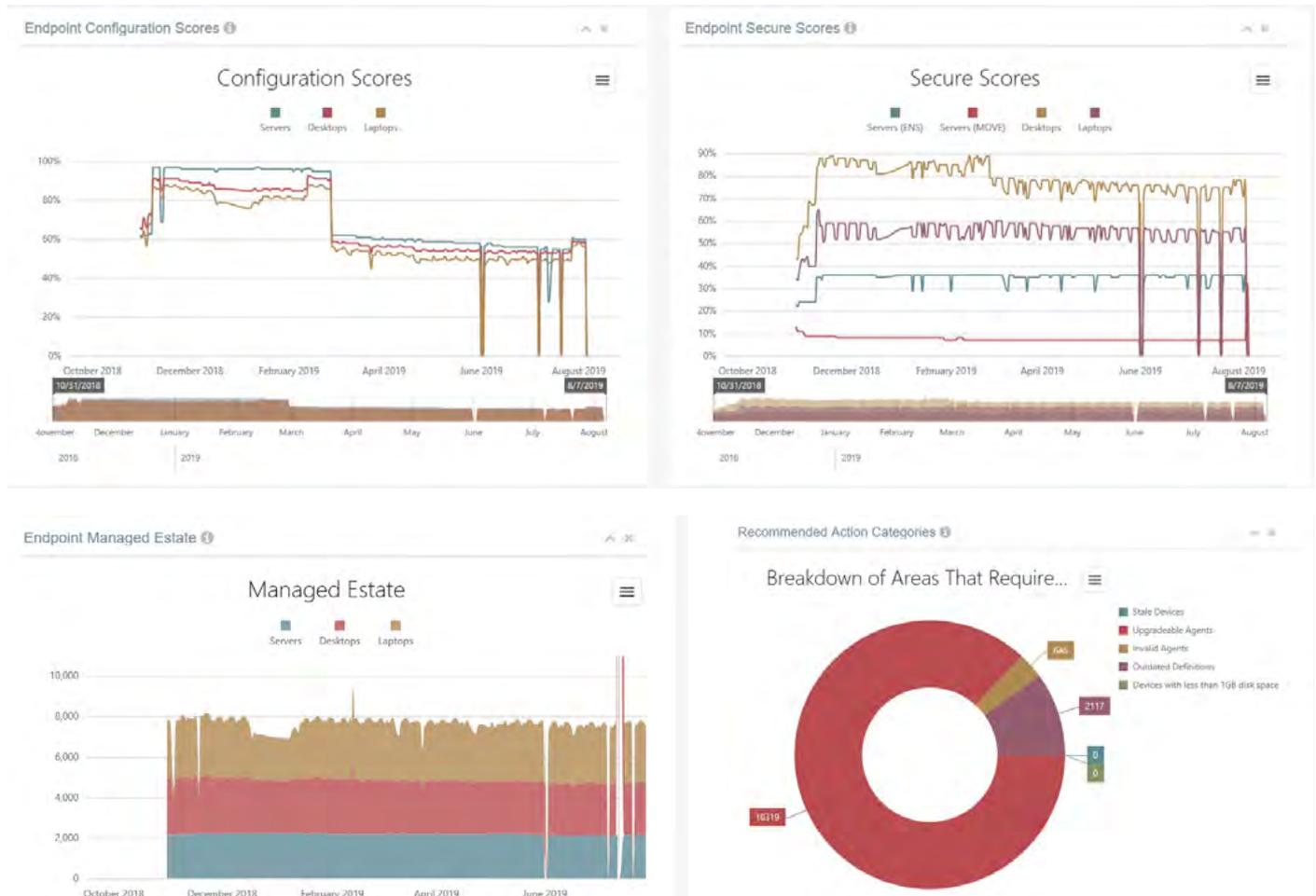
Drag a column header here to group by that column

Domain	Hostname	Operating System	OS Type	Microsoft Windows Defender...	+ Mc Afee e Policy Orchest...	Cyberreas...	Active Directory	Microsoft Patch Management
demo.example.net	412776	Windows 10 Pro	Workstation				2019-07-29T08:04:02	2019-08-06T20:45:36
demo.example.net	5CG52502JX	Windows 10 Pro	Workstation				2019-08-03T11:53:12	2019-07-23T09:39:14
demo.example.net	AAA0411T	Windows 10 Pro	Workstation				2019-08-01T08:49:14	2019-08-06T14:10:21
demo.example.net	AAC2208-L	Windows 10 Pro	Workstation				2019-08-05T09:36:42	2019-08-06T15:17:51
demo.example.net	aad2312-l	Windows 10 Pro	Workstation				2019-07-29T07:00:03	2019-08-06T12:47:00
demo.example.net	AAH1909	Windows 10 Pro	Workstation				2019-07-30T21:26:22	2019-08-06T20:50:54
demo.example.net	AAM1103	Windows 10 Pro	Workstation				2019-07-30T07:44:32	2019-08-06T13:24:47
demo.example.net	AAM1510-L	Windows 10 Pro	Workstation				2019-07-28T14:12:58	2019-08-06T17:27:53
demo.example.net	AAM2602A	Windows 10 Pro	Workstation				2019-08-01T06:42:13	2019-08-06T15:37:19
demo.example.net	AAN0505	Windows 10 Pro	Workstation				2019-08-01T07:37:13	2019-08-06T14:05:19
demo.example.net	AAP1809-L	Windows 10 Pro	Workstation				2019-07-29T07:29:03	2019-08-06T13:25:02
demo.example.net	AAR3103	Windows 10 Pro	Workstation				2019-07-27T19:20:03	2019-07-31T16:29:40

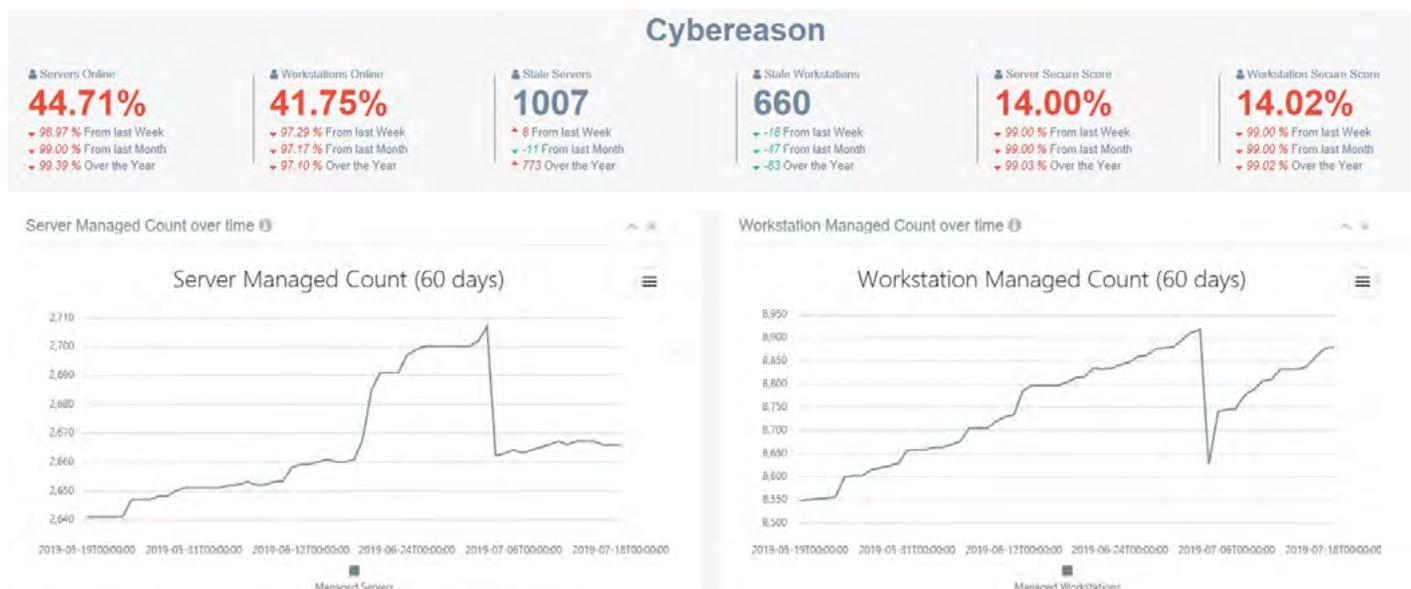
Baseline Product Coverage Over Time



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.



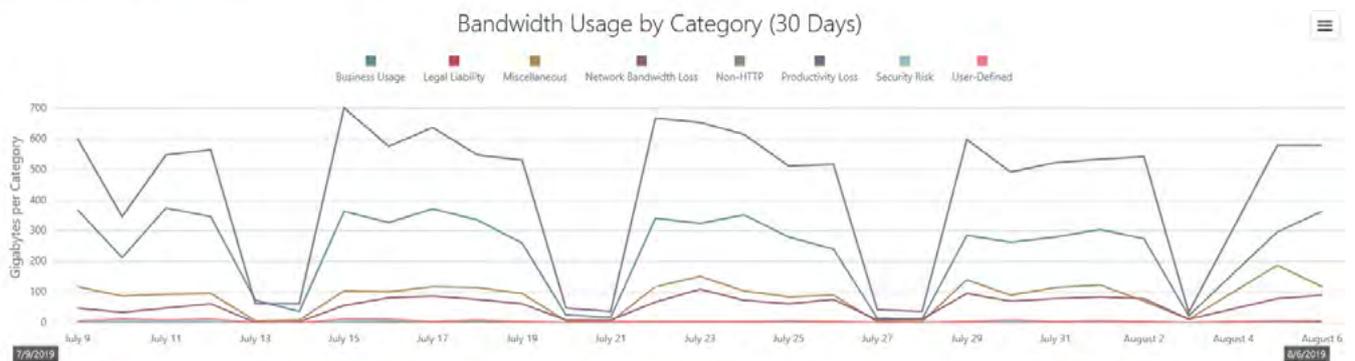
The Cybereason lens provides an instant look at the configuration and coverage of the EDR solution within the organisation.



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.

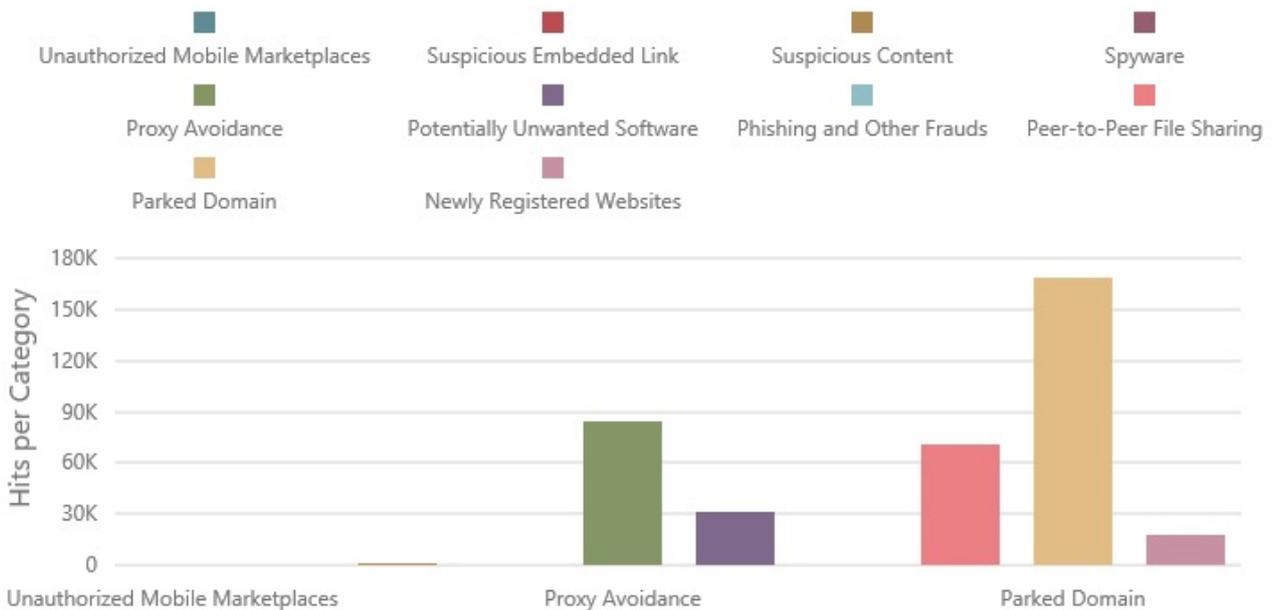


Bandwidth Usage by Browsing Class



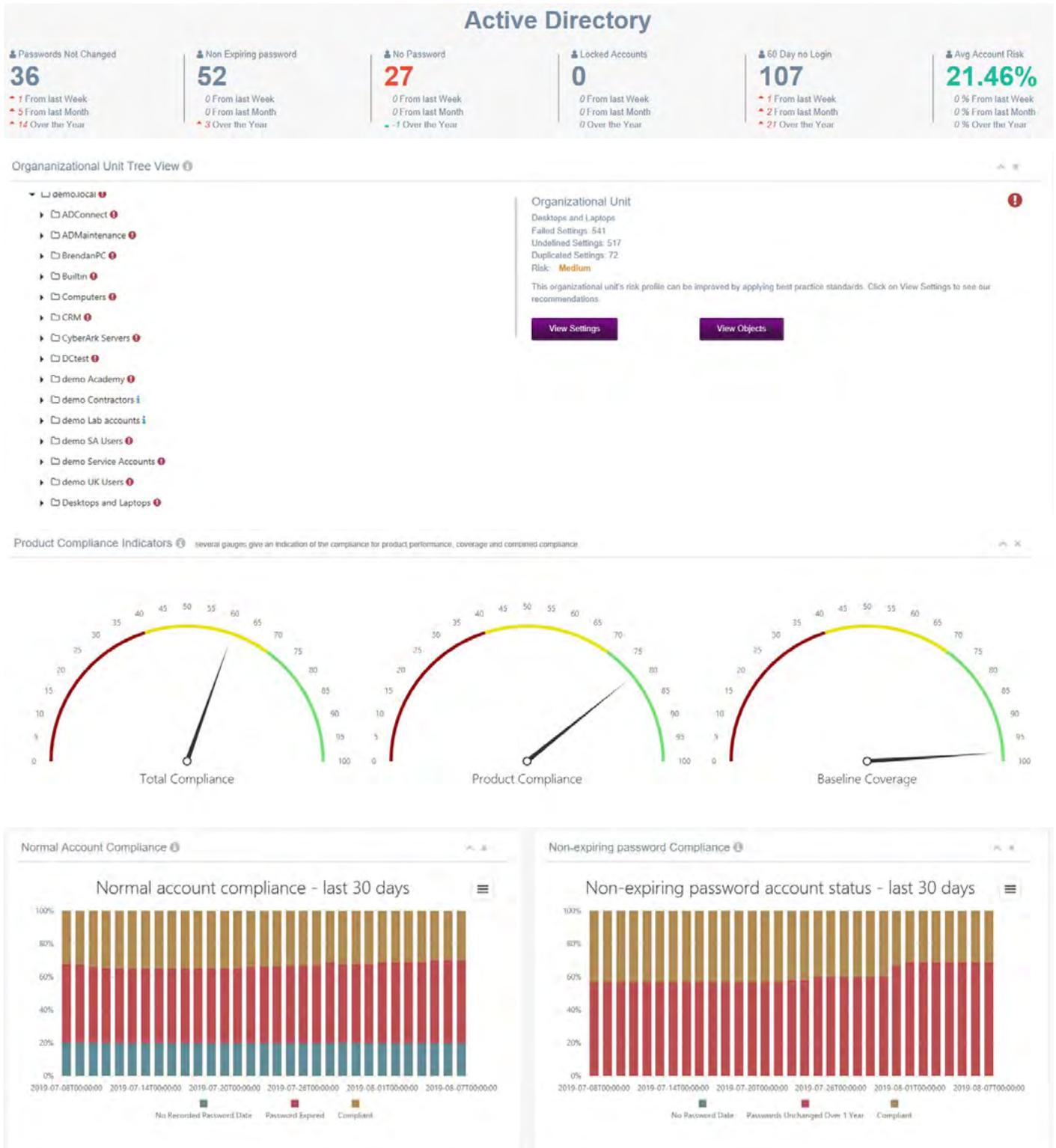
Top Security Class Breaches in the past 7 days

Security Class Breaches



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.

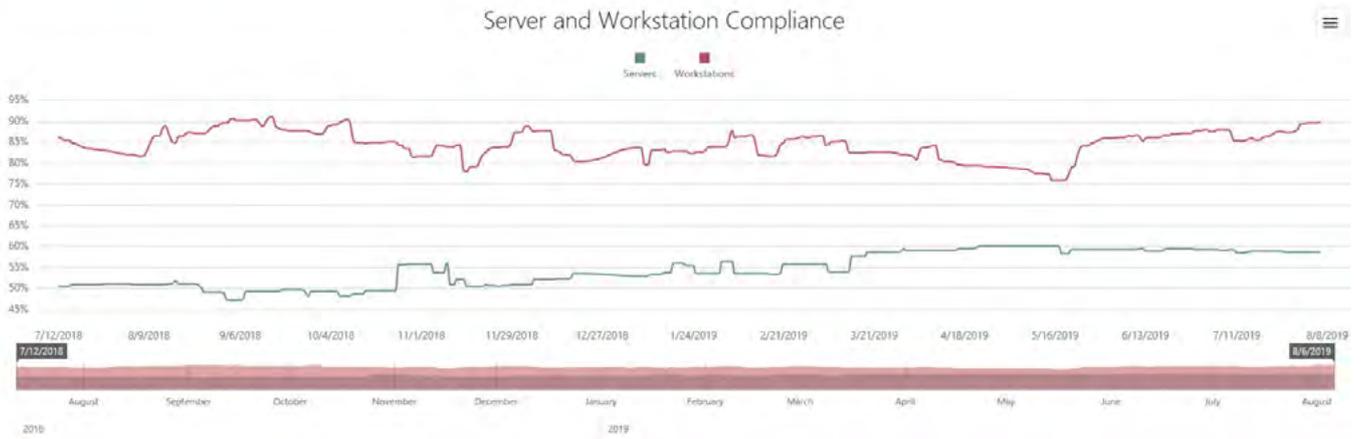
Additional enhancements such as the GPO best practice review and Bloodhound lateral movement add-on make this one of the more powerful lenses within ENCORE.



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



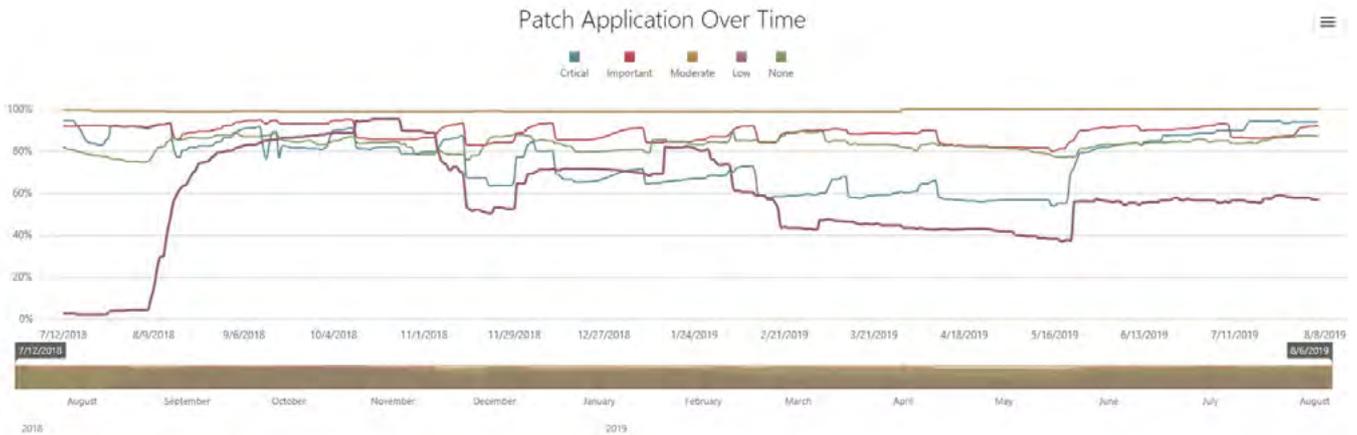
Server and Workstation Compliance Over Time



Product Compliance Indicators several gauges give an indication of the compliance for product performance, coverage and combined compliance.



Patch Application Over Time



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.



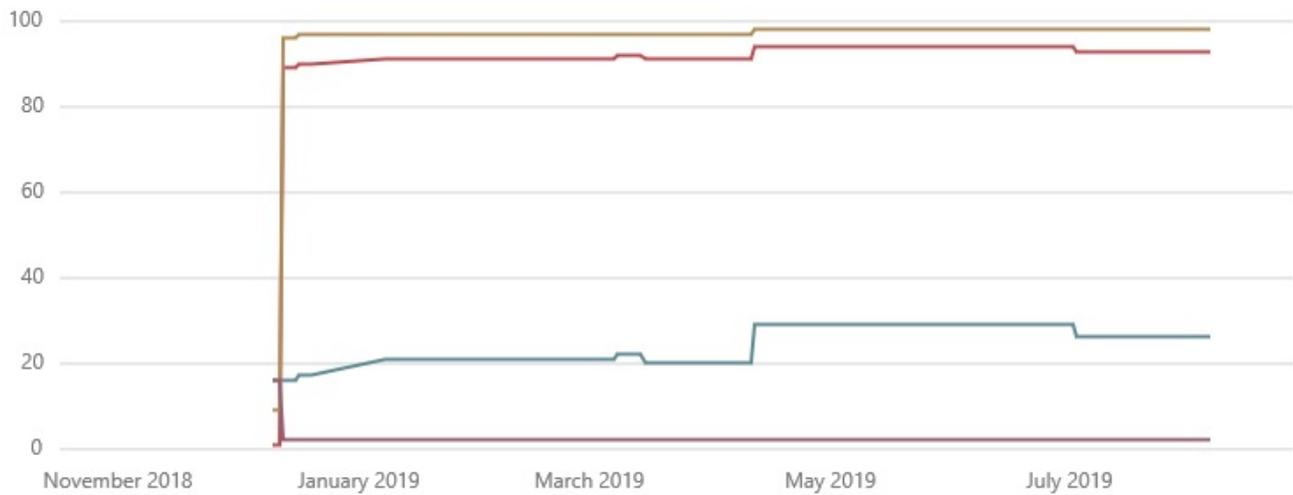
Risk Categories Over Time



Risk Categories Over Time



■ Total Devices
 ■ Risk Score
 ■ Cleanup Score
 ■ High Risk Devices



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.

Infact data selection

Data Selection

User Data **Device Data**

Select a user Select a device

User Details

User Account Selection

Example User

Detected Data: Example User

Active Directory				ForcePoint DLP				Efact				
Date	Name	Domain	Sam Accou...	Disabled	Locked	Pwd Ex...	Pwd Re...	Non-Ex...	Last Logon	Pwd Last Set	Desc.	Distinguished Name
8/7/2019	Example User	example.com	example.user				✓		7/29/2019	6/24/2019		CN=Example User...

Detected Computer Data: ExampleComputer

Product	Is Managed	Host Name	Domain	Last Communication Date	OS
Active Directory	✓	ExampleComputer	example.com	7/29/2019	Windows 10 Enterprise
McAfee ePolicy Orchestrator	✓	ExampleComputer	example.com	8/2/2019	Windows 10
ForcePoint DLP	✓	ExampleComputer	example.com	8/2/2019	Windows 10
Cybereason					
Microsoft Windows Defender ATP					

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



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.

Detailed Report for 10opevrs

Host Name 10opevrs	Display Name 10opevrs	Address 85.1.1.01	Current Status @ 2019-08-07 02:01:55 AM ✔
-----------------------	--------------------------	----------------------	---

Check Result Summary view the results of the individual tasks

Category	Task Date	Type	Description	Result
Priority: Urgent - result: failed (3 checks)				
System Health	Thursday, October 25, 2018, 1:58:09 PM	Memory Usage	85.7% of available memory used	❌
Application Health	Wednesday, August 7, 2019, 2:01:55 AM	Epo Daily Check	Master Repository Task Check	❌
Application Health	Wednesday, August 7, 2019, 2:01:55 AM	Epo Daily Check	Backup Task check	❌
Priority: Low - result: passed (4 checks)				
Priority: None - informational (1 checks)				

Host Health Monitoring view host uptimes and available resources

Device	Address	Last Checked	Status	Memory	CPU Usage	Connections	Load 5 Min	Processes
demo1	85.1.1.01	Wednesday, August 7, 2019, 2:41:00 AM	❌	❌	✔	⌘	⌘	⌘
demo2	65.0.92.271	Wednesday, August 7, 2019, 2:41:01 AM	❌	❌	✔	⌘	⌘	⌘
demo3	65.0.92.271	Wednesday, August 7, 2019, 2:41:00 AM	❌	⚠️	✔	⌘	⌘	⌘
demo4	03.1.1.01	Wednesday, August 7, 2019, 2:41:00 AM	❌	⚠️	✔	⌘	⌘	⌘
demo5	41.1.1.01	Wednesday, August 7, 2019, 2:41:00 AM	✔	✔	✔	⌘	⌘	⌘

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.

Host Daily Checks click on the arrows in the explore column to view the results from the hourly checks done on the required hosts

Explore	Device	Address	Name	Last Checked	Service Check	Type of check	Result	Status
▶▶	Demo Server 1	10.1.1.2	Demo01	Wednesday, February 13, 2019, 4:16:18 PM	Epo Daily Check	Application	Failed	❌
▶▶	Checkpoint Firewall 01	10.1.1.3	FW01	Wednesday, February 13, 2019, 4:16:25 PM	Check Point Daily Checks	Application	Warning	⚠️
▶▶	Checkpoint Firewall 02	10.1.1.4	FW02	Wednesday, February 13, 2019, 4:16:25 PM	Check Point Daily Checks	Application	Warning	⚠️
▶▶	Fortigate Firewall 01	10.1.1.5	FW03	Wednesday, February 13, 2019, 4:16:25 PM	Fortigate Daily Checks	Application	Warning	⚠️
▶▶	Forcepoint	10.1.1.6	Forcepoint	Wednesday, February 13, 2019, 4:24:24 PM	System Checks	System	Passed	✔

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:



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



2102372787732176262
32467732342425 7 43
321342762 6762 47
381327367527 477476
052752621093 4376

526422165 031255 6613
23131 03747 13 090
773 334 3737 7044
2412613161 23116616111
213231216

ENCORE

www.encore.io

30
0.1
0.1
0.1
0.2

304200743 0148
01717 61525 01
561 112 1515
0270473747 01753474

