

The logo for ENCORE, with the letter 'O' replaced by a blue lightbulb icon. The background of the entire image is a dark blue, futuristic digital space filled with glowing lines, data points, and semi-transparent windows containing binary code and numbers.

ENCORE

# The Final Act for Security Visibility

Get real-time insights, actions and reports

[encore.io](https://encore.io)

## Encore integrates your entire security stack into one simple interface, allowing you to focus on what really matters – improving your security posture.

We know how hard it is to get a clear picture of your entire security posture, especially across many different controls. Security teams seek clarity and visibility to enable them to focus on what matters most.

Encore provides a single lens across all of your security tooling, providing cross-platform security coverage information, external threat information and security tooling health monitoring.

Our action-based reporting is designed to deliver insights that matter, giving you one portal providing visibility across all of your security controls.

Our agentless design means you don't need to buy more security controls or install yet another product. We help ensure you are delivering the best possible security value from investments you've already made.

Encore provides push-button executive reports that cover all security controls with industry-leading gap analysis. Find out where you're missing coverage and help lower the risk of a cyber attack.

By consolidating all of your information into one platform, your team will be able to triage incidents quicker with an enhanced risk-based view of each user, device and security control



Improve ROI from existing security technologies



Manage threats and minimize the attack surface



Automate security reporting



Immediate insight into regulatory and audit compliance



Provide proof of visibility and security



Faster security decisions, improve your response

# Visibility & Compliance

ENCORE

Encore provides visibility across all of your security controls in one place, rather than needing to look across multiple platforms and dashboards. This helps reduce the time, training and effort required to see where you have coverage gaps or areas that need attention.

Encore's singular view delivers insight into your entire IT estate by integrating, comparing and contrasting information from all leading EDR, AV, Active Directory, Firewall vendors and many other controls.

By easily comparing coverage and insight from all of your controls, you can quickly delve deeper to find actionable intelligence on where you need to focus next.

Encore draws on deep experience from security operations teams to deliver easily consumable dashboards, reports, metrics and many other features that provide additional context to security managers, operations and the extended business, right up to Board level.

## Baseline

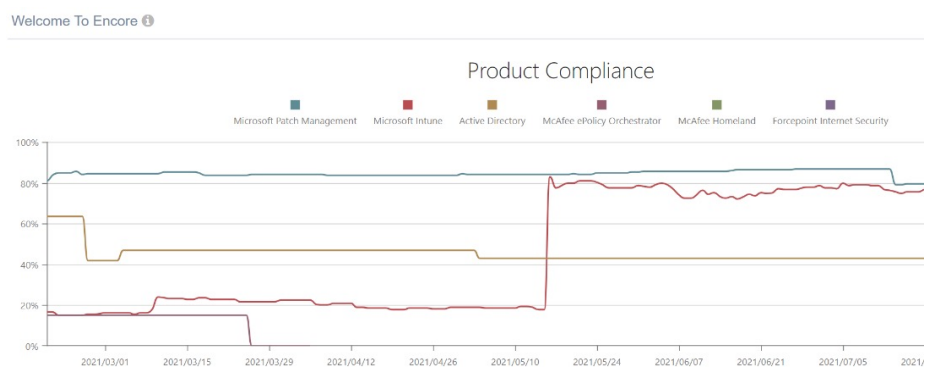
Access a side-by-side comparison of control coverage. By taking data from each security control and correlating it, Encore provides users with actionable intelligence to target devices with missing controls, while also developing an organisational baseline count to measure your coverage against.

Current Baseline Data

Domain	Hostname	Operating System	OS Type	Microsoft Windows Defender...	Mc Afee ePolicy Orchest...	Cybersec...	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	SCG52502JX	Windows 10 Pro	Workstation				2019-08-03T11:53:12	2019-07-23T09:39:14
demo.example.net	AA0411T	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-I	Windows 10 Pro	Workstation				2019-07-29T07:00:03	2019-08-06T14:27:00
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

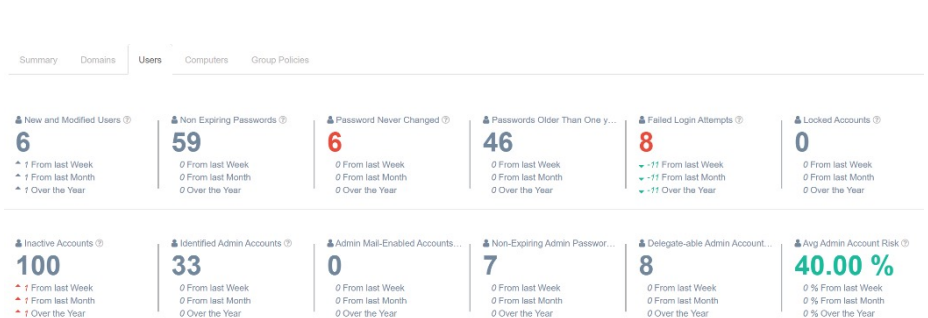
## Compliance

Easily monitor your baseline coverage and compliance over time. Find where you need to prioritise attention and use the tool to measure the impact of your security investments.



## Delve deeper

Dive deeper into each security control, uncover the problem areas, and improve your security posture with Encore delivering granular detail where needed.



# External Attack Surface

Find out what your attacker can see about you. Using open-source threat intelligence, Encore is able to uniquely link your external attack surface to your internal IT users and assets.

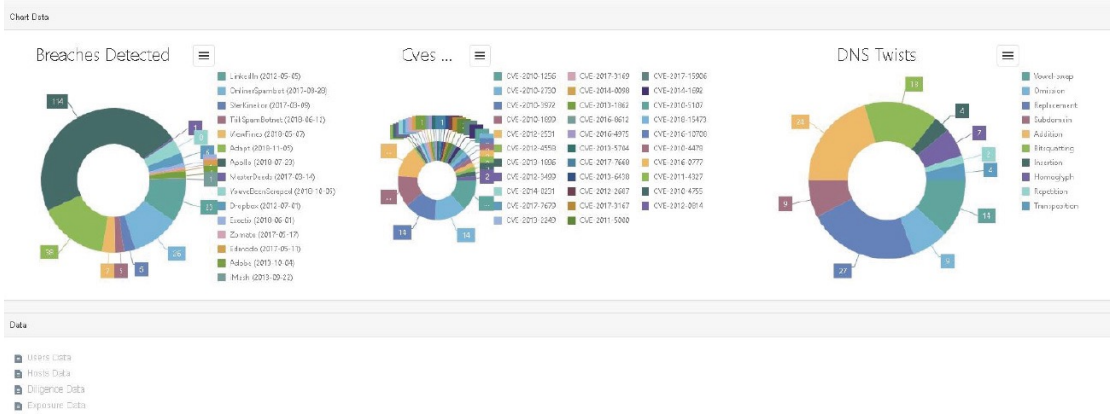
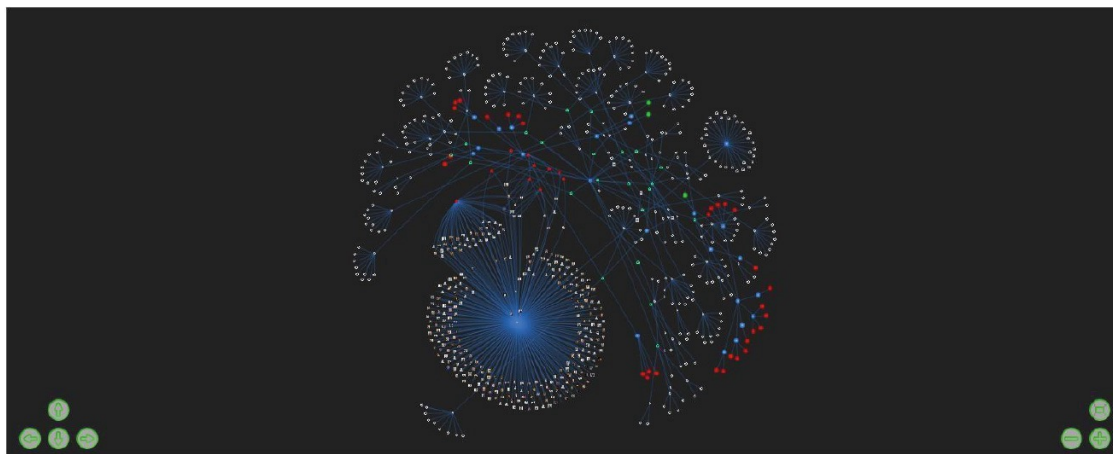
External Attack Surface offers the visibility into your online digital footprint. This is the sensitive data your staff unknowingly expose themselves and your company to. This data is invaluable to a hacker when gathering intelligence on their target.

Attackers are often cautious when gathering information in preparation for an attack, avoiding “noisy” vulnerability scanners that can be easily detected by defenders, and instead opt for lower hanging fruit.

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 URLs 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



# Enhance Incident Triage

ENCORE

Encore not only supports macro and micro views per technology control, but also consolidated views of controls per asset or per user. This allows for faster incident response and remediation activities because analysts no longer need to search and correlate data across multiple systems and platforms. This capability enhances incident response activities, and allows a targeted view across all platforms, including your external attack surface.

By searching on an asset or user you're able to quickly see all security controls and associated devices, along with their status, which Encore then integrates with the External Attack Surface data. This allows your organisation to quickly identify and match users that have been exposed to breaches and/or would be likely candidates for targeted phishing, and then match this external profile to the internal asset and the compliance of that user. This greater visibility allows risk reduction and awareness campaigns to be performed.

**Infact data selection**

**Data Selection**

User Data: Select a user

Device Data: 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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	ExampleComputer	example.com	7/29/2019	Windows 10 Enterprise
McAfee ePolicy Orchestrator	<input checked="" type="checkbox"/>	ExampleComputer	example.com	8/2/2019	Windows 10
ForcePoint DLP	<input checked="" type="checkbox"/>	ExampleComputer	example.com	8/2/2019	Windows 10
Cybereason	<input type="checkbox"/>				
Microsoft Windows Defender ATP	<input type="checkbox"/>				

## Data collection – how does it work?

Encore requires read-only access to the monitored controls, with no need to install agents in multiple places.

All that is required on the network is our collection application that runs on a Windows server. The platform uses security keys and end-to-end encryption to ensure all the data is collected and stored in the cloud service safely and reliably.

# Security Health Monitoring

ENCORE

Security tooling is useless if it's not actively monitoring your IT estate and that's where Encore's Health Monitoring capability comes into its own. The Health capability provides security, network device, server resource utilisation and threshold alerting, providing SNMP and agent-based monitoring across your security stack, 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	Display Name	Address	Current Status @ 2019-08-07 02:01:55 AM
10opevrs	10opevrs	85.1.1.01	

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	

# Supported Technology



Our supported technology list is constantly growing and we can typically add a new integration in a matter of weeks.

If there is a demand for a new product or feature our team of developers is highly receptive to working with clients to drive enhancements to Encore.

## Some of our supported technologies



Interested in a demo to see how  
Encore can protect your security posture?  
Contact our cybersecurity experts today,  
email [sales@encore.io](mailto:sales@encore.io)

**ENCORE**

encore.io