ENCORE

# The Final Act for Security Visibility

Get real-time insights, actions and reports

encore.io

# Executive Summary

ENCORE

## 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

Immediate insight into regulatory and audit compliance

Manage threats and minimize the attack surface

Provide proof of visibility and security

Automate security reporting

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.

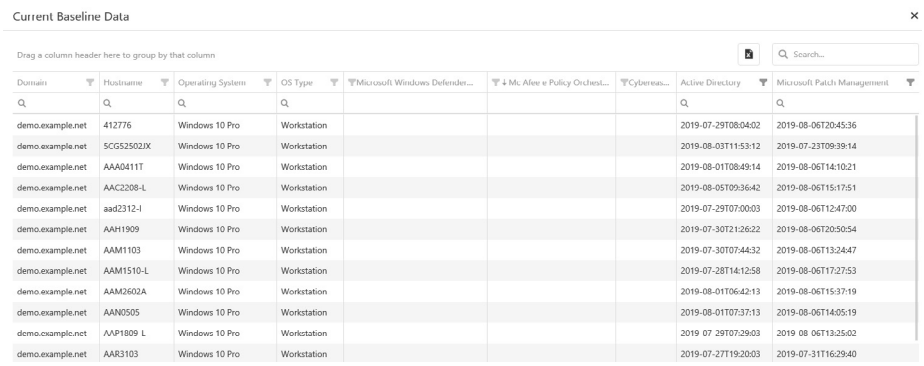
Encore's singular view delivers insight into your entire IT estate by integrating, comparing and contrasting information from all leading EDR, AV, Active Directory, Firewall vendors and many other controls.

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.

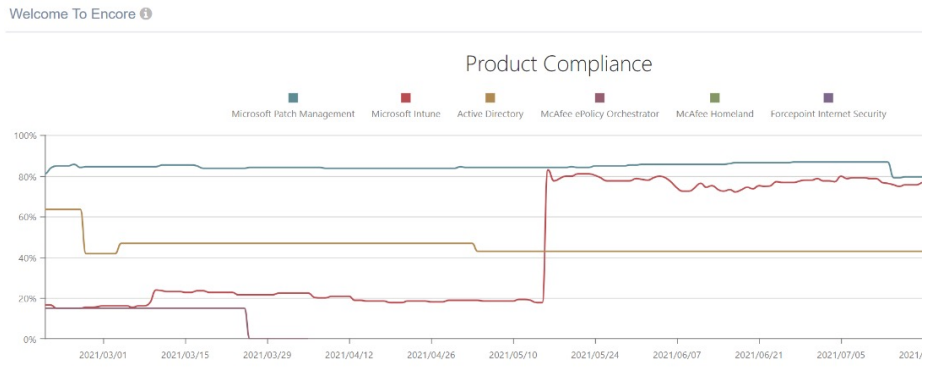
## Baseline

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.



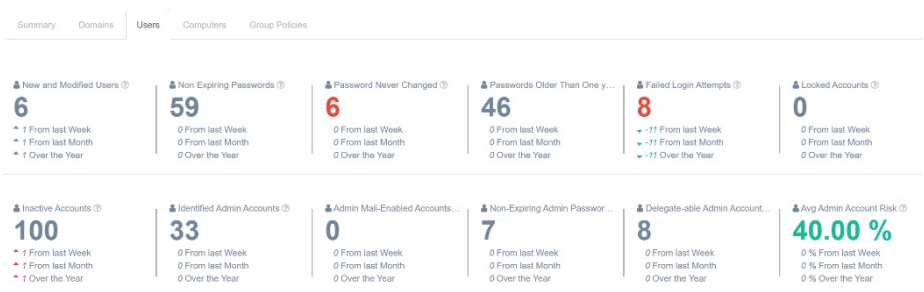

## Compliance

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

ENCORE

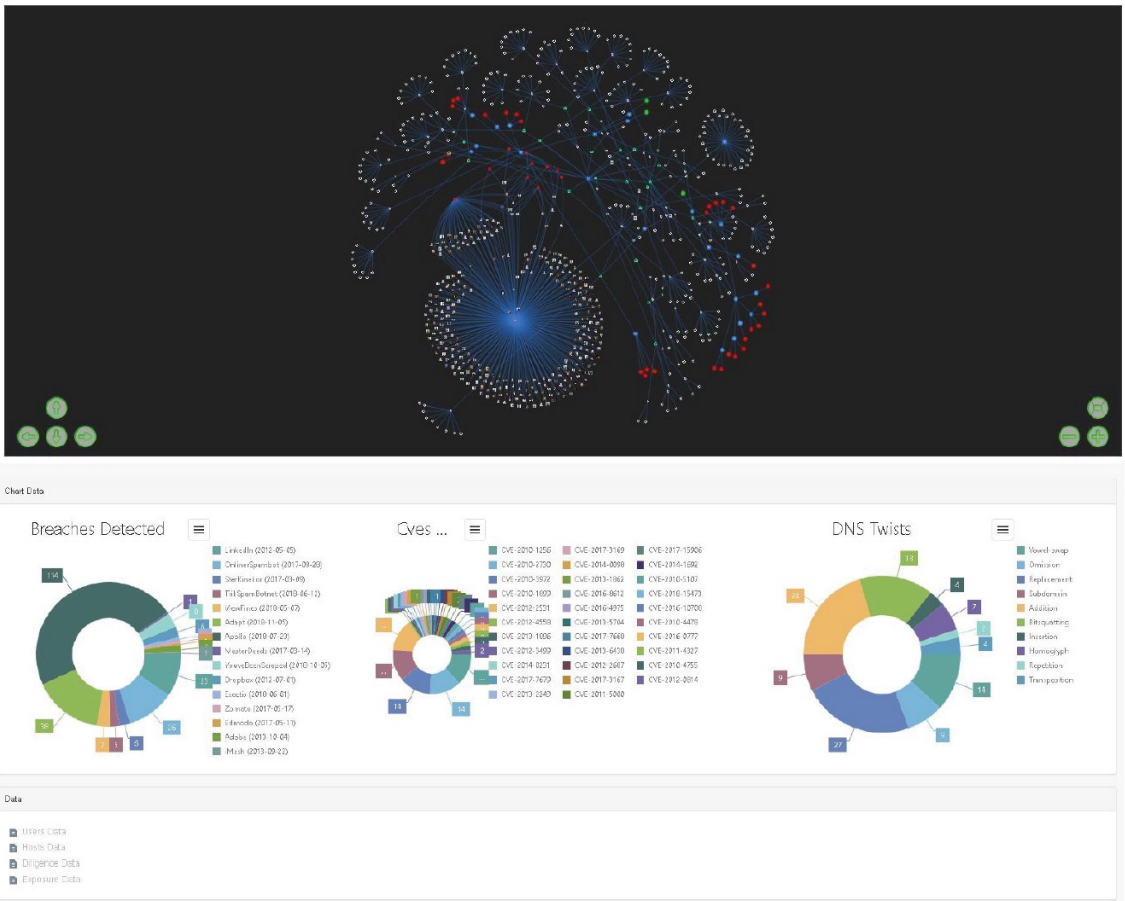
Find out what your attacker can see about you. Using open-source threat intelligence, Encore is able to uniquely link your external attack surface to your internal IT users and assets.

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 Pawned 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

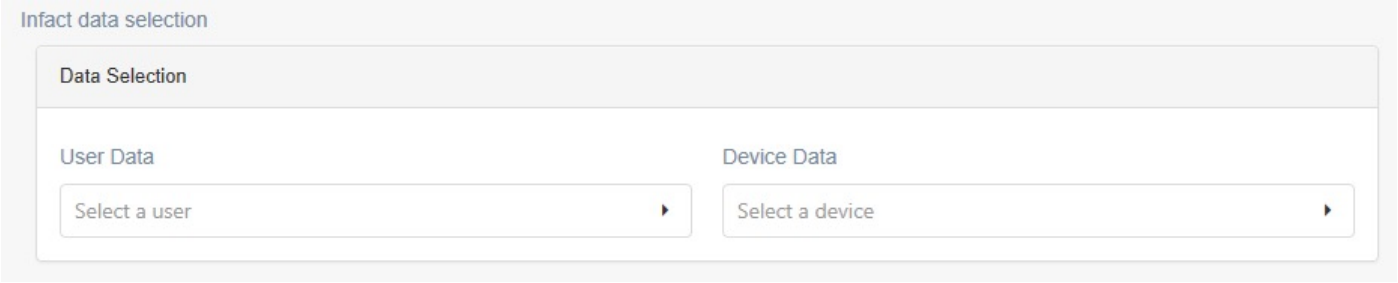


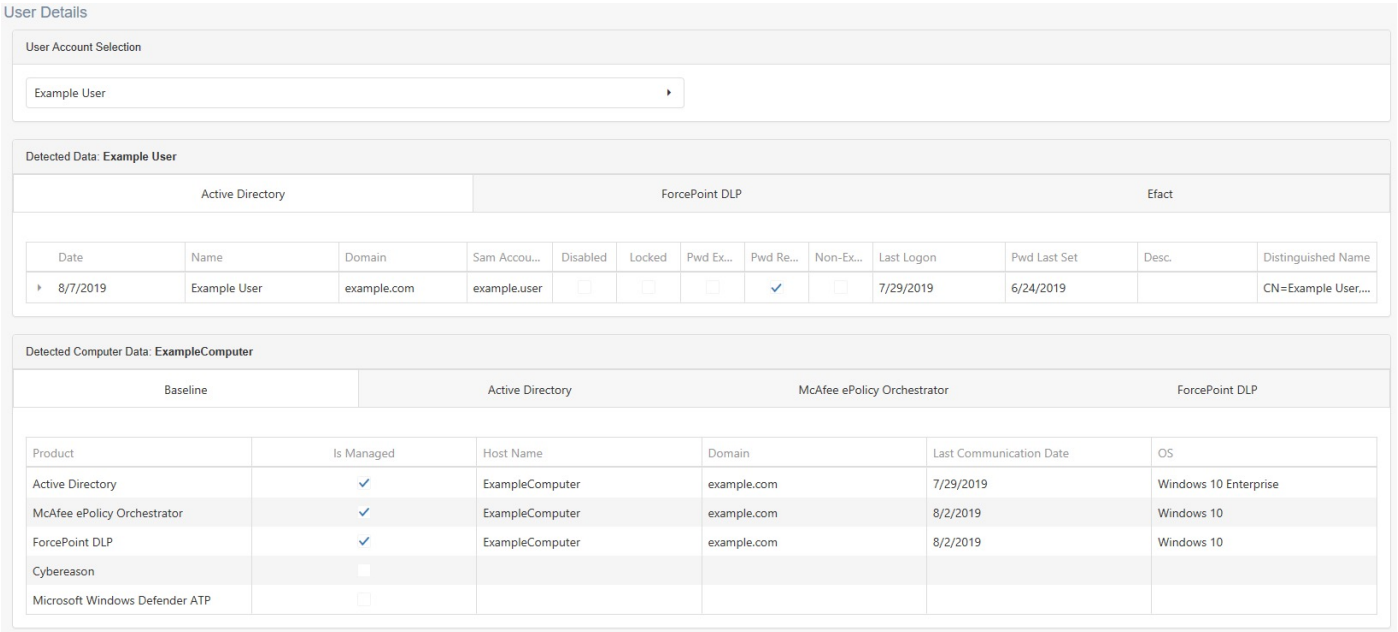
# Enhance Incident Triage

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.




## Data collection – how does it work?

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

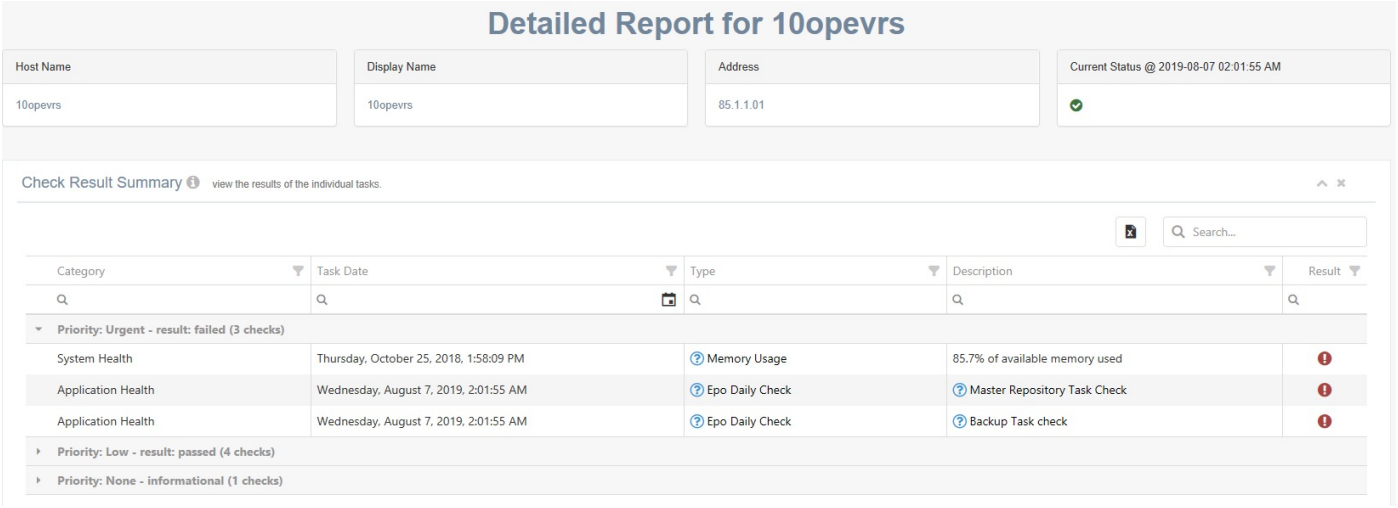
All that is required on the network is our collection application that runs on a Windows server. The platform uses  security keys and end-to-end encryption to ensure all the data is collected and stored in the cloud service safely and reliably.

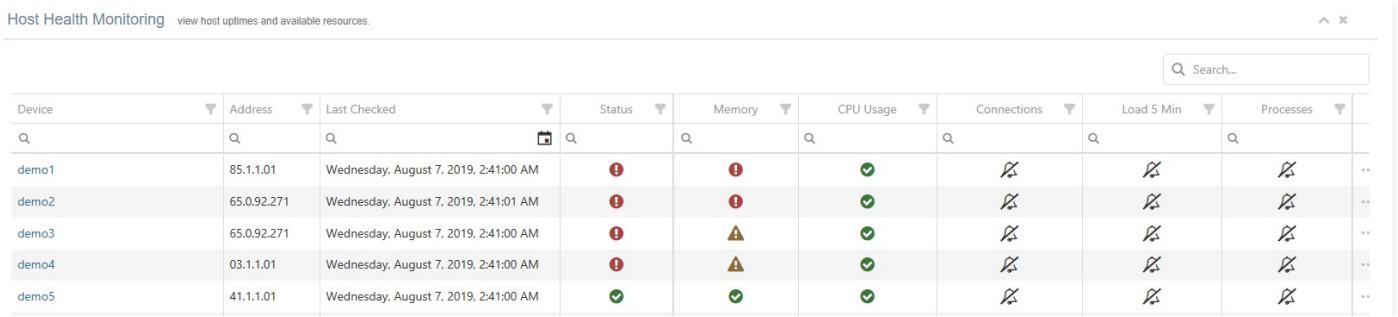
# Security Health Monitoring

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

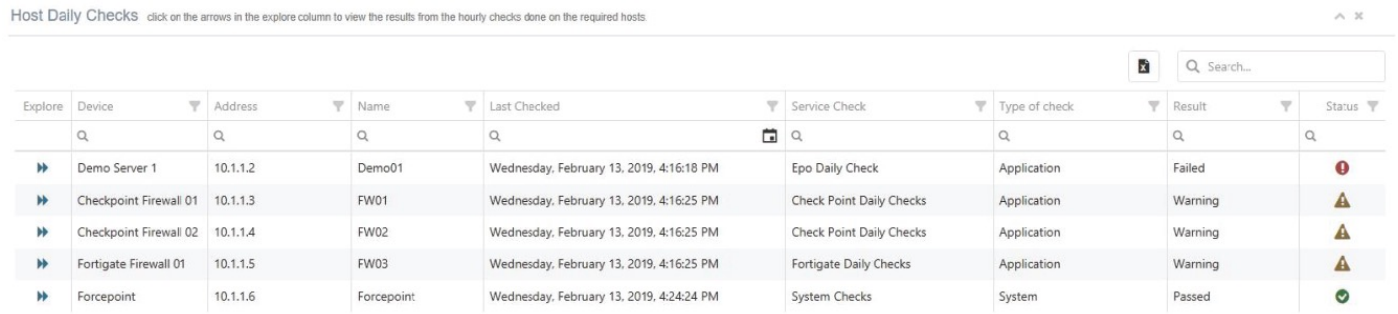
The below shows an example dashboard for the SNMP or Agent based monitoring solution for a single host.




## 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.



# Supported Technology

ENCORE

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**

Microsoft Active Directory · Microsoft Intune · Microsoft System Center · McAfee · TANIUM

tufin · CYBERARK · tenable network security · Qualys · Symantec · SentinelOne

CLOUDFLARE · Check Point SOFTWARE TECHNOLOGIES LTD · paloalto NETWORKS · cybereason

FORTINET · Forcepoint · mimecast · Carbon Black. · BLOODHOUND · Windows Server Update Services · CROWDSTRIKE

Interested in a demo to see how
Encore can protect your security posture?
Contact our cybersecurity experts today,
email **sales@encore.io**


encore.io