Contium in partnership with tenable

Unified Exposure Management Platform:

Our Solution

Background

Cantium Business Solutions

As a Local Authority owned trading organisation (LATCo), Cantium has over 35 years' experience supplying IT services to the Public Sector. As such, we have developed a comprehensive managed service portfolio, built alongside a strong partner network, to support and complement the services we deliver in-house.

Our highly experienced and dedicated teams, consisting of over 300 ICT specialists, provide advice, guidance and support to over 33,000 users. With a customer base of over 700 organisations across the Public, Private and Education sectors, Cantium offers a range of ICT services tailored to our customers' individual needs.

Tenable

A globally trusted exposure management company, approximately 40,000 organisations around the globe rely on Tenable to understand and reduce their cyber risk. As the creator of Nessus®, Tenable has developed and extended its vulnerability expertise, creating the world's first platform to view and secure any digital asset on any computing platform.

Tenable has grown to encompass a portfolio of solutions, identifying, monitoring and prioritising vulnerabilities across entire networks, including on-premise, cloud, OT, mobile and virtual environments.

Working in collaboration to instil cybersecurity awareness and reduce external threats within the Public Sector, Cantium has developed a strong partnership with Tenable to deliver value and security resilience to our customers.

Exposure Management Platform

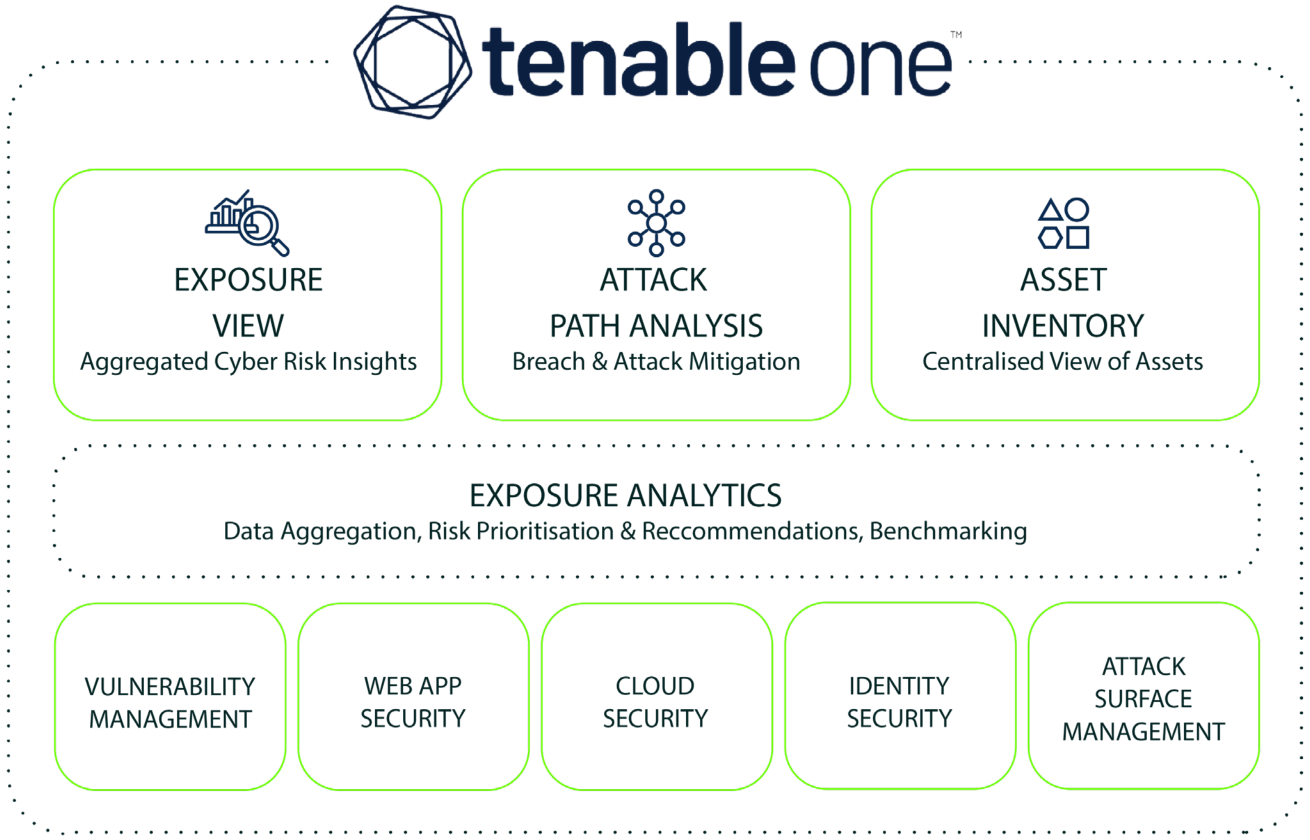
With the dramatic rise of ransomware and targeted cyber-attacks aimed at disrupting organisations and stealing valuable data, cybersecurity suppliers have responded with a plethora of new solutions released into the marketplace. With such a range of products purporting to provide threat detection and incident response, all providing different reporting metrics and training requirements, where is the unification? How do you succinctly communicate your organisation's security status?

- ✓ **Anticipate and prioritise efforts to prevent attacks**
- ✓ **Proactively reduce exposure**
- ✓ **Unify with clear business insights**
- ✓ **Gain comprehensive visibility across the modern attack surface**
- ✓ **Communicate cyber risk to inform better decisions.**

All in one solution

With Tenable One, organisations can now combine all their technical asset, vulnerability and threat data into a clear actionable platform. The solution collates comprehensive analytics from across the organisation to prioritise actions and communicate cyber risk, ensuring threats are captured before they have chance to become risks.

The Tenable One Exposure Management Platform consists of the following modular elements:



tenable one™

EXPOSURE VIEW
Aggregated Cyber Risk Insights

ATTACK PATH ANALYSIS
Breach & Attack Mitigation

ASSET INVENTORY
Centralised View of Assets

EXPOSURE ANALYTICS
Data Aggregation, Risk Prioritisation & Reccommendations, Benchmarking

VULNERABILITY MANAGEMENT

WEB APP SECURITY

CLOUD SECURITY

IDENTITY SECURITY

ATTACK SURFACE MANAGEMENT

Vulnerability Management *(formerly Tenable.io)*

Managed in the cloud and powered by Tenable Nessus, Tenable Vulnerability Management provides comprehensive vulnerability coverage with real-time continuous assessment of an organisation. The system includes a built-in prioritisation element which uses real-time insight, allowing organisations to understand and act on threats, immediately.

Web Application Security *(formerly Tenable.io Web Application Scanning)*

Tenable's Web Application Security provides a comprehensive and accurate vulnerability assessment. Using simple, scalable and automated vulnerability scanning, the system provides full and unified visibility of web applications, ensuring early sight of any vulnerabilities.

Cloud Security *(formerly Tenable.cs)*

Similar to the web application scanning, Tenable Cloud Security provides automated threat detection across an organisation's cloud environment. The solution enables security teams to continuously assess the security posture of cloud environments, offering full visibility across multi-cloud environments and helping organisations prioritise efforts based on business risk.

Identity Exposure *(formerly Tenable.ad)*

Tenable Identity Exposure allows organisations to have a unified view across their complex Active Directory (AD) environment. This proactive approach to AD management allows organisations to proactively reduce risk and eliminate attack paths before attackers have the opportunity to exploit them.

Attack Surface Management *(formerly Tenable.asm)*

Tenable Attack Surface Management continuously maps the internet in its entirety and discovers connections to all internet-facing assets, allowing organisations to discover and assess the security posture of the whole external attack surface. This provides organisations with comprehensive visibility to assess and manage risk, developing a full understanding of their digital footprint.

Key Capabilities:

1 Global Exposure View

Providing clear, concise insight into an organisation's security exposure, helping them to decipher how secure their systems truly are and how they are performing over time.

2 External Attack Surface Management

Allowing organisations to identify risks from the attacker's perspective, enabling preventative action to take place.

3 Attack Path Assessment

Mapping risks to all viable attack paths continuously - both on-premise and in the cloud.

4 Centralised Asset Inventory

Mapping risks to all viable attack paths continuously - both on-premise and in the cloud.

5 Risk-based Vulnerability Management

Dynamically prioritising remediation and incorporating this threat intelligence information into measurements of an organisation's exposure to risk.

6 Comprehensive Assessment

Insight into the cyber exposure of all assets, including vulnerabilities, misconfigurations and other potential security threats.

7 Secure Active Directory

Enabling organisations with an AD-wide view of the environment and address risks in AD before they can develop.

8 Secure Cloud Infrastructure

Complete and continuous visibility and remediations of exposures across all cloud resources and assets.

9 Automated Web Application Scanning

Providing comprehensive and accurate vulnerability scanning, with full visibility of IT, cloud and web application vulnerabilities.

10 Peer Benchmarking

Compare cyber exposure between business units or locations internally, and against industry peers externally, to determine where and when to make key human and financial investments.

11 Program Effectiveness Metrics

Addressing questions such as "How effective are we in meeting our internally set SLAs?"

12 News

Integrating with Tenable Research blogs and allowing for creation of custom exposure cards that reflect cyber security developments.

13 Backed by Tenable Research

World-class cyber exposure intelligence, data science insights, alerts and security advisories.

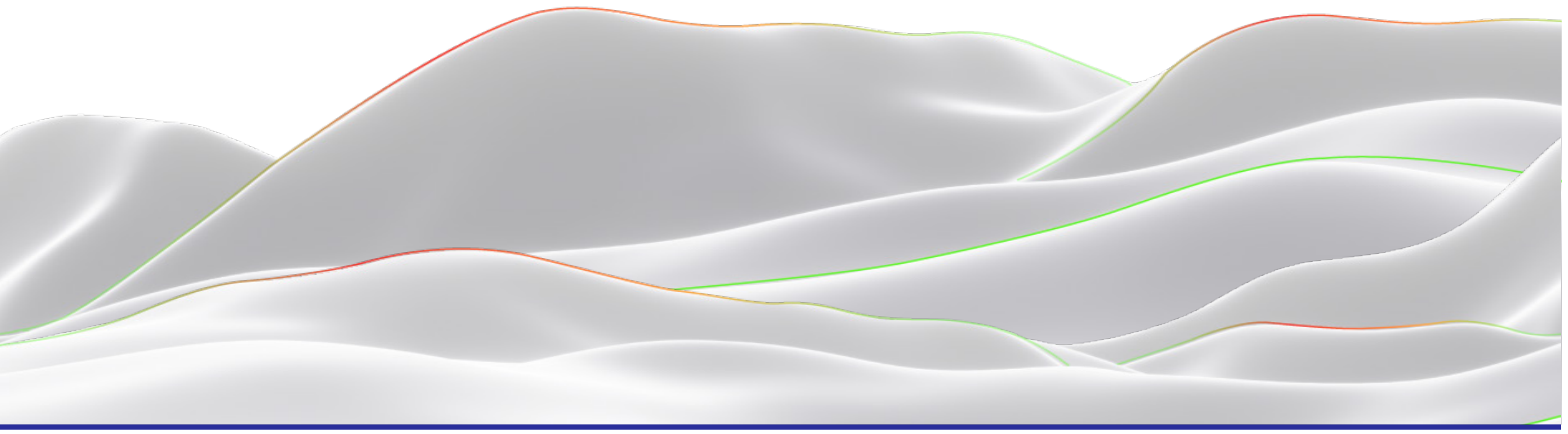
14 Flexible Licensing

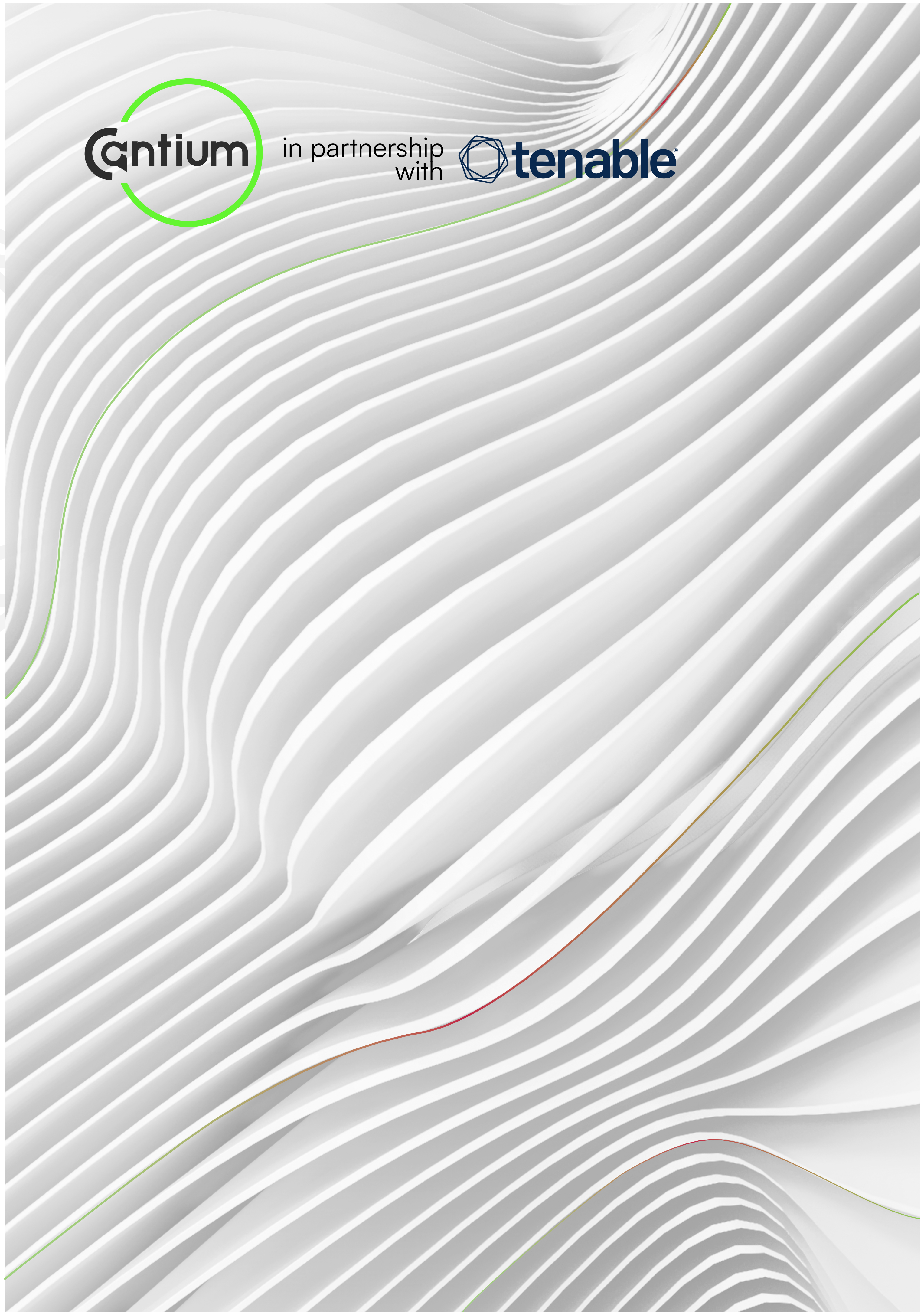
All-inclusive licensing provides the flexibility to dynamically reallocate licensing between IT, cloud, containers, web applications and AD users.

Key Benefits:

- ✓ Safeguard critical infrastructure and sensitive data.
- ✓ Quickly demonstrate compliance with regulatory standards and operational frameworks.
- ✓ Obtain visibility into all the assets and vulnerabilities, on your extended network.
- ✓ Easily prioritise vulnerabilities before they become a breach.
- ✓ Harden defences to prevent ransomware.
- ✓ Accelerate Zero Trust with full visibility into the assets and users on your network.
- ✓ FedRAMP authorised.

For more information on how **Cantium can help your organisation**, please contact **info@cantium.solutions**





Cantium in partnership with tenable