



in partnership  
with



# Unified Exposure Management Platform:

---

# The Key Benefits

---



# 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.

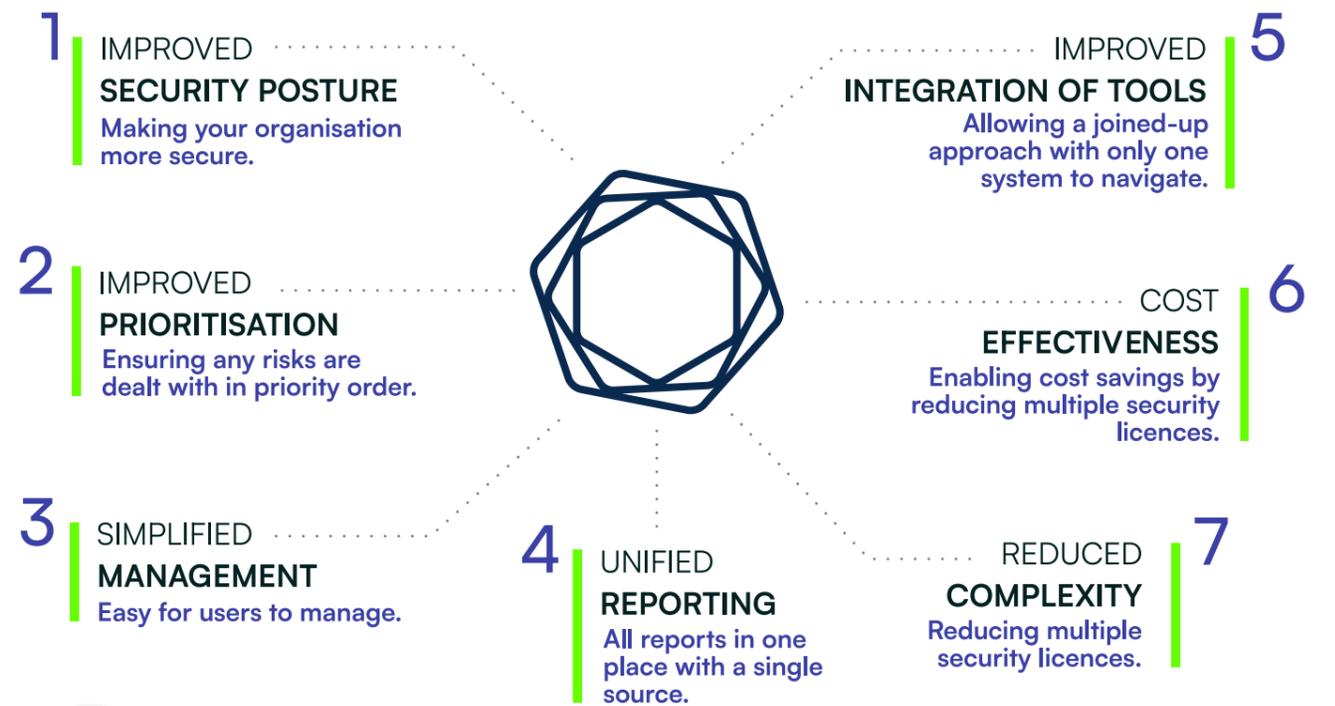
### Tenable One

The Tenable One Exposure Management Platform provides all round security coverage by protecting assets and allowing organisations to better understand cyber risks, make actionable decisions to address them and accurately communicate these risks to support optimal business performance. It also measures your security processes, including how effective the security team is at identifying critical flaws and how quickly they remediate issues to reduce risk.

Organisations are seeking a more streamlined approach to cybersecurity, reducing the number of tools they deploy and opting for a more comprehensive, integrated platform solution.

- ✓ Cloud Security
- ✓ Identity Security
- ✓ Vulnerability Management
- ✓ Web Application Security
- ✓ Attack Path Analysis
- ✓ Attack Surface Management
- ✓ Cyber Risk Analysis
- ✓ Asset Inventory

There are several, important, economic and risk management benefits for taking a consolidated platform approach to exposure management. The most notable are:



## 1 Improved Security Posture

A primary advantage of a platform solution is the improved security posture benefits it provides. A single solution delivers a more complete and integrated security solution. Organisations can gain a better understanding of their security posture, including their strengths and weaknesses. This integrated approach helps organisations identify and address security gaps that may have gone unnoticed in a siloed, multi-vendor environment. Via the Tenable One Reporting Suite, organisations can also easily track KPIs, producing reports to measure performance and creating alerts when resolving vulnerabilities, within or outside of the agreed SLA. This level of automation reduces the resource input required to manually track performance indicators, freeing up technical specialist time to focus on the organisation's security improvements.

## 2 Improved Prioritisation of Exposures

A single platform can combine a variety of different security inputs for a more complete perspective of cyber risk. Allowing organisations to focus on what matters most and ensuring protection of critical assets and data. The efficiencies produced can also free up valuable resources to focus on roadmap improvements for the organisation's technical infrastructure.

## 3 Simplified Management

By using a single solution, the workload for IT departments can be simplified and reduced. Rather than managing multiple solutions from different vendors, Tenable provides one single solution, integrated to cover all of an organisation's security needs. Training costs can also be reduced

due to users only needing to be trained on one system rather than multiple. Users can quickly gain knowledge on a single platform, with technical support greatly improved through a single contact team.

## 4 Unified Reporting

With one solution, reporting becomes significantly easier. Organisations can analyse exposures, track status and measure performance, all from one system. With unified reporting, everything is in one place, eliminating the need to switch between multiple reporting tools and dashboards.

## 5 Improved Integration of Tools

When different systems are not integrated, they can lead to security gaps, duplicated effort and inefficiencies in the IT infrastructure. With a single vendor solution, different cybersecurity systems are integrated into one unified solution.

## 6 Cost-effectiveness

One of the biggest benefits of a single vendor solution for exposure management is the cost savings which can be achieved. Managing multiple vendors requires multiple licenses, subscriptions and maintenance fees. However, with a single vendor solution and a single licensing model, organisations can benefit from bundled pricing, which can lower costs significantly.

## 7 Reduced Complexity

Another key benefit of a single vendor exposure management solution is reduced complexity, with consistency maintained within the security policies and procedures. Security teams are able to detect, respond to and manage exposures more effectively as everything they need to complete their roles effectively is on hand in one place.

For more information on how **Cantium** can help your organisation, please contact [info@cantium.solutions](mailto:info@cantium.solutions)



in partnership  
with



**tenable**