

TRUSTLAYER VS MICROSOFT

Web filtering comparison guide

TrustLayer Web Security Module

TrustLayer™



Welcome

Amid the escalating challenges of the digital landscape, robust web filtering is no longer optional—it's critical to protect against the growing wave of cyber threats.

With organisations relying on the internet to power their operations, the stakes have never been higher. A cutting-edge web filtering solution is your first line of defence against these rising risks.

While Microsoft provides web filtering through Defender for Endpoint and other solutions, it faces significant limitations in terms of granularity, customisation, and threat detection. These limitations can leave organisations vulnerable to sophisticated cyber threats.

This document provides a detailed comparison between **TrustLayer Web Security Module** and **Microsoft Defender for Endpoint - Web Content Filtering**.

We will demonstrate why TrustLayer's solution offers superior protection and greater flexibility, backed by real-world examples of where Microsoft has fallen short.

By the end of this document, you will have a clear understanding of the benefits that the TrustLayer Web Security Module can bring to your organisation.

Web filtering comparison

Picking the right web filtering solution comes down to which platform gives you the control, insights, and support that fit your organisation's needs. This guide breaks down the web filtering functionality of **TrustLayer's Web Security Module filtering** and **Microsoft's Defender for Endpoint - Web Content Filtering**.

We cover management, policy controls, reporting, and actionable insights, highlighting where each solution stands out. By the end, you'll have a clear view of which one aligns best with your security goals.

Management and deployment

Managing web filtering across multiple tenants and devices can be challenging. Here's a comparison of TrustLayer and Microsoft's approaches to multi-tenant management and deployment options, showing which platform offers broader and centralised control.

	TrustLayer Web Security	Microsoft Defender
Multi-tenant management	Managing multiple tenants with a centralised view for easy monitoring and control of each tenant's configurations	Limited multi-tenant support
Deployment	Gateway-based and endpoint-level filtering for all operating systems (Windows, macOS, Linux, iOS, and Android)	Primarily endpoint-based filtering (via Defender for Endpoint)

Policy, control and filtering options

Effective filtering isn't just about blocking sites; it's about having control over who can access what, and when. This section breaks down the options for setting policies, customising filtering by category, and applying time- or location-based rules, comparing how TrustLayer and Microsoft measure up in flexibility.

	TrustLayer Web Security	Microsoft Defender
Granular policy control	Highly customisable: rules based on user, Destination, AD groups, organisational units, tags, device groups, device types, operating system, Time, Quota and browser type	Limited policy control, device-based
Web categories	500+ predefined categories, with options to Warn, Allow, Redirect, Block, and Quota time access with unblock request capability	Less automation, limited threat analysis, uncertain on quota
Custom time-based filtering	Allows custom time-based filtering/reporting (e.g., 6 AM – 6 PM, 6 PM – 6 AM) this can also include other conditions such as AD user, Groups...etc	Not available
Geo-specific controls	Blocks access to specific countries deemed to be high risk at the web filtering level	Limited via Conditional Access

Web filtering comparison

Reporting and insights

Reporting lets you see what's happening on your network and catch potential issues early. Here's a look at how TrustLayer and Microsoft handle reporting and insights, covering data depth, scheduling, integration with other security tools, and options for tracking user behaviour.

	TrustLayer Web Security	Microsoft Defender
Reporting and insights	Raw data for custom analysis, including user-level insights, flexible schedule of sending report, multiple SIEM integrations, and a user-friendly analytics dashboard	Basic endpoint-focused reports, limited customisation
User behaviour insights	User-specific activity reports that can highlight non-productive and potential suspicious activities	Limited detailed user behaviour tracking

Actionable insights and recommendations

Filtering and monitoring are only part of the equation; actionable insights help you actively improve your security stance. This section compares the support each platform offers for customised guidance and recommendations, highlighting which service provides more proactive security insights without extra costs.

	TrustLayer Web Security	Microsoft Defender
Actionable insights	Custom analysis and recommendations provided by dedicated security teams at no additional cost	Recommendations come with extra cost

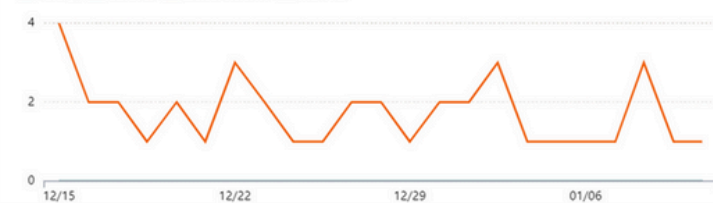
Web protection

Last 30 days ▾

Web threat detections over time

Attempts to access malicious URLs

■ Phishing ■ Malicious ■ Custom Indicator ■ Unknown



Web activity by category

Last 30 days | Updated Mon Jan 13 2020

Web categories with the most activity change

Parent web category | Change in access requests

Adult content ▼ 60%

High bandwidth ▲ 55%

Leisure ▼ 44%

Legal liability No data

Uncategorized No data

Chart example: Microsoft 365 Defender

This dashboard offers a basic 30-day overview of web threats and category changes, showing only broad threat types like Phishing and Malicious.

Where Microsoft falls short

01

Difficulty detecting dynamically weaponised phishing links

While Microsoft's web filtering solution offers basic protection, there have been instances where phishing URLs became weaponised after delivery, leaving organisations vulnerable.

TrustLayer's real-time URL categorisation actively scans URLs, ensuring that dynamically altered threats are identified and blocked as soon as they appear, significantly reducing risks.

Source: [Firewall Times](#)

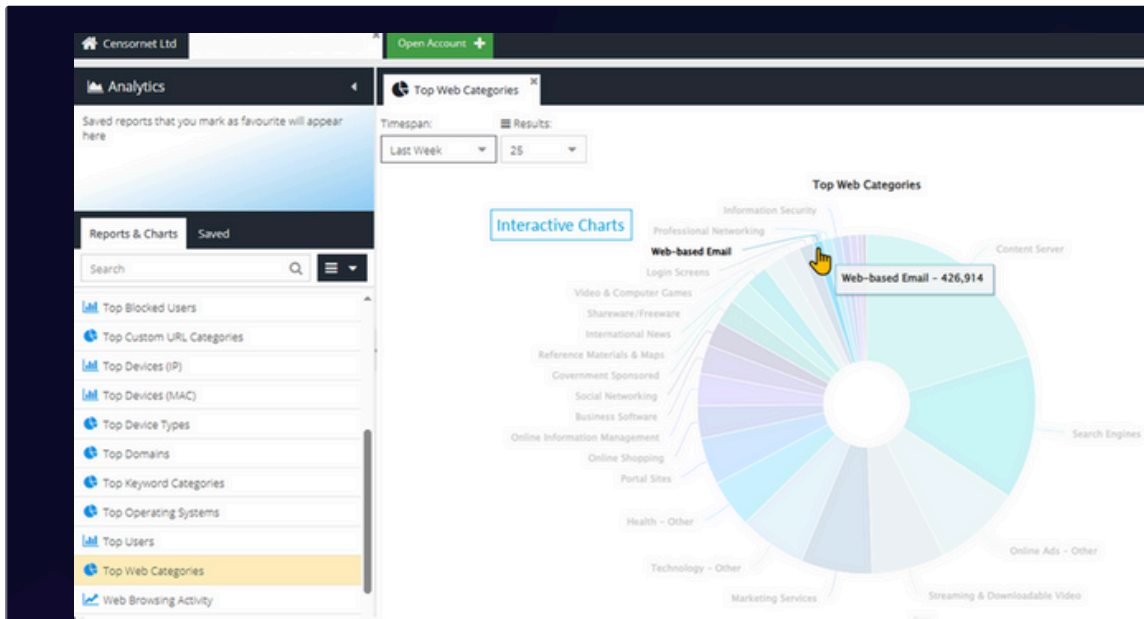
02

Limited real-time geo-blocking capabilities

Microsoft offers geo-specific controls via Conditional Access, but real-time geo-blocking directly at the web filtering layer, is limited.

TrustLayer's geo-specific filtering allows organisations to block traffic to high-risk regions instantly, providing immediate protection against threats originating from known hostile countries.

Source: [TrustLayer Geo Location](#)



TrustLayer Web Security filtering - comprehensive analytics

The TrustLayer dashboard offers in-depth analytics with interactive charts, e.g. top web categories accessed within a configurable time period.

TrustLayer provides granular insights into user activities across multiple categories (e.g., web-based email, social networking, video and computer games), enabling organisations to monitor specific activity trends and make data-driven decisions.

With customisable filters, administrators can easily drill down into user, device, and category-specific details, offering significantly more control and visibility compared to Microsoft's basic reporting.

03

Limited coverage for Bring Your Own Device (BYOD) traffic

Microsoft's web filtering focuses on endpoint protection, which can limit its ability to secure BYOD (Bring Your Own Device) traffic.

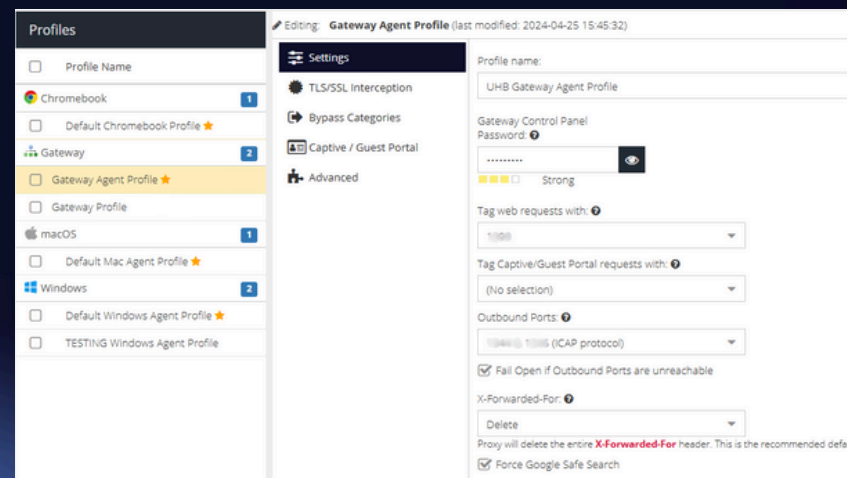
In contrast, TrustLayer's gateway-based filtering ensures all traffic, including personal devices, is protected, helping organisations maintain a consistent security posture across all devices.

04

Limited customisation in reporting

Microsoft's reports, while useful, often require additional manual analysis to identify security trends and anomalies.

TrustLayer provides raw data that security teams can customise and analyse to generate tailored, actionable insights that are specific to an organisation's security posture and user behaviour.



TrustLayer configuration dashboard

This screenshot showcases the TrustLayer Web Security Configuration dashboard, where administrators can manage various profiles for different devices and platforms, i.e corporate devices vs BYOD.

The dashboard offers options to configure agents for Chromebooks, Gateways, macOS, and Windows, enabling comprehensive protection across multiple device types.

This flexibility ensures that organisations can apply specific security policies to different environments, including both default and custom agent profiles, enhancing overall web security management.

Where TrustLayer stands out

01

Multi-tenant management

TrustLayer makes managing multiple tenants straightforward with a centralised dashboard, allowing administrators to control configurations across all tenants.

Microsoft offers limited support for multi-tenant environments, making TrustLayer the better choice for organisations needing efficient, centralised control.

02

Deployment across all devices

TrustLayer provides gateway-based and endpoint filtering that covers all operating systems, including Windows, macOS, Linux, iOS, and Android. It even protects Bring Your Own Device (BYOD) environments comprehensively.

In contrast, Microsoft primarily focuses on endpoint protection, leaving gaps for non-endpoint devices.

03

Granular policy control

TrustLayer, offers granular control with custom block and allow lists from 500 categories and extensive subcategories, such as "Malicious" or "Piracy." This flexibility ensures you can tailor web access to align with your organisation's policies, blocking risks while permitting necessary sites.

Microsoft's controls are more limited, lacking the flexibility and granularity that TrustLayer's platform offers.

04

Extensive web categories

TrustLayer supports over 500 predefined web categories with options to Warn, Allow, Redirect, Block, and Quota access.

This granular category management contrasts with Microsoft's simpler, less granular approach, which could result in security gaps.

05

Actionable recommendations from dedicated teams

TrustLayer's Customer Success Managers (CSM) and Account Managers (AM) provide tailored recommendations at no additional cost, based on thorough analysis of the organisation's activity.

Microsoft charges extra for similar support services.

06

Real-time traffic monitoring and blocking

TrustLayer's web filtering blocks harmful sites in real-time, protecting users from phishing, malware, and other threats. With customisable rules, you can tailor the level of scrutiny based on the risk level of the content accessed.

Microsoft is limited via Conditional Access

Final note:

Microsoft's Defender for Endpoint Web Content Filtering solution has shown significant weaknesses in threat detection and customisation. Its reliance on endpoint protection leaves organisations exposed, particularly when dealing with non-endpoint devices or dynamically evolving threats.

In comparison, **TrustLayer's Web Security Module** delivers flexible, real-time protection against modern threats with fully customisable policies and deep insights. Offering granular control, integration with tools like Posture Management, and the ability to secure all traffic across devices and locations, it ensures robust, adaptable security while supporting productivity.

In addition to web filtering, integrating **TrustLayer's CASB** (Cloud Access Security Broker) provides even more value for your organisation. With CASB, you gain visibility and control over cloud applications, ensuring that only sanctioned apps are allowed and that unsanctioned or risky apps are blocked.

CASB also helps enforce data loss prevention (DLP) policies and protects sensitive information from being shared or uploaded to unapproved cloud apps, adding a critical layer of security to your cloud infrastructure.

Key benefits of TrustLayer CASB include:

- ✓ **Visibility and control over cloud app usage:**
Monitor and control all cloud applications in use, ensuring only approved apps are accessible.
- ✓ **Compliance and security posture management:**
Maintain compliance with regulatory standards and improve your overall security posture by enforcing granular policies on cloud apps.

With TrustLayer CASB combined with Web Security filtering, your organisation gains a holistic security solution that protects not only your network traffic but also your cloud environment, ensuring a secure and compliant infrastructure.

TrustLayer provides superior control, deeper insights, and the ability to secure all traffic—whether from cloud apps, the web, or personal devices—making it the best choice for organisations that require robust, adaptable, and integrated security solutions.

About TrustLayer

Headquartered in an innovation hub in Basingstoke, UK, TrustLayer gives mid-market organisations the confidence and control of enterprise-grade cyber protection.

Its AI powered cloud security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed.

TrustLayerTM

trustlayer.co.uk