UTM

UNIFIED THREAT MANAGEMENT

Centralised management, monitoring, protection and control of all endpoint devices while connected to the internet.

What is UTM?

Unified Threat Management (UTM) is the centralised management, monitoring, protection and control of all endpoint devices including; servers, computers, laptops and mobile devices. UTM protects these devices from cyber threats while they are connected to the global internet.

The global internet, although a reliable cost-effective method of connecting endpoint devices together, comes with inherent security risks for users. Threats such as malware, ransomware, denial of service and network layer attacks can cause the remote user network or end user device to be compromised, potentially spreading the threat and causing financial and operational risk.

Protection against known and unknown threats

UTM ensures business continuity by providing users with the ability to use a single centralised management solution to ensure all endpoint devices, network servers and network firewalls are monitored and protected.

Deep learning device protection

UTM ensures that all endpoints are monitored for cyber threats using deep learning artificial intelligence to detect known and unknown malware without relying on common attack signatures. It simplifies the security management of a network and endpoint devices by implementing a single hardware and software solution across the entire platform. The implemented solution elements collectively engage with one another, monitoring files and traffic on the network and endpoint devices, ensuring that threats and zero-day attacks are pro-actively identified and dealt with to prevent them spreading to any other endpoints, servers or network devices.

Simplicity

Easy to configure, manage and maintain the system includes an intuitive admin workflow, a flexible self-service portal and the ability to allow administrators to centrally manage security, data and application policies that are remotely pushed to devices.

Content Protection

A secure container on the endpoint devices stores and protects corporate applications and sensitive files.

Web Access and Application Control

Web access provides centralised management of which websites can be accessed from the device and how they can be accessed, while application control provides management over which applications can be installed on the device and how they can be used .

Firewalls

UTM is deployed with endpoint and core firewalls providing the added advantage of synchronized cyber security, where all hardware and software elements function in unison to provide a complete in-transit and at rest file protection.

Compatibility

Endpoint devices including Android and iOS mobile devices, Windows and MACOS desktop and laptop device.
Servers including Window OS , Virtual Servers, Hyper-V, ESXi, Azure and Linux.