Unified threat management

Unified threat management (**UTM**) is an approach to information security where a single hardware or software installation provides multiple security functions. This contrasts with the traditional method of having point solutions for each security function.[1] UTM simplifies information-security management by providing a single management and reporting point for the security administrator rather than managing multiple products from different vendors.[2][3] UTM appliances have been gaining popularity since 2009, partly because the all-in-one approach simplifies installation, configuration and maintenance.[4] Such a setup saves time, money and people when compared to the management of multiple security systems. Instead of having several single-function appliances, all needing individual familiarity, attention and support, network administrators can centrally administer their security defenses from one computer. Some of the prominent UTM brands are Cisco, Fortinet, Sophos, Netgear, FortiGate, Huawei, WiJungle, SonicWall and Check Point.[5] UTMs are now typically called next-generation firewalls.

Features

UTMs at the minimum should have some converged security features like

- Network firewall
- Intrusion detection service (IDS)

-
- Intrusion prevention service (IPS)

Some of the other features commonly found in UTMs are:

- Gateway anti-virus
- Application layer (Layer 7) firewall and control
- Deep packet inspection
- Web proxy and content filtering
- Email filtering for spam and phishing attacks
- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Virtual private network (VPN)
- Network access control
- Network tarpit
- Additional security services against Denial of Services (DoS), Distributed Denial of service (DDoS), Zero day, Spyware protection

Disadvantages

Although an UTM offers ease of management from a single device, it also introduces a single point of failure within the IT infrastructure. Additionally, the approach of a UTM may go against one of the basic information assurance / security approaches of defense in depth, as a UTM would replace multiple security products, and compromise at the UTM layer will break the entire defense-in-depth approach.[6]

References

1. *"Unified Threat Management" (https://web.archive.org/web/20170713223746/https://www.gartner.com/reviews/market/unified-threat-management-worldwide)* . *Gartner. Archived from the original (https://www.gartner.com/reviews/market/unified-threat-management-worldwide) on 13 Jul 2017. Retrieved 11 December 2017.*

2. *"Unified threat management devices" (https://web.archive.org/web/20171211171847/http://searchsecurity.techtarget.com/essentialguide/Unified-threat-management-devices-Understanding-UTM-and-its-vendors)* . *Techtarget. Wayback Machine. Archived from the original (http://searchsecurity.techtarget.com/essentialguide/Unified-threat-management-devices-Understanding-UTM-and-its-vendors)* on 11 December 2017. Retrieved 11 December 2017.

3. *"UTM and Firewall Growth Drive the Worldwide Security Appliance Market Expansion in Q2 2017" (https://web.archive.org/web/20171211173416/https://www.businesswire.com/news/home/20170918005122/en/UTM-Firewall-Growth-Drive-Worldwide-Security-Appliance)* . *Business Wire. Wayback Machine. 18 September 2017. Archived from the original (https://www.businesswire.com/news/home/20170918005122/en/UTM-Firewall-Growth-Drive-Worldwide-Security-Appliance)* on 11 December 2017. Retrieved 11 December 2017.

4. *"What are common (and uncommon) unified threat management features?" (https://searchmidmarketsecurity.techtarget.com/tip/What-are-common-and-uncommon-unified-threat-management-features)* . *SearchMidmarketSecurity. Retrieved 2019-04-04.*

5. *"10 Top Unified Threat Management Vendors" (https://web.archive.org/web/20190723094354/https://www.esecurityplanet.com/products/top-utm-unified-threat-management-vendors.html)* . *2019-07-23. Archived from the original (https://www.esecurityplanet.com/products/top-utm-unified-threat-management-vendors.html)* on 2019-07-23. Retrieved 2019-07-23.

6. *Todd McGuiness. "Defense in Depth" (https://web.archive.org/web/20171222145222/https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525)* . *sans.org. Archived from the original (https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525)* on 22 Dec 2017. Retrieved 22 December 2017.

Last edited 8 months ago by Citation bot