ıılııılıı
CISCO

Cisco Umbrella Education Package

Cisco Umbrella secures internet access and controls cloud app usage for students and staff across your campus network. Umbrella acts as a secure onramp to the internet to support compliance and provide effective threat protection for students and staff, both and off-campus. Backed by Cisco Talos, one of the largest threat intelligence teams in the world, Umbrella blocks threats before they can reach your network or endpoints. Delivered from the cloud with 100% uptime, Umbrella offers protection and enforcement for students and staff anywhere they access the internet.

The Cisco Umbrella Education package, exclusively for K-12 schools and higher education institutions, is licensed by the number of faculty and staff users. There is zero charge for students!

	Education	DNS Security Essentials	DNS Security Advantage
	exclusively for schools and colleges	for small education organizations or as first line of defense for any size education organization	for education organizations and mid-size businesses who need deeper inspection and control
Licencing	by # of faculty and staff users. No charge for students	by # of users	by # of users
Security & Controls			
DNS-layer security			
Block domains associated with phishing, malware, botnets, and other high risk categories (cryptomining, newly seen domains, etc.)	●	●	●
Block domains based on partner integrations (Splunk, Anomali, & others) and custom lists using our enforcement API	●	●	●
Block direct-to-IP traffic for C2 callbacks that bypass DNS[1]			●
Secure web gateway			
Proxy web traffic for inspection			Traffic associated with risky domains via selective proxy
Decrypt and inspect SSL (HTTPS) traffic			With selective proxy
Enable web filtering	By domain or domain category	By domain or domain category	By domain or domain category
Create custom block/allow lists	Of domains	Of domains	Of domains
Block URLs based on Cisco Talos and third party feeds, and block files based on AV engine and Cisco Advanced Malware Protection (AMP) data			With selective proxy
Use Cisco Threat Grid cloud sandbox environment to analyze suspicious files (200 files/day)			
Use retrospective security to identify previously-benign files that became malicious			
Cloud-delivered firewall			
Create layer 3/layer 4 policies to block specific IPs, ports, and protocols			
Use IPSec tunnel terimination			
Cloud access security broker			
Discover and block shadow IT (based on domains) with with our App Discovery report	●	●	●
Discover and block shadow IT (based on URLs) with App Discovery report			
Create policies with granular controls (block uploads, attachments, and posts) for select apps			
Umbrella Investigate			
Access Investigate's web console for interactive threat intelligence (5 logins)			●
Use the Investigate on-demand enrichment API to enrich other tools/systems with domain, URL, IP, and file threat intelligence (2,000 requests per day)			●
Integrate with Cisco Threat Response to aggregate threat activity across Cisco AMP, Threat Grid, Email Security, NGFW, and Umbrella	With enforcement API only	With enforcement API only	●

	Education	DNS Security Essentials	DNS Security Advantage
	exclusively for schools and colleges	for small education organizations or as first line of defense for any size education organization	for education organizations and mid-size businesses who need deeper inspection and control
Licencing	by # of faculty and staff users. No charge for students	by # of users	by # of users

Security & Controls

Traffic forwarding

	Education	DNS Security Essentials	DNS Security Advantage
Forward external DNS traffic for: • On-network protection via Cisco (SD-WAN, Meraki MR, Integrated Services Router, & Wireless LAN Controller) and third party integrations (Cradlepoint, Aerohive, & others) • Off-network protection via AnyConnect, Umbrella roaming client, and Cisco Security Connector for iOS	●	●	●
Send outbound network traffic via IPSec tunnel, proxy chaining, or PAC filesl			

User attribution

	Education	DNS Security Essentials	DNS Security Advantage
Create policies and view reports by: • Network (egress IP) • Internal subnet[2] • Network device (including VLAN or SSID)[3] • Roaming device • Active Directory group membership (including specific users)[4]	●	●	●
Create policies and view reports using SAML			

Management

	Education	DNS Security Essentials	DNS Security Advantage
Customize block pages and bypass options	●	●	●
Use our multi-org console to centrally manage decentralized orgs	●	●	●
Use our management API to create, read, update, and delete identities using own internal tools	●	●	●

Reporting and logs

	Education	DNS Security Essentials	DNS Security Advantage
Leverage real-time activity search and our reporting API to easily extract key events	●	●	●
Choose North America or Europe for log storage	●	●	●
Use customer or Cisco-managed AWS S3 bucket to export and retain logs as long as needed[5]	●	●	●
Access domain request logs in our user interface (30 day: detail, 1yr: summary)	●	●	●
Access full URL logs in our user interface (30 days: detail)			
Access firewall (IP, port, and protocol) logs in our user interface (30 days: detail)			

Support

	Education	DNS Security Essentials	DNS Security Advantage
Basic	Basic included — email	Enhanced required — 24 x 7 technical + on-boarding	
Optional	Gold add-on Basic and 24x7 P1 and 24x5 P2 and P3 phone support Platinum add-on Gold Support and dedicated Technical Account Manager	Premium add-on — 24 x 7 technical on-boarding + Technical Account Manager (TAM)	

Footnotes:

1. Requires endpoint footprint (Umbrella roaming client, Chromebook client, or AnyConnect roaming module)
2. Internal IP attribution requires network footprint (our virtual appliance), Meraki MR integration, Cisco ISR integration, or Cisco ASA integration, or Cisco SD-WAN integration. Select third-party integrations available too
3. Requires network device integration with Cisco Integrated Services Router (ISR) or Cisco Wireless LAN Controller or Meraki MR
4. Active Directory (AD) policies and attribution requires Umbrella AD connector with network footprint (Umbrella virtual appliance) or endpoint footprint (Umbrella roaming client or AnyConnect roaming module)
5. No Amazon account required when using the Cisco-managed S3 bucket