Cisco Umbrella

ebook

30 minutes to a more secure network, on campus and off

Protecting school systems from kindergarten through higher ed

Cisco Umbrella

Table of Contents

Taking the stress out of security

Maintaining strong network security has become more challenging than ever in today's educational ecosystem. That's because the adoption of advanced learning technologies, along with an increased reliance on cloud applications and services, have introduced new security threats that must be met head on.

Unfortunately, relying on traditional tools such as anti-virus software and firewalls to protect your network simply isn't enough anymore, leaving your institution at risk. It's time to look for new ways to enhance your digital security without lengthy lead times, prohibitive technical requirements, or additional management responsibilities.

In this ebook, we'll look at today's security challenges facing K-12 and higher education institutions. We'll then explore some simple actions you can take to secure your network in 30 minutes or less – reducing malware, simplifying security, and improving overall performance.

The changing educational security landscape

Educational institutions have long needed to adopt and incorporate new teaching and learning platforms into their ecosystems to keep up with ever-changing technology. For instance, the recent pivot to distance learning has led schools worldwide to rapidly deploy new devices, new applications, and new services to continue their educational missions.

But unfortunately, these new tools have often been implemented without a thorough vetting process or proper training, leaving administrators, educators, and students vulnerable.

School IT systems not only collect and manage sensitive data about students and their families, but about teachers, support staff, and district operations. This data may be hosted locally on premises or in shared hosting arrangements with other local government entities. But increasingly, it's hosted by an ecosystem of vendors in the cloud on systems accessible by any internet-connected device.

The result? A growing number of education institutions have reported identity theft, credit fraud, and other cyber crimes that resulted in stolen taxpayer dollars, breaches of student data, and even school closures.

Schools under siege

Cyber Incidents

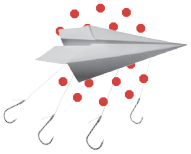
1,180

since 2016[1]

Ransomware

K-12 schools accounted for

57% of all incidents[2]



Spear-Phishing Thefts

$2 million

median cost per incident[1]

Attacks from all sides

As your network changes, so do the attack methods. The speed and adaptability with which attackers spin up attack infrastructures creates new challenges for identifying and blocking malicious traffic, including:

Email spear-phishing techniques

that enable attackers to bypass conventional defenses and install ransomware and malicious code.

Low and slow attacks

that evade network-based defenses and allow attackers to infiltrate infrastructure and take data undetected over extended periods of time.

One-off malware packages

that can't be readily detected using signature-based solutions – regardless of how quickly those signatures and profiles are updated.

Ransomware attacks

that illegally plant malware in a computer or mobile device, disabling its operation or access to data until payment is made to regain control.

Malware kits and malware-as-a-service resources

that increase threat volume by empowering bad actors and criminal organizations to engage in cyberattacks like malicious cryptomining, despite their lack of technical skills.

Cisco Umbrella

DNS-layer security: your first line of defense

Malware, ransomware, phishing, and other scams use DNS servers to look up and connect to your network infrastructure. In fact, 91% of malware uses DNS to gain command and control, exfiltrate data, or redirect web traffic.

But DNS-layer security identifies where malicious domains and other internet infrastructures are staged, and blocks requests prior to making a connection, preventing both infiltration and exfiltration attempts. By resolving internet requests with a recursive DNS service, you can easily check for and block malicious or inappropriate domains.

DNS is one of the most valuable sources of data within an organization. It should be mined regularly and cross-referenced against threat intelligence. This can help your IT staff achieve better accuracy and detection of compromised systems while improving visibility and network protection. Many IT leaders have already made proactive DNS-layer security.

Proactive DNS-layer security made easy

1. Blocks dangerous connections between your users and malicious domains
2. Stops command-and-control (C2) callbacks and data exfiltrations automatically
3. Reduces security incidents and alerts by neutralizing them before they occur

of malware uses DNS to gain command and control, exfiltrate data, or redirect web traffic.

Are your research grants at risk?

Each year, the U.S. government issues $8B in research grants. To be eligible, universities must attain Level 3 of what's known as Cybersecurity Maturity Model Certification (CMMC). Because DNS-layer security is a key requirement of CMMC, it's critical your institution add this capability to your security arsenal – or risk losing out on much-needed funding.

A better, faster way to stop threats

Increase visibility, decrease risk and get back to education

Most organizations leave their DNS resolution up to their internet service provider (ISP). But as more institutions adopt direct internet connections and users bypass the VPN, this can lead to a DNS blind spot. DNS requests precede the IP connection, which enables DNS resolvers to log requested domains regardless of the connection's protocol or port.

Monitoring DNS requests (as well as subsequent IP connections) is an easy way to provide better accuracy and detection of compromised systems, which improves security visibility and network protection.

The bottom line: Your IT team can adopt more effective security strategies without adding complexity to their security operations.

What makes DNS-layer security so indispensable?

DNS-layer security operates on the simple principle that attacks — no matter how sophisticated or unique — must originate from somewhere. By preemptively blocking all requests over any port or protocol to any and all suspicious destinations, DNS-layer security can stop command-and-control exfiltration, malicious cryptomining, ransomware, and other attacks without needing to identify the specific nature of those attacks. Bad domains get blocked because they are quickly and accurately identified.

DNS-layer security delivers:

- **Predictive identification of malicious hosts.** By aggregating and analyzing DNS-related data, including tens of billions of daily DNS requests, WHOIS records, and Border Gateway Protocol routing information, it's possible to identify suspicious domains with a very high degree of accuracy.
- **DNS request blocking as a cloud service.** Armed with a constantly updated list of suspect domains, a cloud service provider can preemptively block requests for any domain or IP that might pose a threat to the business.

1 in 3

reported breaches could have been controlled by DNS[3]

$100 – 200B

global losses could have been prevented by DNS[3]

The Umbrella Advantage

620B
daily DNS requests

24K+
Umbrella enterprise customers

170M+
malicious DNS queries blocked daily

35+
data centers across five continents

1,000+
partnerships with top ISPs and CDNs

Why Cisco Umbrella?

Umbrella is committed to delivering the best, most reliable, and fastest internet experience to every single one of our users. We are the leading provider of network security and DNS services, enabling the world to connect to the internet with confidence on any device.

More than a decade of DNS leadership.

Fifteen years of hands-on experience working with DNS technology and data gives Cisco Umbrella significant advantages when it comes to understanding and blocking attacker infrastructure.

Unmatched DNS data volume and variety.

Cisco Umbrella possesses unmatched visibility into DNS activity worldwide. Umbrella processes 620 billion internet requests from over 24 thousand customers across 190+ countries worldwide.

Predictive intelligence and statistical models.

Cisco Umbrella has developed highly specialized models that block 7 million malicious destinations at any given time.

Highly resilient cloud infrastructure.

Umbrella boasts 100% uptime since 2006. Using Anycast routing, any of our 35+ data centers across the globe are available using the same single IP address. Requests are sent transparently to the nearest, fastest data center, and failover is automatic.

Integrations that amplify investments.

Umbrella unifies multiple security services in a single cloud platform to secure access to the internet and control cloud app usages anywhere users go. Users can manage security policies and enforcement across their entire infrastructure from a single dashboard, through integrations with Cisco SD-WAN architecture, Cisco Meraki MR and MX, and Cisco ISR routers, Cisco Secure Network Analytics, and Cisco Secure Endpoint.

Umbrella DNS-layer security

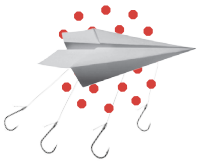
Blocking threats others miss

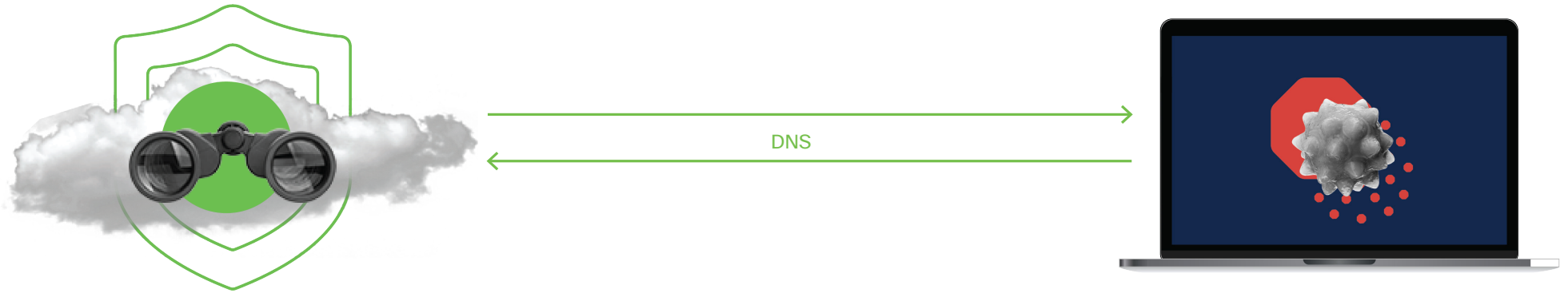
By enforcing security at the DNS layer, Umbrella blocks requests to malware, ransomware, phishing, and botnets before a connection is even established – stopping threats over any port or protocol before they reach your network or endpoints, without adding latency. Umbrella blocks direct IP connections from command-and-control callbacks for roaming users.

Umbrella categorizes and retains all internet activity to simplify the investigation process. Using the Umbrella Investigate console and on-demand enrichment API, it provides context to prioritize incidents and speed up incident response so you can detect and remediate threats faster.

91% of malware uses DNS in attacks

89% of institutions don't protect students and faculty from phishing attacks



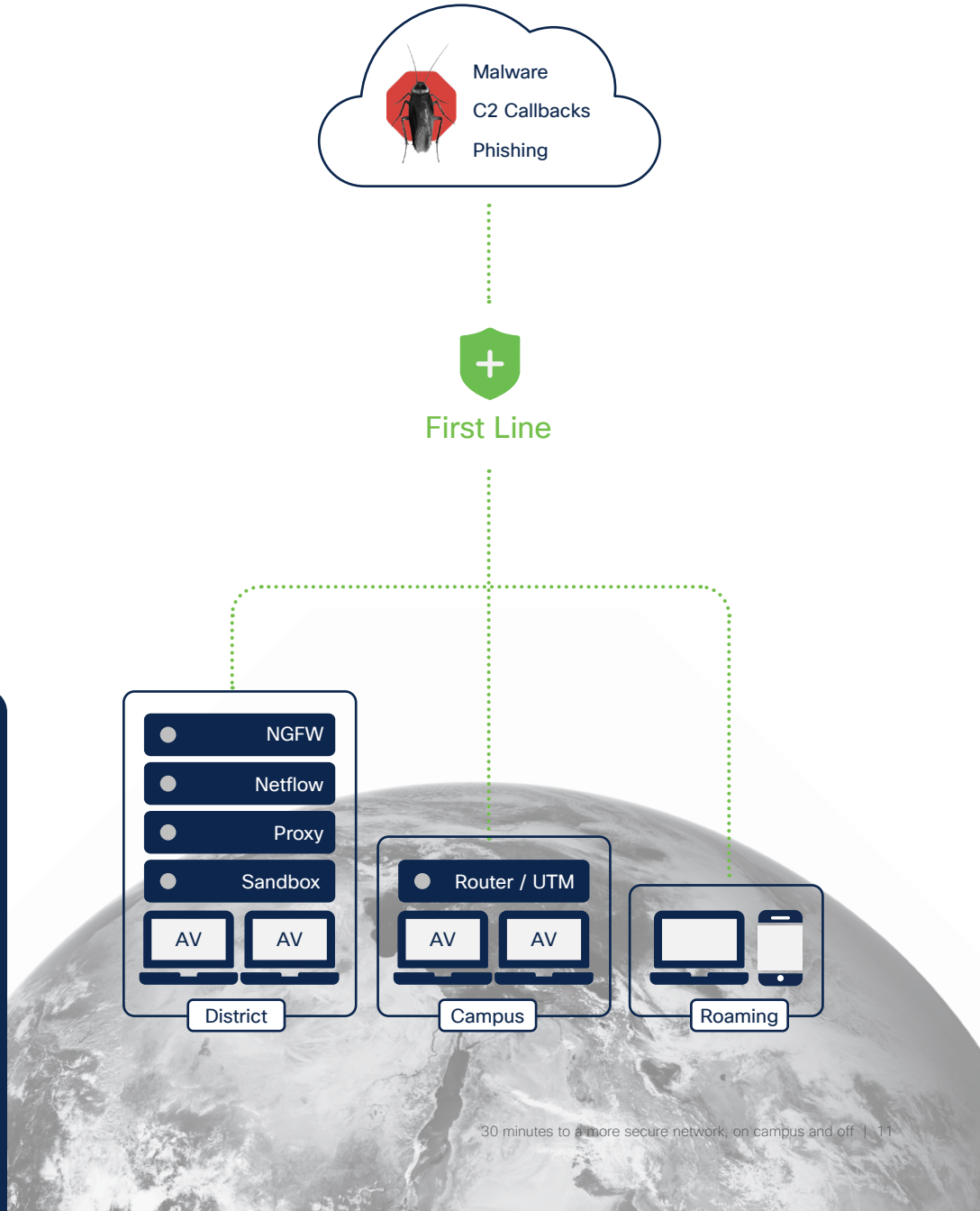


Cisco Umbrella

Where does Umbrella enforce security?

Leveraging unmatched threat insights from Cisco Talos, one of the largest commercial threat intelligence teams in the world, Umbrella uncovers and blocks a broad spectrum of malicious domains, URLs, and files that are being used in attacks. We also feed huge volumes of global internet activity into a combination of statistical and machine learning models to identify new attacks being staged on the internet.

These distinctive attributes make Umbrella inarguably the best choice for K-12 and higher education school systems. Umbrella helps empower security teams of all sizes to take back control of their systems. It provides effective security protection and internet-wide visibility, both on and off network, without adding complexity to their environments



Benefits

- Blocks malware before it hits the organization
- Provides faster internet access
- Contains malware if already inside
- Provisions globally in minutes

Umbrella in Action

Organization:
Lewisville Independent School District (LISD)

Headquarters:
Lewisville, Texas

Users:
50,000 students

Network:
5 high schools,
15 middle schools, and
40 elementary schools

"When everybody went remote last year, we simply deployed the Cisco Umbrella agent to all of the devices so that we had the same filtering off-site that we had when we were on-site. It provided another layer of protection that we didn't have before. In the first month of the 2020–2021 school year, we saw a major increase in phishing emails. Our system blocked 16 million email threat messages during that month alone."

Chris Langford, Director of Network, Infrastructure, and Cybersecurity

Umbrella in Action

Organization:
The Texas A&M University System

Headquarters:
College Station, Texas

Users:
183,000

Network:
11 campuses and 9 state government agencies

"The biggest impact we saw from Umbrella was the drop in the number of security alerts on our other tool sets. We're probably saving about 100 hours per week across all of my employees due to the reduction in these alerts."

Dan Basile, Executive Director, Cybersecurity Service

"We can show our Board of Regents as well as our CEOs at each of the universities how much malware we've blocked and how many sites we've blocked to prove how effective we are. Plus, we can now focus on much deeper threats versus the mass of different malware that's filtered out. That's a big deal."

Danny Miller, Chief Information Security Officer

Cisco Umbrella

Utilize the internet to your security advantage

Proactive DNS-layer security is the simplest decision you can make to improve the security posture of your school or university. Once deployed, it improves visibility and network protection, block threats before they become actual attacks, and simplifies overall security management.

Umbrella is the fastest and easiest way to protect all of your users in minutes, on and off the network. With no hardware to install and no software to manually update, ongoing management is simple. You simply redirect your DNS to Cisco Umbrella. That's it. Then you can leverage your existing Cisco footprint – Cisco AnyConnect, Cisco routers (ISR 1K and 4K series), Cisco Wireless LAN Controllers, and Meraki MR/MX – to provision thousands of network devices and laptops in minutes.

Umbrella customers reduce malware by 75%[6] and reduce remediation times by 50% or more.[7]

Interested in experiencing Umbrella for yourself?

Enable threat protection across your institution in minutes.

Try it out for 14 days.

Start Your Free Trial

Sources:

1. *The K-12 Cyber Incident Map*, The K-12 Cybersecurity Resource Center, February, 2021.
2. *Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data*, CISA, December, 2020.
3. *Measuring The Economic Value of DNS Security*, Global Cyber Alliance.
4. *Cisco Security Research Report: Majority of Orgs Do Not Monitor DNS*, Cisco, January, 2016.
5. *DMARC Adoption Among US Colleges and Universities*, March, 2018.
6. *TechValidate Research on Cisco Umbrella*, TechValidate, March 2019.
7. *TechValidate Research on Cisco Umbrella*, TechValidate, March 2019.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

SOC 2 Compliant