


Cisco Umbrella
vs
Palo Alto Networks DNS Security

Buyer's Guide & Reviews

July 2022

PeerSpot

Get a custom version of this report...personalized for you!

Thanks for downloading this PeerSpot report.

Note that this is a generic report based on reviews and opinions from the entire PeerSpot community. We offer a customized report personalized for you based on:

- Your industry
- Company size
- Which solutions you're already considering

It includes recommendations for you based on what other people like you are researching and using.

It takes 2-3 minutes to get the report using our shortlist builder wizard. We recommend it!

Get your personalized report here.

Contents

Advice From Real Users

Cisco Umbrella

PROS

Dustin Funkhouser

"When it comes to hybrid work it's pretty effective." "We've got the agents." "We can protect people inside our building and, when they're using their laptops out in the field, they're still protected." "It's working well." [Full Review]

Jessica Boutin

"The most valuable features for us include tenant lock, content filtering, and DLP solutions, looking for PII and information being exfiltrated." [Full Review]

Michael Abadeer

"It enables us to go granular in the customization of blocking some categories on the DNS." [Full Review]

J.J. Ruiz

"The Global Block List is one of the most valuable features because it's really easy to block domain names as well as URLs." "Sometimes you don't want to block the whole site, you just want to block one URL." "The Global Block and Allow Lists are the best features for us." [Full Review]

Walter Poole

"If it didn't have a single pane of glass, we would not be using it." "The single pane of glass gives you a one-stop shop." "It's like going to Home Depot." "You find all your stuff there." "You can see all your threats and your endpoints." "It's a very important feature and makes things very simple." [Full Review]

Tony Hon

"Application performance has greatly improved and there are less operational issues." "Productivity has been going up because we have less operational issues." "Also, we have happy customers." [Full Review]

John Okunade

"I like the DNS layer security." [Full Review]

Advice From Real Users

Cisco Umbrella

CONS

Dustin Funkhouser

"If we're trying to deploy it to a Mac through Meraki, it's impossible." "The method of deployment for a Mac, and the features available in Meraki, are not compatible at all." [Full Review]

Jessica Boutin

"There are a couple of different pieces that have different portals." "I know they're working on getting them all into one portal, but that's probably the biggest thing that needs improvement right now." "It's not a single pane of glass yet." [Full Review]

Michael Abadeer

"Having ready-to-go templates with best practices is definitely something that would be an improvement." "Deployment, from day one, is something that definitely needs to be improved for Cisco customers." [Full Review]

J.J. Ruiz

"There are some situations where we would like to block things for specific user groups." "I know that Umbrella does that, but it's not that easy...." "when you want a specific task for specific rules and policies for user groups, you have to go three levels down in the menu, and it's hard to find where you do that task." [Full Review]

Tony Hon

"Network connectivity was a bit of a challenge at the beginning, but we were able to get the right help from Cisco." [Full Review]

John Okunade

"It would be better if there was a little bit of flexibility for organizations that don't have SD One in their environment." "Because of the complexity of the environment, it's not easy to actually turn on the feature of the secure internet gateway for our users." "We have not been able to explore that option yet." [Full Review]

Dan Brunnquell

"There are a couple of interface issues." "I know that they say that there are feature enhancements that are noted." "For example, we've got the Cisco Meraki security appliances, and there, we geofence our company to where we're allowed to send and receive traffic." "So, in our case, by default, we only allow traffic to six different countries, which allows us to effectively prevent traffic for the majority of bad players in the world, but they don't give you an easy way to do that in Cisco Umbrella." "With Cisco Meraki, I can specify or pick the co... [Full Review]

Advice From Real Users

Cisco Umbrella

PRICING AND LICENSING ADVICE

Michael Abadeer

"We have a security Enterprise Agreement with Cisco, so the pricing is good." [Full Review]

J.J. Ruiz

"The pricing is pretty fair." "It's good." [Full Review]

Walter Poole

"There is room for improvement when it comes to the cost." [Full Review]

Dan Brunnquell

"We were using the free version, and we implemented the paid version about two months ago.I'm paying a fair price, but everything is negotiable with Cisco." "One of the benefits that I got by having Cisco Umbrella is the licensing of the Cisco AnyConnect VPN client." [Full Review]

reviewer1407087

"There are no hidden costs with Umbrella." "Everything is included in the package." [Full Review]

Praveen Kumar

"The price depends on the use case, and it's a bit linear." "But it depends on the customer's strategy and how Cisco plans to optimize the costs." [Full Review]

Samuel-Emesoronye

"In the region I'm from, that of EMAR, Europe, the Middle East, Eastern Asia and Africa, our organizations do not have many liquid cash assets, so the price could be better." [Full Review]

Advice From Real Users

Palo Alto Networks DNS Security

PROS

reviewer1692576

"We now have insight into our DNS requests and we can actively see how many thousands of malicious requests have gotten knocked down in the last day or week that we didn't have before." "There's more insight for both security and more insight." [Full Review]

Darshil Sanghvi

"When comparing other cloud-based DNS security solutions to this one I have found the main beneficial feature in this solution to be we do not need to change our architecture." [Full Review]

reviewer1542159

"The stability is excellent and the product is very mature." [Full Review]

reviewer1086276

"The most valuable feature is DNS filtering." [Full Review]

Advice From Real Users

Palo Alto Networks DNS Security

CONS

reviewer1692576

"I'm not really sure what needs improvement." "The only hiccup I've really seen is a couple of the DNS requests get flagged as the Sophos traffic instead of DNS traffic, but that's more of their app detection in the DNS Security." "I haven't really seen any issues with the DNS security." [Full Review]

Darshil Sanghvi

"There should be an on-premise version of this solution." [Full Review]

reviewer1542159

"Every vendor that sells DNS or firewalls needs to be able to protect against DNS look-up attacks and DNS naming hacks." "This is true of Palo Alto as well as others." [Full Review]

reviewer1086276

"We would like to have cloud-based management." [Full Review]

Advice From Real Users

Palo Alto Networks DNS Security

PRICING AND LICENSING ADVICE

Darshil Sanghvi

"There is an annual license for the solution and I am satisfied with the pricing." [Full Review]

Top Reviews by Topic

Cisco Umbrella

Palo Alto Networks DNS Security

VALUABLE FEATURES

Dan Brunnquell

When we have laptops that leave the building, they could connect to public WiFi before they establish a VPN connection back into the company. For that duration or that period of time when they're not docked in the network or on a VPN, they effectively don't have that full layer of security that I provide inside the building. This tool stands in during that period of time, and we extend the security settings through their basic firewall or their cloud-based firewall at that time. So, we do conten... [Full Review]

reviewer1542159

Palo Alto has a range of products. They have very secure 600 DNS as well as 100 DNS. They have anti-hacking features which are quite useful. They have virus protection within the firewall. They have other products that are geared towards protecting the DNS. All of their product line is highly secure with built-in security. You can protect DNS within the firewall as most of the features are built-in. It's not like a product within the firewall. It's already built-in. The initial setup is very, ve... [Full Review]

J.J. Ruiz

The Global Block List is one of the most valuable features because it's really easy to block domain names as well as URLs. Sometimes you don't want to block the whole site, you just want to block one URL. The Global Block and Allow Lists are the best features for us. Cisco Umbrella also provides a single pane of glass for management. It's really helpful and it's important for us because we have multiple locations. Without a single pane of glass, if you want to block websites you have to go to ev... [Full Review]

reviewer1692576

The autofocus piece that gives us insights into how many requests we have and how many malicious requests get denied is the most valuable feature. We didn't really have eyes on the DNS queries. We had some filtering done, but we didn't know which pieces it knocked down and how much work it was doing. The comprehensiveness of DNS Security against emerging DNS layer threats is very good. They seem to have updates nearly daily. My understanding is that it would protect against DNS tunneling, rebind... [Full Review]

reviewer1411335

The most valuable feature which I found in Umbrella is the segmentation of personal accounts from corporate accounts. In order to work with this, Umbrella has a feature where we add the ID of the customer's Gmail account or the Azure account. That ID is then used as a filter to separate access so that only corporate Gmail will be accessible and it can block personal accounts. The second very valuable feature is the web proxy part which is effective in determining if a feed may be malicious. [Full Review]

Darshil Sanghvi

When comparing other cloud-based DNS security solutions to this one I have found the main beneficial feature in this solution we do not need to change our architecture. There was no need to change the configuration or to do any modification to the user's end. The user's DNS will be the same, the traffic will flow through the same firewall, and it will give us the DNS level security. For other OEMs or other solutions, we need to map their DNS to the public DNS and there is a need to modify the DN... [Full Review]

Top Reviews by Topic

ROOM FOR IMPROVEMENT

Cisco Umbrella

Dan Brunnquell

There are a couple of interface issues. I know that they say that there are feature enhancements that are noted. For example, we've got the Cisco Meraki security appliances, and there, we geofence our company to where we're allowed to send and receive traffic. So, in our case, by default, we only allow traffic to six different countries, which allows us to effectively prevent traffic for the majority of bad players in the world, but they don't give you an easy way to do that in Cisco Umbrella. W... [Full Review]

J.J. Ruiz

There are some situations where we would like to block things for specific user groups. I know that Umbrella does that, but it's not that easy. When you go to the Global Allow and Block Lists, that's the easy part. But when you want a specific task for specific rules and policies for user groups, you have to go three levels down in the menu, and it's hard to find where you do that task. Also, the policies are not that easy to manage. [Full Review]

reviewer1411335

Data reporting is something I would like to see improved. Cisco is currently rolling out data centers for this type of solution. Currently, they do not have data centers everywhere. For example, they do have one in Singapore but they do not have one in India. My clients are in India and they find an issue of slowness in the services from the Singapore data center. Cisco is working on building a data center in India to address the issue but information about the completion of that project are lac... [Full Review]

Palo Alto Networks DNS Security

reviewer1542159

Every vendor that sells DNS or firewalls needs to be able to protect against DNS look-up attacks and DNS naming hacks. This is true of Palo Alto as well as others. The IDS and IPS should be built-in. With EDS and IDS, some are proud to have built-in IDS and IPS intrusion protection and intrusion detection as some vendors sell IDS and IPS separately. They shouldn't be separate. Instead of selling two products, it really should just be one. [Full Review]

reviewer1692576

I'm not really sure what needs improvement. The only hiccup I've really seen is a couple of the DNS requests get flagged as the Sophos traffic instead of DNS traffic, but that's more of their app detection in the DNS Security. I haven't really seen any issues with the DNS security. [Full Review]

Darshil Sanghvi

There should be an on-premise version of this solution. There are companies that have asked for a solution that is on-premise. The reason for this is some companies might want to have control of where their traffic is going. For example, banking companies do not want their DNS queries or any such traffic to be sent over the cloud, because the cloud can be inside India or anywhere. This is why they might want the solution to be on-premise to allow them to have full control of the security. [Full Review]

Overview

SOLUTION	Cisco Umbrella	Palo Alto Networks DNS Security
OVERVIEW	Cisco Umbrella offers flexible, cloud-delivered security according to users' requirements Cisco Umbrella includes secure web gateway, firewall, and cloud access security broker (CASB) functionality all delivered from a single cloud security service. Cisco Umbrella's protection is extended to devices, remote users, and distributed locations anywhere. As company employees work from many locations and devices, Cisco Umbrella is the easiest way to effectively protect users everywhere in...	Automatically secure your DNS traffic by using Palo Alto Networks DNS Security service, a cloud-based analytics platform providing your firewall with access to DNS signatures generated using advanced predictive analysis and machine learning, with malicious domain data from a growing threat intelligence sharing community.
SAMPLE CUSTOMERS	Chart Industries, City of Aspen, Eastern Mountain Sports, FLEXcon, George Washington University, Jackson Municipal Airport Authority, Ohio Public Library Information Network, PTC, Richland Community College...	
TOP COMPARISONS	Zscaler Internet Access vs. Cisco Umbrella Compared 27% of the time Infoblox Advanced DNS Protection vs. Cisco Umbrella Compared 12% of the time Microsoft Defender for Cloud Apps vs. Cisco Umbrella Compared 7% of the time	Cisco Umbrella vs. Palo Alto Networks DNS Security Compared 71% of the time Infoblox Advanced DNS Protection vs. Palo Alto Networks DNS Security Compared 17% of the time Infoblox BloxOne Threat Defense vs. Palo Alto Networks DNS Security Compared 5% of the time
TOP INDUSTRIES, BASED ON REVIEWERS*	Consumer Goods Company ... 6% Educational Organization ... 9% Computer Software Company ... 9% Financial Services Firm ... 18%	
TOP INDUSTRIES, BASED ON COMPANIES READING REVIEWS*	Government ... 5% Financial Services Firm ... 7% Comms Service Provider ... 22% Computer Software Company ... 25%	Educational Organization ... 6% Government ... 7% Comms Service Provider ... 16% Computer Software Company ... 22%
COMPANY SIZE, BASED ON REVIEWERS*	201-1000 Employees ... 25% 1001+ Employees ... 34% 1-200 Employees ... 41%	
COMPANY SIZE, BASED ON COMPANIES READING REVIEWS*	1-200 Employees ... 19% 201-1000 Employees ... 16% 1001+ Employees ... 65%	1-200 Employees ... 23% 201-1000 Employees ... 16% 1001+ Employees ... 62%

* Data is based on the aggregate profiles of PeerSpot Users researching this solution.

Cisco Umbrella review by a real user

Works exactly how it's supposed to and gives confidence that when our laptops leave the building, they are protected as if they were behind our firewall

Director Of Information Technology at a financial services firm with 11-50 employees

Dan Brunnquell

WHAT IS OUR PRIMARY USE CASE?

We use Cisco Umbrella to secure our gateway. All of the DNS forwarding coming out of the company from any site or all the DNS requests are forwarded through Cisco Umbrella, and then they determine if that is a safe address and if the content coming back is safe. They will either reject the addressing out of hand, or they'll look at the Layer 7 content and reject that from making it back to us.

We are using the Secure Internet Gateway (SIG) Advantage package. In terms of deployment, effectively, it's deployed from our private cloud. It's in our data closet on our servers.

HOW HAS IT HELPED MY ORGANIZATION?

It enables us to finally allow laptops to be used as workstations and allow data to leave the building. In the past, laptops were only used for VPN access, but they would connect back to their data inside the company. This has allowed us to have a level of confidence that they're protected as if they were behind our firewall. So, now, we've got work-from-home people who literally have their workstations with them.

We have six sites with 60 to 70 users. The baseline configuration allows for additional protection for any DNS requests as they leave those sites, and then the secondary policy is for the mobile devices as they leave the premises. When they're connected to public WiFi, they have an additional policy that kicks in for that time that they're not connected back to the company. So, when they're on public WiFi without a VPN, the tool will actually put that second policy in place that's more aggressive and offers a higher level of protection when it's not sitting behind the firewall. All that is automated. It's all built into the agent.

We don't allow WiFi inside of our network for connection to our actual business network. As soon as a device is docked, it disables WiFi on that mobile device.

Continued from previous page

WHAT IS MOST VALUABLE?

When we have laptops that leave the building, they could connect to public WiFi before they establish a VPN connection back into the company. For that duration or that period of time when they're not docked in the network or on a VPN, they effectively don't have that full layer of security that I provide inside the building. This tool stands in during that period of time, and we extend the security settings through their basic firewall or their cloud-based firewall at that time. So, we do content filtering and control access, but they also are looking at new domains, IP addresses, and bad requests. They're blocking them on my behalf when a laptop is not sitting behind our security appliances.

WHAT NEEDS IMPROVEMENT?

There are a couple of interface issues. I know that they say that there are feature enhancements that are noted. For example, we've got the Cisco Meraki security appliances, and there, we geofence our company to where we're allowed to send and receive traffic. So, in our case, by default, we only allow traffic to six different countries, which allows us to effectively prevent traffic for the majority of bad players in the world, but they don't give you an easy way to do that in Cisco Umbrella. With Cisco Meraki, I can specify or pick the countries. I can say that I want to only allow traffic from these six countries, and I'm done. With Cisco Umbrella, I have to rely on the fact that they're going to prevent traffic to other countries. They're going to decide if it's good or bad. I can't geofence out. I can plot top-level domains, but .com and .net go global. I can certainly block a China (CN) or a Russia (RU) domain, but that doesn't give me the same level of granularity.

Apparently, Cisco Umbrella has got that as a feature request to allow an administrator to say, "I specifically only want traffic to and from these countries. Everything else should be dumped." That way, when they're sitting behind my network or they go out in the wild, they have that same level of traffic being blocked.

FOR HOW LONG HAVE I USED THE SOLUTION?

I have been using it for 14 to 15 years.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

We've had no issues. It has done exactly what it's supposed to do.

Continued from previous page

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

It is cloud-based. So, scalability should not be an issue.

Any increase in its usage is all relative to the growth of our staff. Currently, we deploy the laptops for people who need to work from home or are traveling between the banks. That's roughly about 20% of our total staff. Some people aren't going to be working from home, and some of their jobs can't be done from home. They have no need for mobile devices. If there is a need to work from home, its usage will increase. It is there if we need it to scale, but at this point, it is not scheduled to change.

HOW ARE CUSTOMER SERVICE AND SUPPORT?

Once I became a paying customer, it was much better. The preliminary training is there, but when you get into the nuances and the details of some of its capabilities, you need to talk to tech support. Once you're a paid customer, you get direct access, and then it's good. When I'm able to get a hold of them, their technical support is a 10 out of 10.

HOW WOULD YOU RATE CUSTOMER SERVICE AND SUPPORT?

Positive

WHICH SOLUTION DID I USE PREVIOUSLY AND WHY DID I SWITCH?

I didn't use any similar solution previously.

HOW WAS THE INITIAL SETUP?

I was a hundred percent involved in its deployment. We had a couple of issues. The proof of concept was done without a lot of planning. So, there were some mistakes made along the way. If I was doing it again the second time, I wouldn't make the same mistakes.

The default configurations have your baselines. Those are never supposed to get changed, and I changed and tweaked those for our proof of concept. After a couple of weeks, I had some additional guidance from the Cisco Umbrella team. You leave the baseline configuration, and then you clone and create a new configuration that sits in front of it. So, everyone gets the baseline, and you don't change that. If you want to change it, you make a new policy and then make the changes to that. If you change the baseline default policy and you make a mistake in it, you've to back that all out. If you make it in the new policy, in

the worst case, you just delete it, and automatically everyone goes back to baseline. So, there's still a policy in effect. That was a training issue that should have been resolved. Now that I've done it, if somebody asks me, I would say that this is the way you've got to do it.

WHAT ABOUT THE IMPLEMENTATION TEAM?

It was just me taking care of its deployment. In terms of maintenance, once it's configured, unless you're retweaking and adding or removing something that was blocked, it pretty much runs itself.

WHAT WAS OUR ROI?

I have less maintenance to resolve, fix, and reconfigure VPN clients personally, and the feedback from the end-users is that they're more productive.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

We were using the free version, and we implemented the paid version about two months ago.

I'm paying a fair price, but everything is negotiable with Cisco. One of the benefits that I got by having Cisco Umbrella is the licensing of the Cisco AnyConnect VPN client. There has always been an issue for years and years with Cisco Meraki in terms of VPN clients and using the native built-in Windows client. It keeps reconfiguring itself. By using Cisco AnyConnect as the VPN client, it's not affected by Windows patching or people typing in passwords by mistake. It's more resilient and doesn't change. With just Meraki solution, there was an extra expense for the Cisco AnyConnect VPN client. By having Cisco Umbrella, that licensing is now included.

WHICH OTHER SOLUTIONS DID I EVALUATE?

There were a couple of other options, and I discussed them with another consultant. As a regulated industry, we have to do vendor management, and vendors have to be vetted. So, Cisco was already a vetted vendor. There are other companies that do the same thing, but Cisco didn't require me to do any more vetting. They were already a vendor.

WHAT OTHER ADVICE DO I HAVE?

When it's configured the way it's supposed to work, it turns itself on and off based on the status of the VPN or the dock condition. Once it's configured, it does exactly what it's supposed to do.

If you're doing a proof of concept on it, fully understand how the policies are configured and what the flow is. You should understand the hierarchical status of the policies to configure it right the first time. You don't really want to guess it.

I would rate it a 10 out of 10.

WHICH DEPLOYMENT MODEL ARE YOU USING FOR THIS SOLUTION?

Private Cloud

Palo Alto Networks DNS Security review by a real user

Mature with good scalability and an easy initial setup

Senior Technical Project Manager at a university with 10,001+ employees

reviewer1542159

WHAT IS OUR PRIMARY USE CASE?

We primarily use the solution for security reasons.

WHAT IS MOST VALUABLE?

Palo Alto has a range of products. They have very secure 600 DNS as well as 100 DNS. They have anti-hacking features which are quite useful. They have virus protection within the firewall.They have other products that are geared towards protecting the DNS. All of their product line is highly secure with built-in security. You can protect DNS within the firewall as most of the features are built-in. It's not like a product within the firewall. It's already built-in.

The initial setup is very, very straightforward.

The scalability is good.

The stability is excellent and the product is very mature.

WHAT NEEDS IMPROVEMENT?

Every vendor that sells DNS or firewalls needs to be able to protect against DNS look-up attacks and DNS naming hacks. This is true of Palo Alto as well as others.

The IDS and IPS should be built-in. With EDS and IDS, some are proud to have built-in IDS and IPS intrusion protection and intrusion detection as some vendors sell IDS and IPS separately. They shouldn't be separate. Instead of selling two products, it really should just be one.

Continued from previous page

FOR HOW LONG HAVE I USED THE SOLUTION?

I've been using the solution for about six years at this point. It's been a while.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

The solution is a very mature product. That's what I like about Palo Alto. They said they don't have breaches on their firewall. There are no bugs or glitches. It doesn't crash or freeze. It's great.

WHAT DO I THINK ABOUT THE SCALABILITY OF THE SOLUTION?

Cisco and Palo Alto, right off the bat, are very scalable. That's why I'm studying cloud computing, as, right now, all of the cloud computing platforms have automation and start with automation. We're going away from humans having to configure routers, switches, stories, and firewalls. Everything is done through automation in the stack as well as through virtualization. Maybe in five years, we'll then have so many Cisco routers engineers, NetApp engineers, who would be mostly working through virtualization and the cloud.

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

Palo Alto has a very mature library of documentation. That's what I like about Palo Alto. They don't have so many breaches so, and you're dealing with a good mature product.

You can go and visit the support webpage and check the size of their tech support libraries. If it's huge, then you know you have a product that has, let's say, a lot of incidents, so you maybe want to stay away from it.

WHICH SOLUTION DID I USE PREVIOUSLY AND WHY DID I SWITCH?

I'm in the process of certifying for cloud computing, Amazon cloud computing. I'm focusing not so much on hardware, but on the solutions that Amazon has. We deal primarily with Route 53, which is the Amazon product, which has built-in security features within the configuration of Route 53.

I have experience with Cisco, which is pretty easy to set up.

Sonicwall and Sophos I don't use at all.Checkpoint is not an easy firewall to set up, although is a very good firewall. Checkpoint has also been around for a very long time and it still has instruction sets and comments. It's software-driven, most of the time.

Continued from previous page

HOW WAS THE INITIAL SETUP?

The initial setup is not complex. That's the beauty about Palo Alto. If you set up a firewall, it is very easy and very straightforward. Unlike other vendors, the two firewalls that are easiest to set up are Cisco and Palo Alto. The other vendors are a little bit more work.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

I'm more focused on supporting the product, I don't buy it. I go to the webpage and I see prices, however, I don't pay too much attention to the cost. I'm more interested in the product features and doing the work and the support than actually buying the product.

It's my understanding that they are closely competitive with Cisco, and likely their pricing is on par.

WHAT OTHER ADVICE DO I HAVE?

We are customers and end-users.

I'm not sure which version of the solution we're using.

I'm currently during training with new virtual firewalls.

DNS is a very ancient protocol. The protocol 53 and the UCP and so on, and ARP. We need to review that architecture due to the way we do networking is open to hacking. People can poison the cache, and therefore we need to look at a way of doing away with ARP, doing away with the UCP and having, let's say, the address convert automatically into the IP address and do away with IP version 6. IP version 6 was a total mess. Although the protocol works, it consumes too much overhead and it's too much of a fat protocol. It uses 64 bit, 128 bit, hex addressing at the Mac layer and also at the network layer when using hex.

We need to stick with expanding IP version 4, data in notation. That works at a human level better than working at the network layer. When you use, let's say, IP version 6 it is very difficult to troubleshoot. It's a lot easier to troubleshoot IP version 4, that it's decimal and hex at the network layer. It's a lot easier to identify patterns, easier for the eye to be able to recognize that something is negative or to understand how protocols are working or how routing is working.

Right now, most companies operate with all the DNS. What's surrounding the DNS are the firewalls, intrusion protection and detection, load balancing, fault tolerance et cetera. Other than that, we don't have a secure DNS. That's why we need to reinvent networking. We need to switch to a new method of networking, where we have a truly secure DNS. Without the DNS the internet does not work. That's like having a store open to pirates. DNS is the best thing that has been invented, as far as the internet goes, as that's what allows the browsers to work, that's what allows network solutions to work. Without it we're dead.

I'd rate the solution at an eight out of ten.

Researched Palo Alto Networks But Chose Cisco

Review by a real user:

Tetsuya Suenaga

Manager and Senior Consultant at NTT DATA

WHAT IS OUR PRIMARY USE CASE?

Our customers used an older version of Cisco, but we proposed Cisco Umbrella for their POC phase.

WHAT IS MOST VALUABLE?

The user interface is great. It's very easy to tailor to our client's environment and needs.

WHAT NEEDS IMPROVEMENT?

There should be some programs for the POC phase.

I would like to see more integration between Cisco Umbrella and Cisco DNA center

FOR HOW LONG HAVE I USED THE SOLUTION?

I have been using Cisco Umbrella for one and a half years.

WHAT DO I THINK ABOUT THE STABILITY OF THE SOLUTION?

Cisco Umbrella is very stable.

Continued from previous page

HOW ARE CUSTOMER SERVICE AND TECHNICAL SUPPORT?

The support is very good.

WHAT'S MY EXPERIENCE WITH PRICING, SETUP COST, AND LICENSING?

The price of Cisco Umbrella is a little higher than similar solutions; however, I am not exactly sure what the price difference is.

WHICH OTHER SOLUTIONS DID I EVALUATE?

We compared Cisco Umbrella to other solutions including vScaler and Palo Alto.

Integration is better with Cisco. Cisco Umbrella performed very well compared to vScaler and other solutions.

WHAT OTHER ADVICE DO I HAVE?

On a scale from one to ten, I would give this solution a rating of nine.

WHICH DEPLOYMENT MODEL ARE YOU USING FOR THIS SOLUTION?

Public Cloud

Vendor Directory

Akamai	Akamai Enterprise Threat Protector
Akamai	Akamai SPS Threat Avert
BlueCat	BlueCat DNS Edge
CIRA	CIRA DNS Firewall
CIRA	CIRA Anycast DNS
Cisco	Cisco Umbrella
Comodo	Comodo Dome Secure Internet Gateway
DNSFilter	DNSFilter
EfficientIP	EfficientIP DNS Blast
EfficientIP	EfficientIP DNS Firewall
EfficientIP	EfficientIP DNS Guardian
F5	F5 BIG-IP DNS
Infoblox	Infoblox BloxOne Threat Defense
Infoblox	Infoblox Advanced DNS Protection
Mimecast	Mimecast Web Security
N-able	N-able DNS Filtering
Neustar	Neustar UltraDNS Firewall
NS1	NS1 Domain Security Suite [EOL]
OpenText	Webroot DNS Protection
Palo Alto Networks	Palo Alto Networks DNS Security
TitanHQ	TitanHQ WebTitan
Verizon	Verizon DNS Safeguard

Top Domain Name System (DNS) Security Vendors

Over professionals have used PeerSpot research. Here are the top vendors based on product reviews, ratings, and comparisons. All reviews and ratings are from real users, validated by our triple authentication process.

Chart Key

Views	Comparisons	Reviews	Words/Review	Average Rating
Number of views	Number of times compared to another product	Total number of reviews on PeerSpot	Average words per review on PeerSpot	Average rating based on reviews

Bar length

The total ranking of a product, represented by the bar length, is based on a weighted aggregate score. The score is calculated as follows:

For each ranking factor of **Reviews**, **Views**, and **Comparisons**, the product with the highest count in each ranking factor gets a maximum 18 points. Every other product gets assigned points based on its total in proportion to the #1 product in that ranking factor. For example, if a product has 80% of the number of reviews compared to the product with the most reviews then the product's points for reviews would be 18 * 80% = 14.4.

Both **Rating** and **Words/Review** are awarded on a fixed linear scale. For Rating, the maximum score is 28 points awarded linearly between 6-10 (e.g. 6 or below=0 points; 7.5=10.5 points; 9.0=21 points; 10=28 points). For Words/Review, the maximum score is 18 points awarded linearly between 0-900 words (e.g. 600 words = 12 points; 750 words = 15 points; 900 or more words = 18 points). If a product has fewer than ten reviews, the point contribution for Rating and Words/Review is reduced: 1/3 reduction in points for products with 5-9 reviews, two-thirds reduction for products with fewer than five reviews.

Reviews that are more than 24 months old, as well as those written by resellers, are completely excluded from the ranking algorithm.

All products with 50+ points are designated as a Leader in their category.

1 Cisco Umbrella

45,311 views **36,049** comparisons **35** reviews **536** words/review **8.6** average rating

2 TitanHQ WebTitan

2,303 views **1,351** comparisons **12** reviews **1,198** words/review **9.5** average rating

3 Infoblox BloxOne Threat Defense

2,865 views **1,394** comparisons **8** reviews **1,279** words/review **8.5** average rating

4 Palo Alto Networks DNS Security

3,134 views **2,388** comparisons **3** reviews **793** words/review **9.0** average rating

5 Infoblox Advanced DNS Protection

8,291 views **6,619** comparisons **3** reviews **638** words/review **7.3** average rating

6 Webroot DNS Protection

822 views **600** comparisons **3** reviews **320** words/review **9.3** average rating

7 EfficientIP DNS Guardian

777 views **626** comparisons **1** reviews **865** words/review **8.0** average rating

8 F5 BIG-IP DNS

934 views **653** comparisons **4** reviews **372** words/review **8.3** average rating

9 EfficientIP DNS Firewall

87 views **52** comparisons **1** reviews **478** words/review **8.0** average rating

10 BlueCat DNS Edge

404 views **225** comparisons **1** reviews **479** words/review **6.0** average rating

Top 5 Solutions by Ranking Factor

Views

		VIEWS
1	Cisco Umbrella	45,311
2	Infoblox Advanced DNS Protection	8,291
3	Palo Alto Networks DNS Security	3,134
4	Infoblox BloxOne Threat Defense	2,865
5	TitanHQ WebTitan	2,303

Reviews

		REVIEWS
1	Cisco Umbrella	35
2	TitanHQ WebTitan	12
3	Infoblox BloxOne Threat Defense	8
4	F5 BIG-IP DNS	4
5	Webroot DNS Protection	3

Words / Review

		WORDS / REVIEW
1	Infoblox BloxOne Threat Defense	1,279
2	TitanHQ WebTitan	1,198
3	EfficientIP DNS Guardian	865
4	Palo Alto Networks DNS Security	793
5	Infoblox Advanced DNS Protection	638

About this report

This report is comprised of a list of enterprise level vendors. We have also included several real user reviews posted on peerspot.com. The reviewers of these products have been validated as real users based on their LinkedIn profiles to ensure that they provide reliable opinions and not those of product vendors.

About PeerSpot

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors but what you really want is objective information from other users.

We created PeerSpot to provide technology professionals like you with a community platform to share information about enterprise software, applications, hardware and services.

We commit to offering user-contributed information that is valuable, objective and relevant. We protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

PeerSpot helps tech professionals by providing:

- A list of enterprise level vendors
- A sample of real user reviews from tech professionals
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of vendors and products
- Request or share information about functionality, quality, and pricing
- Contact real users with relevant product experience
- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendors

PeerSpot
244 5th Avenue, Suite R-230 • New York, NY 10001
www.peerspot.com
reports@peerspot.com
+1 646.328.1944