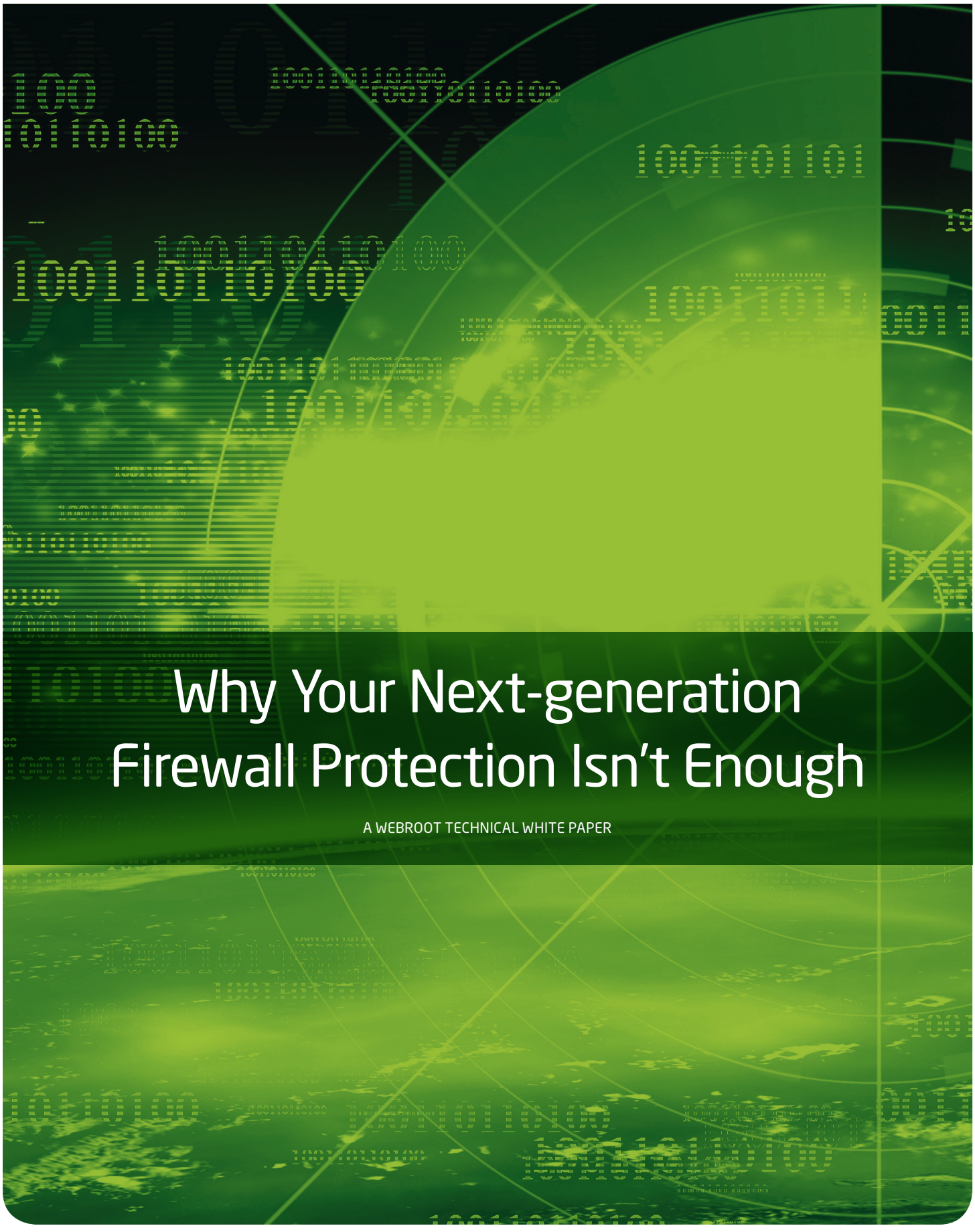
WEBROOT
BrightCloud® Threat Intelligence

WHITE PAPER



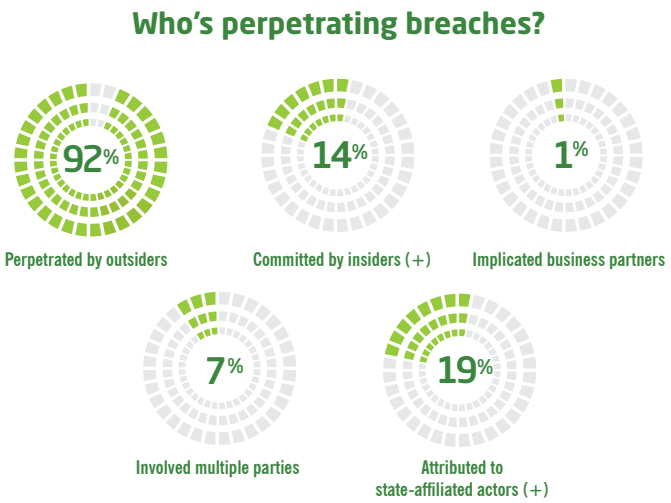
Why Your Next-generation Firewall Protection Isn't Enough

A WEBROOT TECHNICAL WHITE PAPER

CONTENTS

PROBLEM: A TSUNAMI OF EXTERNALCYBER SECURITY THREATS

Enterprise security organizations face a daily onslaught of external attacks. According to a recent survey by IBM X-Force and Verizon's 2014 Data Breach Report, 92% of attacks are being perpetrated by outsiders (Figure 1). Because of this, organizations have to focus on how these attacks successfully penetrate their network perimeter security defenses. Many organizations have invested in next generation firewalls (NGFWs) to protect them from network-based attacks. However, the majority of NGFWs employ static lists of malicious IPs and URLs that are loaded into memory when the device is booted. These lists are often out of date as soon as they are published, resulting in the NGFW not having the ability to protect the organization against the latest threats. Some NGFWs try to compensate for this by incorporating sandboxing mechanisms that are used to evaluate applications and portable executable (PR) files that enter the corporate network through either unknown or newly published IPs and URLs.



Another year, another report dominated by outsiders. Another crop of readers shaking their fists and exclaiming "No – insiders are 80% of all risk!" Perhaps they're right. But our findings consistently show – at least by sheer volume of breaches investigated by or reported to outside parties – that external actors rule.

Pro-insider majoritists may see some justification in the results for all security incidents (rather than just confirmed data breaches), as insiders take the lead in that dataset.

State-affiliated actors tied to China are the biggest mover in 2012. Their efforts to steal IP comprise about one-fifth of all breaches in this dataset.

Figure 1: Who Perpetrates Breaches

It is important to understand that successful attacks have five key characteristics. **The first characteristic is that they typically involve a user.**

- A user **clicks** on something that they shouldn't, such as a phishing email with a malicious URL embedded in it, or surfs to a website that contains malicious content.
- A user **inserts** an unprotected device into their computer, introducing malware from a USB drive, a removable hard drive, CD, DVD, etc.
- A user **installs** an application containing a malicious payload on their computer or mobile device while outside of the organization's network perimeter, resulting in malware infecting the network once that user's device rejoins.

The second characteristic is that these attacks originate from the internet. Malicious applications are downloaded from malicious websites and non-credentialed app stores. Phishing attacks occur from emails that contain bad URLs, such as low popularity IP addresses that deliver malware payloads. Removable devices can be easily host web-based malware that infects the device when used outside the control of enterprise network and endpoint security defenses.

The third characteristic is that attacks have gotten much more sophisticated. The old world of linear growth of long-lived viruses with random targets created by hacktivists for fame and nuisance has given way to a new world of exponential growth of zero-day threats created by organized criminals. Organizations need to better understand threats that emerge from the internet, as well as a better way to predict where the next set of threats will originate.

Every day, the following new threats appear on the internet:

- 25,000 new malicious URLs
- 790,000 new unknown files, many of which are malicious
- 6,000 new phishing sites[1]

The fourth characteristic is that, in the majority of cases, criminals target data that can be monetized. Failing to recognize viruses and malware delivered via the newest internet threats has cost organizations dearly. Between 2004 and 2014, not only did more companies across more verticals get breached, but the breaches themselves have gotten bigger.[2]

But how did these companies get breached? Didn't they all invest in network and endpoint security solutions? Wouldn't those solutions protect the organizations?

[1]Webroot® Intelligence Network
[2]www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

The problem with the vast majority of network and endpoint security solutions is that they operate on the premise of static whitelists and blacklists. These lists do not account for the changing nature of URLs, IPs, files and applications, nor for the volume of unknown threats permeating the web, meaning they cannot be used to provide adequate protection.

Compounding this problem is that commercial network security technology, such as NGFWs and unified threat management systems, can easily flood the organization's network security teams with too many alerts and false positives, making it impossible to understand and respond to new threats. As a result, not only do these threats evade the security technology and land with the victim's infrastructure, but they also have plenty of time to steal sensitive data and inflict damage to the victim's business. The final characteristic of the latest attacks is how quickly they compromise and exfiltrate data from the organization, compared to the average time it takes to detect their presence.

According to the Verizon 2013 Data Breach Investigations Report, 62% of the 221 enterprises surveyed took months to discover they had been breached, even though the data exfiltration took place in just a few hours.

Beyond the fact that unknown malware is, by virtue of its newness, difficult to catch, blacklist-based security faces a variety of challenges addressing unknown internet objects.

» **Short life span** – In the past, when malicious objects existed for months, if not years, the security industry could rely on a kind of sacrificial lamb strategy. Once a virus has attacked one or more systems, threat analysts could research the infection, create a signature or add it to the blacklist, and then publish it to the user community. This typically worked well enough because there was plenty of time after the publish date for the signature or blacklist to catch the malicious object. But these days, malicious objects only exist for a day, sometimes a few hours, rendering the traditional approach all but useless. By the time a new signature is created, the malicious object is no longer in use, and the desired damage is done.

  CONCLUSION: *Enterprises need security solutions that predict in real time the likelihood of a never-before-seen IP, URL, file, or mobile app being malicious, so they can take the appropriate action, i.e. block or allow the object based on level of potential risk.*

» **Multi-vector** – With the increasing prevalence of drive by downloads and other multi-vector attacks that utilize a combination of URLs, IPs, files and mobile apps, enterprises can no longer rely on single-vector threat analysis. For example, an adversary could send a legitimate URL to an unsuspecting recipient and trick him into downloading a malicious file. A URL-only single-vector blacklist would deem that URL safe because it doesn't keep track of its relationship with the malicious IP or file.

  CONCLUSION – *Enterprises need security solutions that correlate the relationships between IPs, URLs, files and mobile apps to predict the likelihood of an object being malicious, and also which other objects are likely to attack in the future.*

» **Dynamic** – Advanced polymorphic threats change all the time. What is benign or trustworthy today may become a threat tomorrow and vice versa. For example, an attacker may use a completely new and benign IP or URL, or even hijack a legitimate website, to deliver malicious payloads and evade detection. Likewise, a company may be able to rescue a previously hijacked site and make it legitimate again.

  CONCLUSION – *Enterprises need security solutions that continually monitor and track changes in the billions of IPs, URLs, files, mobile apps, and their relationships to effectively block malicious objects and recognize the formerly-bad objects that are now safe.*

WHAT THREAT INTELLIGENCE IS AND HOW IT REDUCES ATTACKS

According to a recent threat intelligence report from Gartner Research, "Threat Intelligence is evidenced-based knowledge – including context, mechanisms, indicators and implications, and actionable advice – about an existing or emerging menace or hazard to IT or information assets. It can be used to inform decisions regarding the subject's response to that menace or hazard."[3] In the report, Gartner recommends that CISOs use a commercial threat intelligence service to develop informed tactics for current threats and to plan for threats that may exist in the near future. Gartner states that many vendors provide raw threat information but only a comparative few provide truly anticipatory threat intelligence.

Collective threat intelligence protects enterprises by anticipating malicious unknown URLs, IPs, files, and applications objects. It has the following capabilities:

- Predicts the likelihood that a never-before-seen IP, URL, file, or mobile app is malicious
- Updates risk prediction continuously to account for changes in the rapidly evolving threat landscape
- Predicts which other malicious IPs, URLs, files, or mobile applications are likely to attack in the future
- Customizes the predictive intelligence for each device so it is relevant and actionable

To accomplish these goals, predictive threat intelligence solutions use risk scoring models that provide numerical indicators of the likelihood that a URL, IP, file or application constitutes a current or future threat.

To better understand the role of collective threat intelligence in the face of today's threats, let's look at another popular predictive intelligence in the real world: credit scores. When a consumer wants to obtain a loan for a house purchase, banks look at his credit score together with a number of other factors to determine credit worthiness. The credit score predicts the likelihood of the individual being able to pay back his loan by taking into account the individual's payment history, amount owed, length of credit history, new credit, and types of credit used. Individuals with high credit scores are predicted to be more credit worthy—they usually get loans with a low interest rate. Individuals with low credit scores are predicted to be more likely to default—they don't always get their loans approved or have to settle for high interest rates which banks use to compensate for their higher default risk.

In the cyber world, millions of brand new, never-before-seen IPs, URLs, files, and, mobile apps are created every day. While most are legitimate, many are malicious, and were created with criminal intent. The nature of all these objects is essentially unknown to enterprises just as the risk of default for a loan-seeking consumer is unknown to a bank. Just as banks need credit scores to predict the credit worthiness of the unknown individuals, enterprises need predictive threat intelligence (e.g. a reputation score) to predict the trust worthiness of these unknown objects so they can decide what to do with them (i.e. block or delete objects with a low reputation score and accept objects with high a reputation score).

THE CHALLENGE OF PREDICTING THREATS IN THE VASTNESS OF THE INTERNET

There are over four billion unique IP addresses and URLs on the internet. Applications, specifically those for mobile devices, grow at a rate of over 250,000 new apps per month. Millions of portable executables are available for users to install. To resolve this problem, internet security companies use automated classifiers to scan and detect new threats across the web. Even if an automated classifier categorized one IP per second, it would take over 120 years to score all of the IPs that make up the internet. If a classifier could score one million IPs a day, the process would take over 10 years.

As you add the relationships of IPs and URLs to applications and executables, you geometrically increase the number of calculations needed to determine reputation. Analyzing related URLs or files means you also have to consider all of their data points and their distance from the entity of interest. Automated classifiers also have to scan enough links away for the reputation effect to drop to near zero when determining the association to real threats and not false positives.

Because of the vastness of the internet, continuous real-time scanning of every IP, URL, executable file, and application to predict its good or bad direction is extremely problematic. Even with the largest, most scalable automated classifiers, running in parallel, they simply cannot keep up with all the changing internet data in real time. It is computationally impossible to continually examine every IP, URL, application, and file to determine when something new might appear or something previously legitimate has been compromised. The only solution to overcome these challenges is to apply advanced behavioral recognition and highly accurate risk prediction.

[3]Market Guide for Security Threat Intelligence Services, Gartner Research, October 14, 2014

IMPROVING THE EFFECTIVENESS OF YOUR NGFW THROUGH SANDBOXING AND COLLECTIVE THREAT INTELLIGENCE

Next-generation firewalls have been a valuable security solution for enterprises for several years. However, like all other security solutions, they are now being challenged to handle the massive explosion of unknown threats. While most NGFWs come with some level of protection against malicious IPs, URLs, files, and mobile apps, the reality is that no single vendor can claim to have 100% coverage of all new and unknown threats. Gartner Research recommends that enterprises add threat intelligence to their security arsenal, providing greater depth of defense so that organizations can more effectively identify and block malicious unknown objects and new threats.

Let's consider two alternative approaches, integrating a predictive threat intelligence service into your NGFW, or adding sandboxing technology to the device. It is important to understand that these options are not mutually exclusive.

Option 1 – Adding Sandboxing to Your NGFW

A sandbox is a tightly controlled environment where files and applications can be executed and monitored. Using behavioral analysis techniques, the execution behavior is examined and the file is either determined to be good or bad. Depending on the resulting determination, the file is then released from the sandbox or blocked accordingly. With some vendor solutions, a separate physical or virtual appliance is dedicated to the sandboxing analysis (Figure 2).

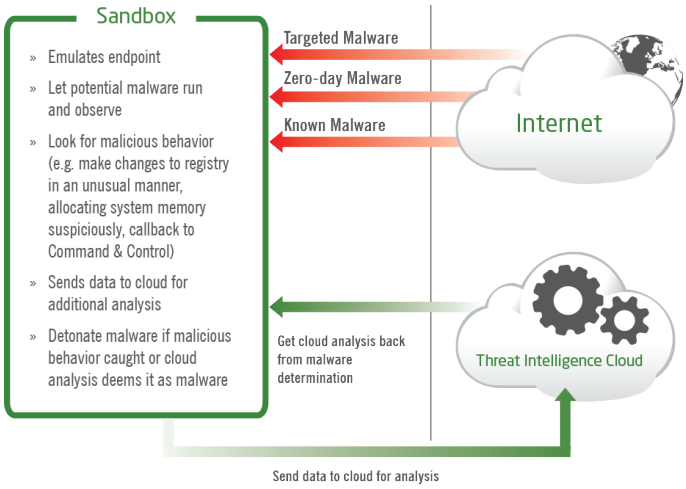


Figure 2: Sandboxing and monitoring technology

As new files come through your NGFW, they are identified and submitted for sandbox analysis. Sandboxing doesn't rely on any prior knowledge of the application or executable and doesn't use signatures. The determinations are made based on the actual behavioral execution, such as renaming, allocating system memory in an unusual way, or writing inappropriately to the system registry. Because sandboxing uses actual execution behavior, it has relatively low false positives.

The Limitations of This Approach

Sandboxing can miss a lot of different things. It assumes that you can control all program and executable files being introduced into your organization by routing them through a sandbox appliance or engine for evaluation purposes. Unfortunately, many users operate on mobile devices and install applications on them completely outside of the control of the network perimeter. In addition, peer-to-peer communication protocols (such as Skype, BitTorrent, and others) are transparent to firewall appliances and can escape detection. And new protocols such as IPv6 use encrypted tunneling that go directly through your NGFW without any analysis because the data stream is encrypted.

Sandboxing is also resource intensive. Every sandbox needs to reflect a given combination of OS, patch level, installed apps, and browsers. Beyond that, each exploit takes time to run – which can be from a few seconds to several minutes. And with polymorphic malware that lies dormant for an extended period of time, the initial sandbox analysis may mark the item as good because no bad behavior is determined during the sandboxing time period. Only days or weeks later does the file execute malicious behavior.

Option 2 – Adding Collective Threat Intelligence to your NGFW

Collective threat intelligence is delivered to next generation firewalls via a direct ingest, either as an automated list service continuously sending updates to the device, or through a direct API call from the NGFW to a threat intelligence service. BrightCloud Threat Intelligence Services provide continuously updated risk scores for IPs, files, websites, URLs, mobile applications and more.

IP addresses have many different characteristics. Age and popularity are two main ones to consider. The longer lived a site is and the more popular it is, the higher the reputation score. However, those two characteristics alone do not tell the entire story. Many long lived sites with high popularity are targeted by malware writers and malicious websites.

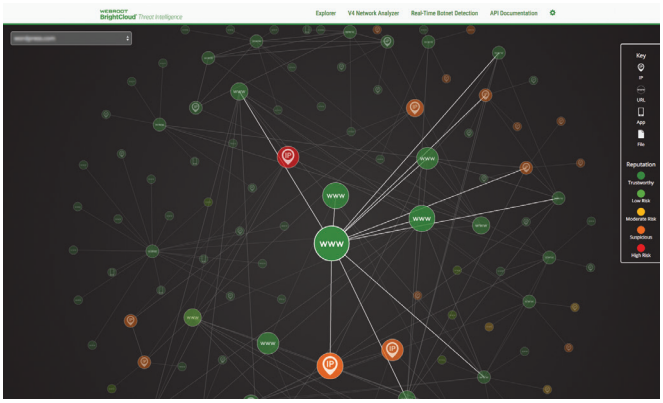
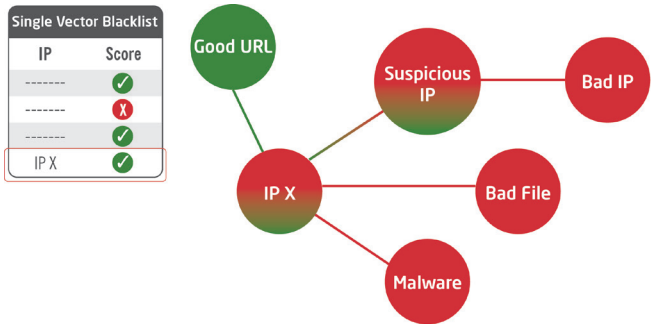


Figure 3: The BrightCloud Threat Intelligence Services User Interface shows all the URLs, IPs, files and mobile apps related to a website

If we were only using an NGFW with only a single vector blacklist, you could see how the relationship or link association with known bad sites could be missed, with the potential for a resultant attack.



- *Single vector blacklist misses relationships between objects and assumes IP X is benign*
- *BrightCloud Threat Intelligence Platform keeps track of relationships between URL, IP, file and mobile app*
- *BrightCloud Threat Intelligence Platform deems IP X malicious and assigns it a low reputation score due to its affiliation with malicious items*
- *Customer obtains the score from BrightCloud IP Reputation Service and blocks IP X accordingly*

Figure 4: Contextual database uses relationships between internet objects to predict if an unknown is malicious.

If we were only using a NGFW with only a single vector blacklist, you could see how the relationship or link association with known bad sites could be missed, with the potential for a resultant attack.

A good IP, linked to a number of malicious files, may be part of a multi-vector attack (e.g. if the customer accepts traffic from that IP, that IP may trick the customer into downloading malicious files). Collective threat intelligence will correctly assign a low reputation score and predict it as a malicious IP and customers can block it at the NGFW level.

If a malicious IP has attacked an enterprise before, there is a good probability that the same criminal organization owns the other IPs, URLs, files, or mobile apps affiliated with that malicious IP and would use those to attack that enterprise in the future. BrightCloud Threat Intelligence Services can provide all those affiliated malicious items to the NGFW so that it can block these likely future attackers.

In order to effectively catch unknown threats, a threat intelligence service should have the following capabilities, which are far beyond traditional list-based threat data:

» **Contextual Relationships Between IPs, URLs, Files & Mobile Apps** – Core to the internet is the interlinking of all the different entities. This makes the web incredibly useful for legitimate businesses, but also dangerously easy for criminals to exploit. Effective predictive threat intelligence services need to track the relationships between IPs, URLs, files, and mobile apps to correctly predict whether a never-before-seen item is malicious. For example, a bad IP has a bad reputation influence on other IPs to which it is directly linked. A bad IP linked indirectly, i.e., through another IP or URL, has a less bad reputation influence. A state-of-the-art predictive threat intelligence service needs to trace enough connections for the reputation influencing effect to drop to near zero, however far that may be, in order to have a comprehensive reputation picture of given internet item. It also needs to do perform this thorough analysis for each of the billions of IPs, URLs, files, and mobile apps across the internet. That relationship tracking can also help predict where future attackers may come from. As an example, if a malicious IP launched an attack, future attacks may come from other IPs, URLs, files, or mobile apps related to this IP, since the criminal responsible may control these as well.

» **Comprehensive Coverage Across Multiple Segments: Consumer, SMB & Enterprise** – Trends such as Bring Your Own Device (BYOD) and Internet of Things will continue to blur the line between consumers, SMBs, and enterprises, giving criminals a brand new attack surface. They could start by attacking an unsuspecting individual using public Wi-Fi in a coffee shop, and subsequently use that device as the gateway to launch more targeted attacks at the enterprise which employs that individual. A comprehensive collective threat intelligence service needs data across all segments – consumer, SMB, and enterprise – to predict which unknown threats may bridge them.

» **Real Endpoint Data** – Threat intelligence services that solely rely on data from crawlers, network monitors, passive sensors, honeypots and other simulation techniques, such as sandboxing, are missing a very important data source: real endpoints (clients or servers). While cybercriminals can find ways to evade detection (e.g. advanced malware can detect the presence of a virtual machine sandbox and suppress malicious behavior to avoid detection), all threats will eventually exhibit their malicious behavior on real endpoints where the targeted assets,

such as a credit card PIN, reside. Accurate threat intelligence correlates data from real endpoints with that from crawlers, and other sources to improve accuracy in identifying unknown threats.

» **Big Data Volume & Velocity** – Accurate prediction is built on statistics. Statistical systems need big data volume to build prediction models, as well as big data velocity to refine them. As an example, there are approximately 4.3 billion IPs in the world. A comprehensive predictive threat intelligence service not only collects data on all 4.3 billion IPs from multiple data sources across multiple segments to train the statistical model but it also needs to continuously monitor changes and feed them into the statistical model so it can update its reputation score on each of these ever-changing IPs.

» **Across Many Network Topologies** – Users only operate part time in traditional fixed corporate network devices. As users are more mobile, the networks they operate on are increasingly less trusted and have more open security models. This subjects the user and their device to a much greater possibility of an attack.

» **Computational Scale and Machine Learning** – Gone are the days when security companies could rely solely on human threat research analysts to analyze and combat threats. To deal with the billions of data points collected on a daily basis and analyze the complex relationships between them, the only conceivable solution is real-time, automated machine learning. In order to scale efficiently and meet growing demand in the war against unknown threats, a predictive threat intelligence service should run in the cloud to take advantage of its elastic supply of computing power, network, and storage.

» **Experience & Threat History** – A best-in-class threat intelligence service cannot be built overnight. It takes time to architect the engine, gather enough data points to build the statistical model, and collect data on a regular basis to finely tune the model and improve the accuracy of its predictions.

The Limitations of This Approach

The biggest limitation in delivering collective threat intelligence to a NGFW is that many of the devices are limited in the amount of data they can consume due to system memory, disk space, and CPU limitations. They also may have a limit on how frequently they can poll new data (e.g. hourly, daily, etc). It is important that you understand the limitations of your device when considering whether or not to integrate an external predictive threat intelligence service into your NGFW.

Webroot BrightCloud® Threat Intelligence Services overcome any limitations of NGFWs by leveraging the IP addresses found in the NGFW Syslog to create a customized list of IPs and IP reputation scores for only the IPs that have been observed being accessed through the network users associated with each NGFW. Each NGFW receives customized IP reputation scores based on the actual IPs its users are accessing, tailoring the analysis to what's relevant to the organization as opposed to the entire internet.

WEBROOT BRIGHTCLOUD® COLLECTIVE THREAT INTELLIGENCE

Leading network security technology vendors such as Cisco, F5 Networks, Palo Alto Networks, and others have already added Webroot BrightCloud® Threat Intelligence Services directly into their products, providing an additional layer of defense:

» F5 integrates BrightCloud® IP Reputation Service into their network devices to block malicious IPs from penetrating their customers' networks.

» Palo Alto Networks integrates the BrightCloud® Web Classification Service into their NGFW products to prevent their customers' users from accessing malicious or inappropriate websites.

BrightCloud® Threat Intelligence Services are powered by the BrightCloud Threat Intelligence Platform, an advanced cloud-based security platform. The BrightCloud Threat Intelligence Platform continuously collects data on billions of URLs, IPs, files, and mobile apps from internet sensor networks, global threat databases, and the millions of consumer, SMB, and enterprise endpoints protected by Webroot and its technology partners. It uses big data technology, such as Cassandra database management, third generation machine learning (Maximum Entropy Discrimination), and a massive number of classifiers (400 IP classifiers that can classify 20,000 IPs per second) running in parallel on Amazon Web Services to analyze all these data points to determine the reputation and classification of billions of internet objects.

BrightCloud Threat Intelligence Services provide continuously updated numerical risk scores, similar to a FICO score, that supply predictive threat indicators of the known and potential risks that will occur with any IP, URL, application, or executable file. The BrightCloud Threat Intelligence Platform evaluates the popularity, reputation, whois, geographic location, URLs hosted on to IPs and vice versa, IPs that are close numerically and in function and ownership, and many other factors in making BrightCloud reputation scores. For known bad targets, it continuously examines some targets so that threat indicator scores are as up-to-date as possible because bad actor IPs continuously attempt to link to known good IPs and URLs through link association.

BrightCloud Threat Intelligence Services gather significantly more data points per reputation entity (URL, IP, or file) and uses third generation maximum entropy discrimination techniques to provide much more accurate prediction of new and emerging threats. Rather than relying solely on human threat researchers, BrightCloud Threat Intelligence

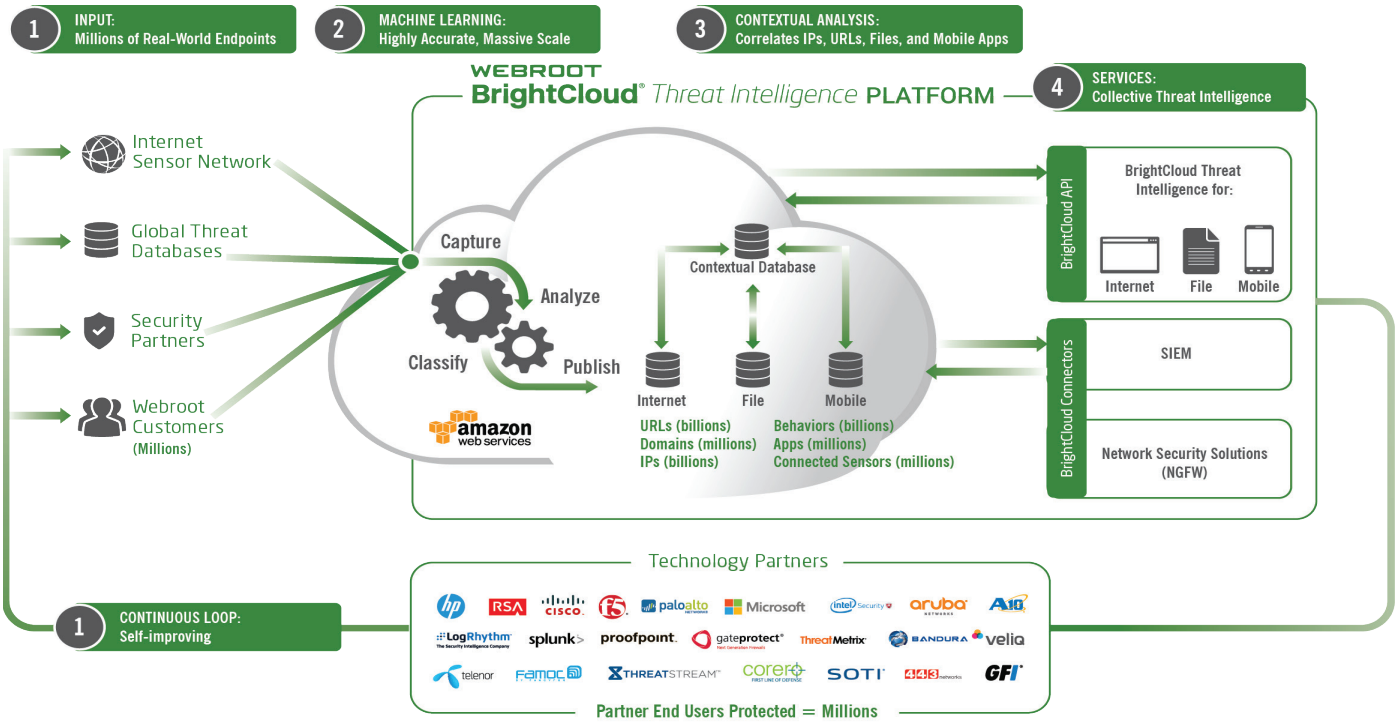


Figure 5: BrightCloud Threat Intelligence Platform

Services use the machine learning of the BrightCloud Threat Intelligence Platform, which trains the scoring algorithms to provide better and more accurate predictions. This requires labeled data, such as good and bad IPs, to train the models.

BrightCloud Threat Intelligence Services employ over 400 different automated classifiers from the BrightCloud Threat Intelligence Platform that run in parallel or in separate workloads. Each classifier performs over 20,000 automated classifications per second, and just one of these automated classifiers can scan over 4B IPs in two and a half days. Using hundreds of classifiers working in parallel, BrightCloud Threat Intelligence Services can collect and score many more data points, and continuously update the new linkages between IPs, URLs, apps, and executable files in near real-time.

The BrightCloud Threat Intelligence Platform collects data from millions of Webroot, and our partner users connecting via endpoints in the wild to determine new threats that manifest from users behavior. BrightCloud services bring visibility into real internet traffic and attacks that is highly relevant. Rather than using simulations, data is gathered from real endpoints. Tapping into this real-time sensor network of customers and sending back that flood of information to the BrightCloud Threat Intelligence Platform for analysis provides significantly greater real world threat data from endpoints than competitor solutions that do not incorporate sensors.

BrightCloud Threat Intelligence Services reveal threats to your NGFW via a number of offerings:

- **IP Reputation Service** – predicts the likelihood of an IP being malicious
- **Web Reputation Service** – predicts the likelihood of an URL being malicious
- **Web Classification Service** – categorizes URL (e.g. business, adult content, gambling)
- **File Reputation Service** – predicts the likelihood of a file being malicious

BRIGHTCLOUD® IP REPUTATION SERVICE SCORES

TheBrightCloud Threat Intelligence Platform monitors all 4.3 billion IP addresses, as well as their affiliated URLs, IPs, files, and mobile apps on a daily basis. It has identified 900 million IPs that have had at least one security infraction at some point, which is over 20% of the total IPs used in the world. The Webroot BrightCloud® IP Reputation Service pays closer attention to this group and collects more data more frequently on these. Out of that 900 million IPs, approximately 12 million have been identified as malicious due to their involvement in security infractions or their affiliated IPs, URLs, files, or mobile apps' involvement. These 12 million malicious IPs fall into the following categories:

- Botnets
- Web Attacks
- Anonymous Proxies
- Scanners
- Windows Exploits
- Phishing
- Spam Sources

The BrightCloud Threat Intelligence Platform assigns each of the 4.3 billion IPs an IP Reputation Score, which predicts the likelihood of it being malicious. This score is updated every five minutes and is delivered via the BrightCloud® IP Reputation Service.

IP Rep	Category	Description	Number of IPs
1-20	High Risk IPs	There is a high risk that these IPs will deliver attacks to your infrastructure and endpoints in one of the following categories: botnets, Windows exploits, web attacks, phishing, anonymous proxies, spam sources, and scanners.	~12 million
21-40	Suspicious IPs	There is a higher than average risk that these IPs will deliver attacks to your infrastructure and endpoints.	
41-60	Benign IPs	These IPs have exhibited some potential risk characteristics. There is some risk that they will deliver attacks to your infrastructure and endpoints.	~882 million
61-80	Low Risk IPs	These IPs rarely exhibit characteristics that expose your infrastructure and endpoints to security risks. There is a low risk of attack.	
81-100	Trustworthy IPs	These are clean IPs that have not been tied to any security risk. There is very low risk that your infrastructure and endpoints will be exposed to attack.	~3.4 billion

The BrightCloud IP Reputation Service exposes this data to NGFWs through a file list updater service that is used to improve the threat intelligence of the NGFW as well as through an API (for more direct integrations with NGFW vendors). Capabilities include:

- **Lookup service** – submit an IP and get an answer on whether the IP is malicious (score <= 40)
- **Download service** – download all 12 million malicious IPs
- **Update service** – get updated on the malicious IP list

The Webroot BrightCloud® IP Reputation Service employs an innovative prosecution methodology to determine if an IP is malicious:

- Uses over 400 automated classifiers that can scan at a rate of 20,000 per second, per classifier, to score the billions of IPs' activities and their tens of millions affiliated IPs, URLs, files, and apps in the cloud
- Applies third generation machine learning algorithms to score the results
- Correlates all the data in a contextual database that can be used to understand visual associations
- Judges and sentences the IP as a risky item (Reputation Score <= 40) for a term if it or its affiliated URLs, IPs, files, or mobile apps have exhibited enough malicious behavior
- Re-evaluates the IP after serving a time-based sentence
- Re-sentences or releases IP on parole with heavy monitoring

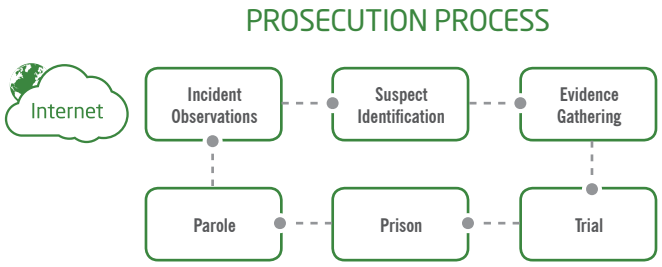


Figure 6: Prosecution methodology keeps IP Reputation Score up to date.

- If an IP was previously deemed Benign or Low Risk (41 - 80 Reputation Score) but has not exhibited any malicious behavior (including its affiliated IPs, URLs, files & mobile apps) for a significant amount of time, BrightCloud will start improving its IP Reputation score. The process will continue over time and may eventually move the IP Reputation Score above 80, categorizing it as Trustworthy.
- If an IP was previously deemed Trustworthy but has started exhibiting malicious behavior (including its affiliated IPs, URLs, files & mobile apps), the BrightCloud IP Reputation Service will start lowering its IP Reputation score. If this continues, the IP may drop into the risky category (Reputation Score <= 40).

BRIGHTCLOUD® IP REPUTATION SERVICE FOR PALO ALTO NETWORKS

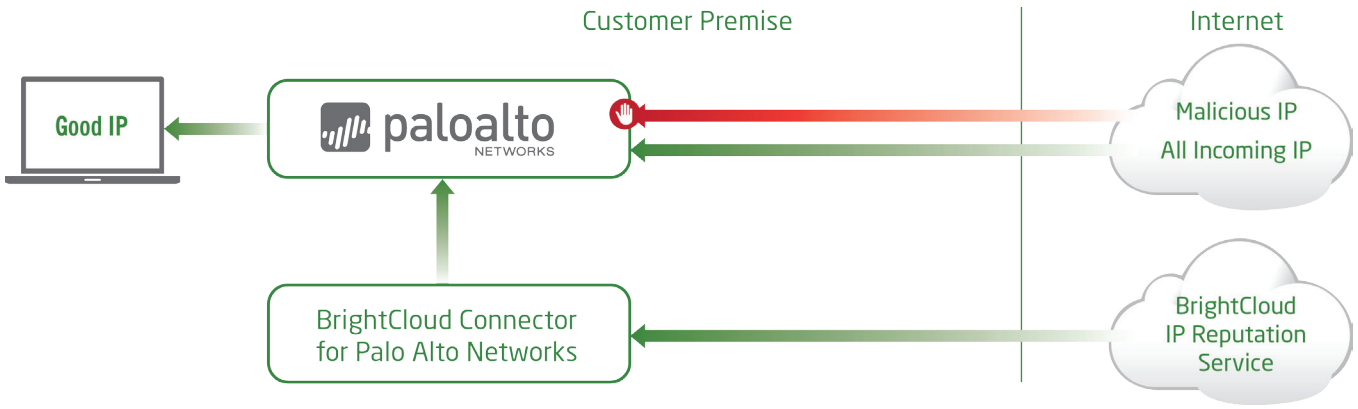


Figure 7: BrightCloud IP Reputation Service for Palo Alto Networks

Palo Alto Networks (PANW) is a leading provider of NGFWs that help customers control application traffic and protect their networks. Since 2008, PANW has licensed and integrated BrightCloud® Threat Intelligence into all its NGFWs so PANW customers can control what categories of URLs their users can access and which are blocked (e.g. gambling, social, adult entertainment).

In recognition of the need to improve the capabilities of the PANW NGFW, Webroot has developed and now offers direct to customers BrightCloud IP Reputation Service for PANW NGFW devices. Unique to the industry, the service includes a customized list of IPs that represent the highest potential risk to each customer through analysis of each PANW NGFW SysLog, providing customized threat intelligence that is unique to risks your organization and users actually encounter.

How the IP Reputation Service Works

- The customer configures the BrightCloud connector (virtual appliance) to regularly download the most up-to-date IP information from BrightCloud IP Reputation Service.
- For each PANW NGFW device, the customer configures it to point to the BrightCloud connector to obtain the device-specific block list of malicious IPs. The device-specific customized list is created automatically by the BrightCloud connector using its innovative Threat Intelligence Customization feature.
- Once the PANW device gets the device-specific block list, it starts comparing all incoming IPs and blocking all those that appear in the list. This is how a PANW customer can use the BrightCloud IP Reputation Service to protect each individual PANW device from malicious IPs.

Threat Intelligence Customization

Unlike other generic threat intelligence services, the BrightCloud IP Reputation Service is customized for each PANW NGFW device for each customer, so it is 100% relevant to the customer's needs and always actionable.

- After the customer points a specific PANW device to the BrightCloud connector for the device-specific block list, the customer would configure the BrightCloud connector to retrieve the Syslog of all incoming IPs for that specific PANW device in the last 24 hours.
- The BrightCloud connector maps the list of IPs in that Syslog to its malicious IP database downloaded from the BrightCloud IP Reputation Service. Any IPs that appear in both the Syslog and the malicious IP database will be added to the device-specific block list, so that any malicious IPs that attacked the device in the past will be blocked in the future.

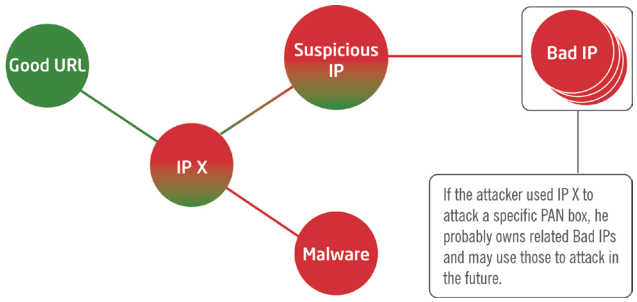


Figure 8: Prediction of likely future attackers

- The BrightCloud connector will also get a list of other malicious IPs that are affiliated with the malicious IPs already in the device-specific block list. The rationale is that criminals might use other affiliated IPs to attack that device in the future.
- Once the device-specific block list is complete, the customer can review the different categories of IP threats, such as botnets or spam, in the list and decide which ones to keep or drop. Once this process is complete, the customer can configure how often this threat intelligence customization feature runs automatically to keep the device-specific block list up to date.
- Each PANW NGFW device would retrieve the most up to date device-specific block list from BrightCloud connector and start blocking malicious incoming IPs that appear in the list.

Customized IP block list for **each** PANW box in your environment	Relevant and actionable IP threat intelligence for **each individual** PANW box so it can block attacks **targeted** at a specific geo, country, city, office, network segment or the box itself
IP reputation score based on **collective threat intelligence** across multiple vectors (URL, IP, File)	**Accurate** identification of past-attacker and **predictive** identification of likely future attacker IPs
Proven threat intelligence platform integrated by technology partners like Palo Alto Networks, Cisco/SourceFire, RSA, etc	**Trusted** and actionable threat intelligence that expands your IP protection beyond Palo Alto Networks' coverage

SUMMARY

Malicious unknown IPs, URLs, applications, and executable files have created substantial threats to organizations. Detecting and thwarting attacks before they ex-filtrate data is imperative and requires a much greater level of real-time situational awareness and actionable threat intelligence. Failure to do so can result in significant monetary losses, erosion of customer confidence, and damage to your brand.

Threats have changed. Signature-based detection and out-of-date threat lists are no longer effective. Threat data changes significantly on a day to day basis, with more than 25,000 new malicious URLs and 1,000 phishing websites emerging daily. Users work differently today, traversing different locations and networks, often on personally owned devices. The attack vectors have changed from a user on a PC within the network to any user on any device, operating inside and outside of the organization. To combat these threats, you need real-time collective threat intelligence that can be easily integrated into your NGFW to protect at the network layer or on the endpoint itself.

The massive increase in data losses and breaches proves that traditional security has failed to protect your network and users at the moment of truth, when they encounter a new or unknown threat in the wild. Additionally, the time to detect these breaches is measured in months, while it only takes hours for threats to compromise and exfiltrate sensitive information.

Webroot is the market leader in providing the most innovative endpoint protection and real-time threat intelligence solutions in the industry. Over 7.6 million consumers and 1.9 million business users use our internet security solutions to keep them safe. Industry leaders, including HP, F5, Cisco, RSA, Palo Alto Networks, and many others include our BrightCloud® Threat Intelligence Services as a core component of their product offerings to protect their customers.

The core of Webroot technology, the BrightCloud Threat Intelligence Platform, scans the vastness of the internet using hundreds of automated classifiers and uses machine learning that can automatically classify and correlate the interrelationships of URLs, IPs, applications, and files to provide true collective threat intelligence in a timely fashion via BrightCloud Threat Intelligence Services. Unique in the industry, BrightCloud Threat Intelligence Services offer real-time situational awareness through customizable device block lists and accurate risk prediction data to identify the real threats that your organization and users are encountering.

Threats are getting smarter. It's time your NGFW got smarter, too. Integrate BrightCloud Threat Intelligence with your NGFW and outsmart the threats.

About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900