DenyAll enhances Web Application Firewalls with IP Reputation Service powered by Webroot

The next generation application security vendor announces DenyAll IP Reputation Service, an add-on to its Web Application Firewalls (WAF), based on the Webroot® Threat Intelligence Platform. Subscribers will be able to feed their WAF's filtering engine with up-to-date and actionable threat intelligence in order to implement smart response strategies.

DenyAll is taking advantage of FIC, the annual Cybersecurity Forum opening today in Lille, France, to announce a new offering: **DenyAll IP Reputation Service** is an optional add-on subscription for its Web Application Firewalls. It enables administrators to filter incoming requests based on up-to-date threat intelligence on IP addresses known to be used by attackers. With this information, the DenyAll products can help determine the appropriate response in scenarios where additional contextual information helps make better security decisions.

Enhancing application security effectiveness with IP Reputation scoring

Protecting Web applications and services from attacks can be done using a variety of methods. IP addresses have been used traditionally to prevent connections from certain geolocations. Smart attackers however use different IP addresses to evade such basic controls. Hence the need to consider the reputation of an IP address over time. The DenyAll IP Reputation Service combines information about the category of threats an IP address has been associated with (botnets, scanners, DDoS, anonymous proxies, spammers, malware), together with a reputation score, providing additional color about the level of trust security administrators can have in that source IP.

"*The reputation of IP addresses is a valuable source of information for making security decisions*", says Stéphane de Saint Albin, DenyAll Chief Marketing Officer. "*DenyAll WAFs can correlate that data with various sources and help administrators create even smarter responses to potential threats,*" said the DenyAll spokesperson.

The key benefits associated with the new add-on service are performance optimization and false positive reduction, because the WAFs can be setup not to filter requests coming from IP addresses with a low reputation score, or to do so using a less stringent policy if the source is indeed considered trustworthy. But the intelligence feed can also enable more adaptive response scenarios, such as triggering a stronger authentication process when an otherwise trusted user connects from an unusual address with a questionable reputation, for example.

Powered by Webroot

As the result of an agreement signed by DenyAll and Webroot, the market leader in next-generation endpoint protection and cloud-based collective threat intelligence, the new DenyAll service will be powered by the Webroot® Threat Intelligence Platform to detect and block malicious incoming IPs. The Webroot BrightCloud® IP Reputation Service correlates IP reputation data with URL, file, and mobile application data to determine relationships between object types while providing a predictive risk score for each IP. BrightCloud continuously monitors and maintains a database of over four billion IP addresses from which a dynamic list of approximately 12 million malicious IPs is updated and made available to DenyAll customers in near real-time.

A new data source for User Reputation Scoring

DenyAll IP Reputation Service is a natural addition to DenyAll's Next Generation Application Security portfolio. It represents a new and reliable source of data for DenyAll's ground-breaking User Reputation Scoring engine. This next generation technology takes several contextual data sources

into consideration, such as user behavior, security events, geolocation and IP reputation to block bad bots and evaluate the intent of human users, with the goal of blocking actual offenders without preventing access for legitimate users of the applications. The new service will be sold as an optional annual subscription via the company's usual channels.

About DenyAll
DenyAll is a software vendor and an expert in application security. Building on 15 years of experience securing web applications and services, the company keeps on innovating to meet the needs of organizations of all sizes, worldwide. Its products **detect** IT vulnerabilities, **protect** infrastructures against modern attacks targeting the application layer, and **connect** users to the applications that allow them to create and share information. The company leverages an ecosystem of value-added resellers, outsourcers, hosters, and cloud providers. A member of the Hexatrust alliance, DenyAll partners with other vendors to deliver innovative, integrated solutions. Look for more information on www.denyall.com.

About Webroot
Webroot delivers next-generation endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions and BrightCloud® Threat Intelligence Services protect tens of millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Palo Alto Networks, A10 Networks, Aruba Networks, and more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at www.webroot.com.

Social Media: Twitter | LinkedIn | YouTube | Facebook

Press contacts:		
Oxygen	**Kafka Kommunikation**	**DenyAll**
Laure Mazzesi	Ursula Kafka	Stéphane de Saint Albin
Tél. : +33 1 41 11 37 77	+49 89 747470-580	Tél. : +33 1 46 20 96 21
laurem@oxygen-rp.com	info@kafka-kommunikation.de	sdesaintalbin@denyall.com
www.oxygen-rp.fr		www.denyall.com