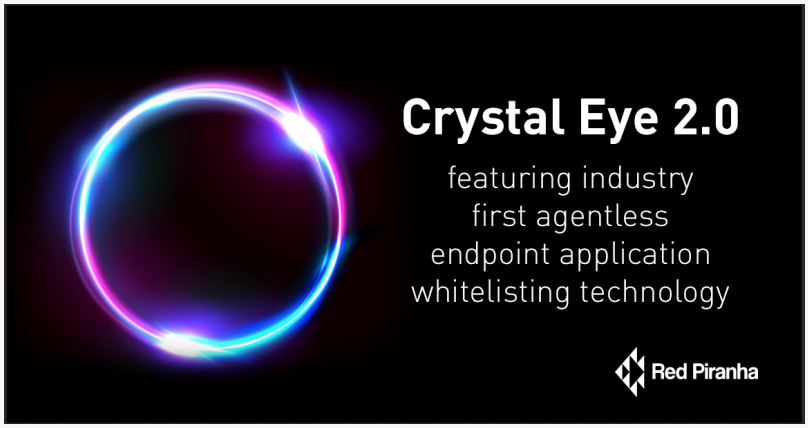
Red Piranha Announces Industry First, Agentless, Application Whitelisting Technology

Red Piranha has announced the information security industry's FIRST ever agentless endpoint Application Whitelisting (AWL) technology.



CANBERRA, WA, AUSTRALIA, March 15, 2019 /EINPresswire.com/ -- Red Piranha has today announced the information security industry's FIRST ever agentless endpoint Application Whitelisting (AWL) technology.

Red Piranha, developer of Australia's first next-generation firewall, Crystal Eye, has released its latest technology in their already cutting edge, feature-packed Crystal Eye, Unified Threat Management (UTM) platform.

The company announced the gateway-controlled device Application Whitelisting (AWL) technology at its product launch in Canberra, Australia, to guests from both industry and government sectors.

This purpose-built technology, developed by Red Piranha, is explicitly designed to undertake endpoint AWL managed from a network gateway appliance at scale. This addition to Crystal Eye not only streamlines an otherwise complex process but also simplifies the implementation on large or complex networks with scanning managed from one source remotely.
Crystal Eye's Patent AWL technology allows the gateway appliance to control applications running on endpoint devices without the need to install and manage endpoint device agents as well as allowing protection on BYOD, IOT and SCADA devices.

This purpose-built technology, developed by Red Piranha, is explicitly designed to undertake AwL on network gateway devices at scale. This addition to Crystal Eye not only streamlines an otherwise complex process but also simplifies the implementation and scanning on large or complex networks with scanning managed from one source.

Crystal Eye 2.0 makes generating, implementing and maintaining device application whitelists significantly faster, meaning organisations are able to be protected and meet, and often exceed, compliance requirements sooner.

With this new Crystal Eye technology, organisations can deploy and manage the whitelisting "AWL" process from the gateway UTM without the need for agents or needing to have physical access to devices, significantly reducing the burden on IT teams to deploy this critical security control. Remote IT, and security teams can deploy and manage the endpoint application control process remotely and within minutes across large networks with multiple endpoints.

"It seems that the extended security community has come to a consensus that AWL is one of the

most important security technologies/techniques an organization can and should implement"
-U.S. Department of Homeland Security, Application Whitelisting Readiness Questionnaire

While no single mitigation strategy is guaranteed to prevent an incident, the Australian Signals Directorate (ASD) recommends businesses implement eight essential mitigation strategies as a baseline. These strategies, known as the 'Essential Eight', make it significantly harder for systems to be compromised with AWL being number one on the list.

Unlike traditional signature-based file blocking (commonly known as 'blacklisting') such as antivirus programs, Crystal Eye AWL only allows programs it has been instructed to trust, to run on the network. If the software is not on the whitelist, it will be prevented from running, regardless of whether a file is known as good, bad or indifferent. This feature proactively prevents malicious code from running on a network, before any damage occurs.

Until now, AWL has been difficult to deploy and maintain within an organisation because it required implementation on every device rather than at the gateway.

Crystal Eye AWL has been developed from the ground up by security professionals to solve real-world problems faced with application whitelisting. The AWL technology also tracks software encrypted network communications making it the world leader in dealing with encrypted unknown malware threats and new emerging threats.

Shannon Fleming
Red Piranha
+61 8 6365 0450
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
