

Premium Desktop & Security Solutions Overview









Tighter Security. Lower Risk. Better Peace of Mind.

Sophisticated Security at a lower cost

Sedona Security with CROPS Premium enables dealers to deliver a complete, end-to-end cyber security solution without having to build and maintain in-house operations. The solution combines powerful software with a suite of SOC services to deliver both foundational security and highly advanced protections for John Deere Dealers—including endpoint management, SIEM, dark web monitoring, real time security auditing, advanced threat intelligence and the capabilities and reporting required to ensure compliance in Ag, Construction, and mixed dealer environments.

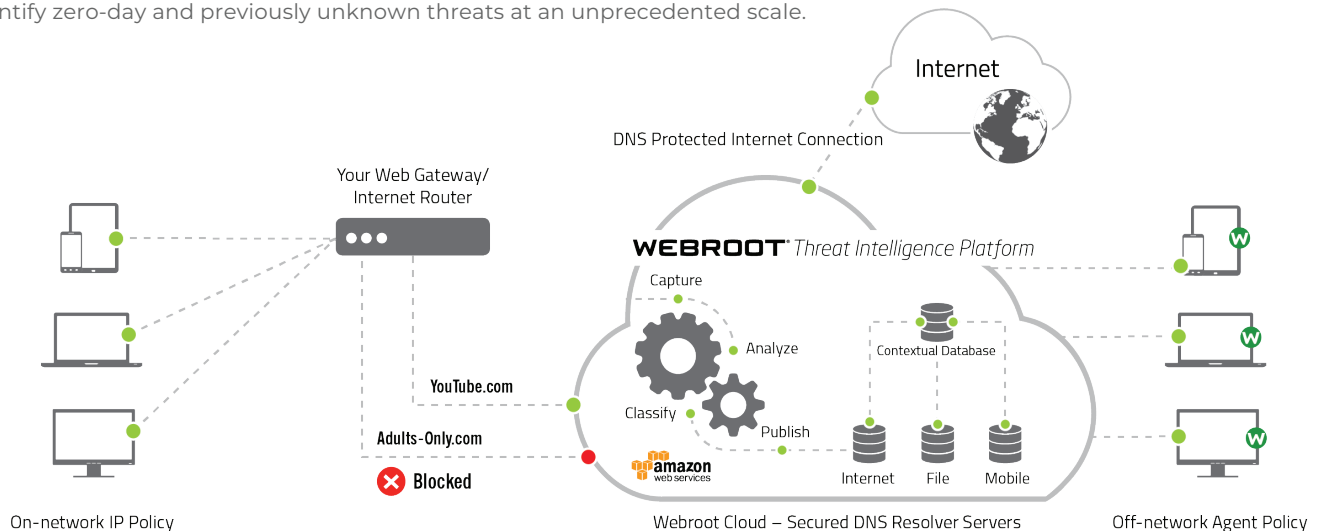


CROPS Premium adds 8 additional security layers to your Endpoints:

Security Awareness	DNS Protection	Detection & Response	Risk Score Profiles
 <p>Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and pre-built "done for you" security policies for dealerships.</p>	 <p>Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the Internet, and blocks them on your network within seconds – before they reach the user.</p>	 <p>Protect your computers data from malware, viruses, and cyber attacks with advanced security. Today's latest technology protects against file-less and script based threats and can even rollback a ransomware attack.</p>	 <p>Pre-built and customizable profiles that tell you exactly what's needed to protect against certain threat types. These recipes identify specific gaps in protection on each device helping you identify vulnerabilities and take corrective action.</p>
CO-Managed SOC	Dark Web Monitoring	Security Assessments	Full Patch Management
 <p>We'll constantly monitor and analyzing your endpoints to effectively protect against threats. If an attack happens, we activate remediation steps including scrubbing the system of any remnants of an attack.</p>	 <p>Knowing in real-time what passwords and accounts exist on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your dealership from stolen credentials that have been posted for sale.</p>	 <p>It's important to establish a baseline and close existing vulnerabilities. The new CROPS assessment tool provides you with all the necessary information to identify security gaps, and our team will help you understand them.</p>	 <p>If there's ever any problems with patches not being installed properly on any of your endpoints, we'll proactively make sure each machine on your network is up to date and secure without the need for you to take any action.</p>

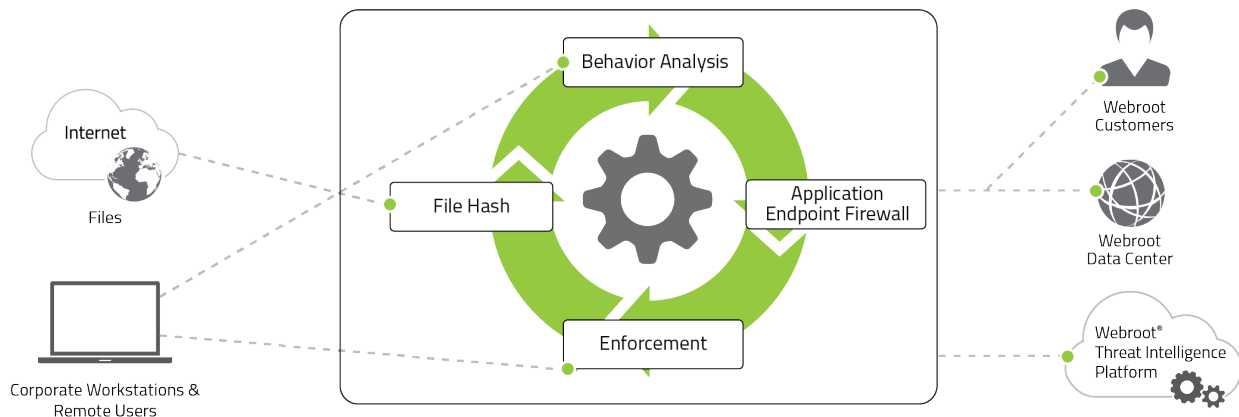
Webroot SecureAnywhere DNS Protection

Webroot SecureAnywhere DNS Protection is powered by Webroot's BrightCloud Threat Intelligence – the same threat intelligence relied upon by industry-leading networking and security firms such as A10, Cisco, Citrix, HPE Aruba, and Palo Alto Networks. BrightCloud leverages an advanced, cloud-based security platform with advanced fifth-generation machine learning and a contextual analysis engine used to determine relationships with known malicious objects in order to gain deep insight into today's threat landscape. This advanced self-learning platform continuously scans the Internet and incorporates inputs from millions of real-world endpoints, along with active scanning and passive sensor networks to quickly and accurately identify zero-day and previously unknown threats at an unprecedented scale.



Webroot SecureAnywhere Security Awareness Training

Webroot Security Awareness Training is a SaaS offering and is integrated into our existing web-based hierarchical console, the Global Site Manager. That's the same streamlined console used to administer award-winning Webroot SecureAnywhere® Business Endpoint Protection and DNS Protection. This has two major benefits: it makes Security Awareness Training extremely easy to deploy, use, and manage; and allows administrators to access and manage a variety of Webroot protection solutions in one convenient cloud-based location.



SentinelOne Protection Platform



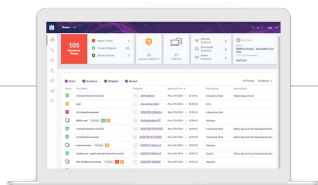
The SentinelOne Endpoint Protection Platform (EPP) unifies prevention, detection, and response in a single purpose-built agent powered by machine learning and automation. It provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, and complete visibility into the endpoint environment with full-context, real-time forensics.

CROPS Premium Features

Sedona Technologies Detect & Respond

Dealer IT Operations Powered by Advanced SOC Expertise

Easily implement advanced operations without the need for in-house security expertise. The complete Sedona Co-Managed SOC analyzes quarantined applications and files, reducing false positive and ensuring comprehensive protection. It delivers a powerful service to help you overcome the significant labor challenges associated with providing managed security services.



Threat Detection

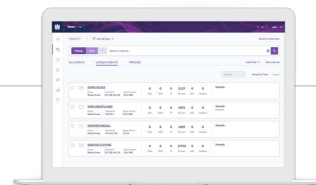
Rapidly identify thousands of variants of viruses, malware and root causes of malicious behaviors by quickly diagnosing source processes and programs.

We use a static AI engine to provide pre-execution protection.



Rapid Response

Our behavioral AI engines and SOC team tracks all processes and their interrelationships regardless of how long they are active. When malicious activities are detected, the agent responds automatically at machine speed.



Visible Remediation

Our automated EDR and SOC provide see rich forensic data in real time and can mitigate threats automatically, perform network isolation, and auto-immunize the endpoints against newly discovered threats.

CROPS Profile & Protect

Out-of-the-Box Security Profiles

Profile & Protect features pre-built and customizable profiles that tell you exactly what's needed to protect against certain threat types. These recipes identify specific gaps in protection on a client device (e.g. no endpoint protection is installed, poor results of phishing simulation, patches are out-of-date, etc.), helping you identify potential vulnerabilities and take corrective action where needed.

Risk Scoring and Alert Thresholds

Each device also receives a risk score, allowing you to quickly understand how a particular gap in protection impacts the threats you're trying to protect against. Alert thresholds can be customized, allowing you to clearly articulate acceptable risk on a per-device basis—and tickets are only generated when a risk score exceeds its threshold, eliminating much of the clutter and white noise found in other solutions.

Dealer Growth and Protection with Managed Security Services

Profile & Protect enables dealerships to protect their dealership against vulnerabilities they might not have known existed, with functionality that supports baseline security assessments and analyses as well continuous monitoring and optimization which translates into monthly recurring revenue and protection for dealerships.

CROPS Empower+

Realtime Security Assessments

Target compelling security events with Sedona Security Assess. This Empower suite assessment tool provides you with all the necessary information to identify dealer security gaps, and reports to help you understand your security gaps. Run scans for dark-web exposure, perform endpoint and user risk analyses and generate accessible reports to help you understand your environment vulnerability, and grasp how your cyber security protection compares to other John Deere dealers.

Dark Web Monitoring & Security Understanding

Get real time alerting and notifications if your dealer or employees appears on the Dark Web, we'll send you the list of passwords and where they came from any time something new appears. Understand any vulnerabilities and security gaps is key to deciding what additional layers could help your dealership be protected.

