NORMAN **SHARK**

RED SKY ALLIANCE AND NORMAN MALWARE ANALYZER G2

ADDRESS ADVANCED PERSISTENT THREATS

"One of the most important technologies we needed to integrate from the beginning were automated malware analysis tools that allowed us to give clients complete peace of mind that they were protected at the highest levels"

Jeff Stutzman
Chief Operating Officer.

A private, subscription-based service, red sky® Alliance (www.redskyalliance.org) enables its members to share information about the latest malware and other network security threats as well as assist each other with attack analysis, best practices, and threat prevention within the privacy of a closed environment. Through a full set of social media tools, companies can research, collaborate, share indicators, and provide mitigation recommendations for the latest threats. These findings are then compiled and delivered to Red Sky members in a comprehensive 'Fusion Report' that provides actionable information about the threat to alliance members.

With more than a dozen member companies responsible for nearly four million computer systems worldwide, Red Sky's clients are well-known, global corporations, and are exposed to thousands of daily cyber attacks. "Processing, analyzing, and mitigating this amount of malware, in addition to dealing with valid network traffic, puts a heavy load on any company's systems," said Jeff Stutzman, Chief Operating Officer of Red Sky Alliance. "Not only must companies consider the overhead costs to simply process this volume of malware and Advanced Persistent Threats, or APTs, but they also must plan for potential down time and other unforeseen costs when these threats go undetected or unmitigated. In a large, Fortune 100 company, network security can be a six- or seven-figure line item in the IT department's budget."

"With Norman Malware Analyzer G2, we can give our clients access to an extremely sophisticated technical solution that helps them keep their systems and networks safe and secure."

In today's economy, most companies can't afford such a large line item, but they also cannot afford not to implement stringent network security. Enter Red Sky Alliance. To ensure its clients remain safe and secure from malware and other APTs in a costeffective manner, Red Sky must rely on proven network security technologies and services that protect clients' most

sensitive customer data and intellectual property from theft or other malicious use. "One of the most important technologies we needed to integrate from the beginning were automated malware analysis tools that allowed us to give clients complete peace of mind that they were protected at the highest levels," Stutzman said.

Solution

After researching several malware analysis solutions and test-driving a handful of them in-house, Stutzman was immediately impressed with the Norman Software Malware Analyzer G2. "Norman next generation automated malware analyzer delivers a fully emulated Microsoft Windows environment, plus an IntelliVM. IntelliVM uses a KernelScout capability embedded for intelligence observation at the lowest level of a system's kernel to monitor for signs of malicious behavior. This gives us the flexibility to analyze even the toughest malware problems and gives us more precise mirroring of custom environments for advanced and targeted threats," Stutzman said.

"Malware threats are one of those areas where even the biggest companies struggle to adequately fund proper cyber defense."

"Red Sky® Alliance participants expect instant notification when attacks are noted, and Norman's tools help us meet our customer's demanding expectations." Deploying the Norman Malware Analyzer in Red Sky's network was a simple process, which is important in a smaller organization with few employees. "Ease of integration, deployment, and management are key decision-factors for any solution we purchase because we don't have a lot of time to dedicate to these activities," Stutzman said. "We need cost-effective solutions with great customer support that enable us to start delivering value-added services to our clients as quickly as possible. Norman delivers on this requirement."

Results

For Stutzman, the significant productivity improvements delivered by the detailed malware analysis and reporting capabilities are a key benefit of the Norman Malware Analyzer G2. "When one of our clients receives a piece of malware, he immediately zips the malware code so it doesn't execute and uploads it to Norman Malware Analyzer G2 on the Red Sky Alliance portal. Then, Norman's malware experts do a first run of analytics," Stutzman said. "Without automated analysis, this type of challenge could take days, or even weeks; with Norman, it's a simple 30- to 60-minute process between the time a client uploads a piece of malware and when he has an initial report on the who, what, where, when and why of the code's potential impact." When asked to summarize his overall thoughts about Norman Software and Malware Analyzer G2, Stutzman doesn't hesitate. "Malware threats are one of those areas where even the biggest companies struggle to adequately fund proper cyber defense. With Norman Malware Analyzer G2, we can give our clients access to an extremely sophisticated technical solution that helps them keep their systems and networks safe and secure – at a reasonable cost that is within today's tight IT budgets," Stutzman said. "Plus, from a customer support perspective, Norman has bent over backward with our membership to make sure we are all well taken care of. That's a win-win for both the Red Sky Alliance and our clients."