PARTNER CASE STUDY

Pine Cove Consulting Safeguards K-12 from Ransomware with Sophos XG Next-Generation Firewall Appliance

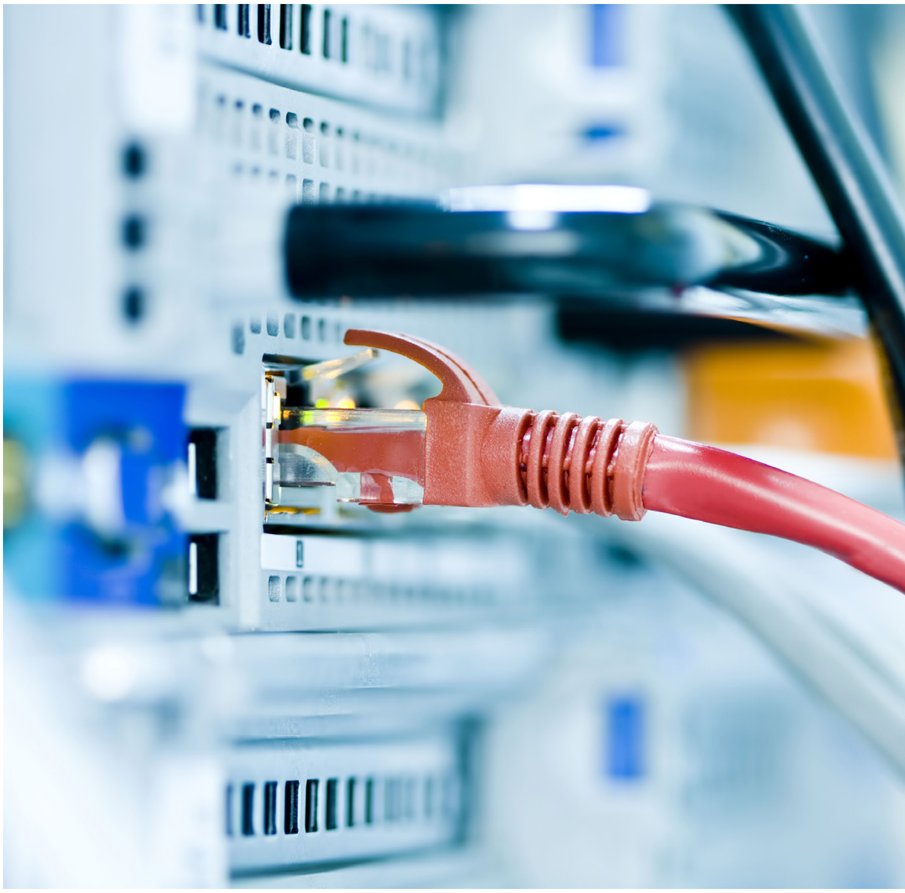
Partner-at-a-Glance

Pine Cove Consulting, a technology provider for K-12 educational institutions, businesses, and government agencies in the Rocky Mountain region of the US, has been a Sophos partner for 15 years and has fully integrated the Sophos XG firewall and other products into its security portfolio. Named Sophos Complete Security Partner of 2016, Pine Cove Consulting offers its customers a comprehensive, end-to-end, coordinated defense against ransomware and other advanced threats through the Sophos Synchronized Security approach.

Industry
Technology solutions provider

Sophos Solutions
Sophos XG Firewall
Sophos SG UTM
Sophos Intercept X
Sophos Wireless
Sophos Email Gateway
Sophos Endpoint Protection

Sophos Partner
Since 2001



Pine Cove Consulting is a technology solutions provider working primarily with rural K-12 school districts and businesses in the Rocky Mountain states. A Sophos partner for over 15 years, Pine Cove Consulting has expanded its portfolio of Sophos security products to include security solutions for the network, endpoints, Wi-Fi, and email. Pine Cove Consulting is committed to providing its clients with flexible, comprehensive security and is a leading partner for Sophos in its region.

'Synchronized Security is a simple and elegant way to achieve better security and reduce the time spent on incident response.'

Dan Russell
CIO
Pine Cove Consulting

Business Challenge

Over the past several years, in response to a dynamic and ever-changing threat environment, Pine Cove Consulting made a strategic decision to change its direction. When customers started to voice concerns about ransomware and other advanced threats, the technology provider made security the primary focus of its business. The company's aim was to deliver comprehensive, flexible, and easy-to-use security solutions to its customers and achieve a deep level of expertise across the entire Sophos portfolio.

Among both education and business clients, the proliferation of rapidly evolving ransomware threats became a major concern. A recent survey reveals that ransomware has increased fourfold over the past decade, and new variants are emerging constantly.[1] Ransomware attacks operate by installing malware on a system that encrypts and locks down valuable data or compromises the operating system. Perpetrators promise to release the files only upon payment of a substantial ransom. Typical ransomware delivery methods include phishing emails, exploit kits embedded in web pages, and malicious ads, also known as malvertising.

Pine Cove Consulting's K-12 customers were looking for a better way to prevent ransomware from infiltrating their systems across multiple threat vectors. Point solutions from other vendors that only addressed specific threat vectors were proving to be inadequate.

"In the past, K-12 customers didn't exert much energy on security. But today they look at security differently, largely because of the proliferation of ransomware. Schools and school districts are now taking the problem quite seriously," explains Pine Cove Consulting CIO Dan Russell. "Instead of a separate, unintegrated approach to security, education customers are more interested in adopting total protection solutions. Our K-12 customers want to ensure that students don't visit malicious websites and download malware-ridden content. As a result, strong web filtering is one of the top priorities."

[1] https://www.scmagazine.com/microsoft-detects-400-percent-ransomware-increase/article/572835/

'Sophos XG's Security Heartbeat allows the firewalls to talk to endpoints and share insights and information on threats and security status.'

Dan Russell
CIO
Pine Cove Consulting

Making the Big Switch to Sophos

The propagation of sophisticated ransomware threats motivated many schools, school districts, and businesses to make the switch to the Sophos XG firewall, largely because of its ability to defend against complex, multi-stage attacks. Sophos XG provides a comprehensive defense, including network, wireless, IPS, VPN, web, app control, email, and web application firewall technologies.

"Schools feel more confident knowing that advanced web protection from Sophos XG can safeguard staff, students, and systems from ransomware, which often uses a variety of methods to carry out the attack. Sophos XG looks at threats from different angles and applies a variety of detection techniques. Behavioral analysis and origin reputation play a big part in that—as does HTTPS scanning, which looks for threats hiding in encrypted traffic," remarks Russell. "In an environment where tablets and other mobile devices are as common as computers, K-12 customers also value the user-level policy controls over applications, websites, and categories, regardless of device or network."

Russell has found that both education and business customers are eagerly getting on board with the Sophos Synchronized Security story and the visibility and centralized management afforded by Sophos Firewall Manager. "When we present Sophos to customers, we rarely need to review the point-by-point product comparisons with competitive products. I'm seeing that our customers are drawn by the bigger picture, by the forward-thinking approach that Sophos delivers," comments Russell.

Flexible Firewall Protection

The Sophos XG firewall appliance is one of Pine Cove Consulting's core offerings. When it comes to firewall protection, Russell finds that education customers and small businesses have similar needs, though there are some important differences. The K-12 environment overall has stricter policy requirements, though Russell finds that they end up making exceptions quite often, based on changing curriculums and staff needs. Businesses, on the other hand, simply want to be protected so that they can be productive without interruption.

For schools, a must-have is the ability to easily create a policy, apply it to a rule, and modify it when necessary. Staff members often need to override a category or a URL for a particular class or project or for their own use. "In most schools, there are generally two different policies for web surfing: one for the staff and one for the students. Sophos XG enables clients to easily make a policy change for all users over a limited period of time." notes Russell. "With Sophos XG, they have the flexibility of keeping it simple or getting granular. For example, at some school districts, web surfing policies are defined according to the student user's grade level: elementary, middle school, or high school. We even have a business customer that has defined thousands of policies—and Sophos XG is able to handle that level of detail with ease."

Typically, Pine Cove Consulting implements the firewall installations, sets up the policies, and then makes refinements. Russell has remote access to almost all of his customers, which enables him to assist with initial setup or step in when his help is required. The pre-defined policy templates for applications like Microsoft Exchange or Microsoft SharePoint make it easy for Dan to set up firewall rules and security settings.

"Some of our customers are completely at home managing their own security, whereas others contract with us to manage their entire security infrastructure. In either case, Sophos XG's new unified policy model makes it simple for anyone to manage user, application, and network policies from one screen. Thanks to Sophos Firewall Manager, our customers are readily embracing the 'push' notion, where policy is conveniently provisioned from the central management tool rather than from the appliance itself," states Russell.

Synchronized Security

Pine Cove Consulting understands that advanced threats like ransomware are becoming increasingly difficult to detect, which poses a challenge for traditional defenses. “Sophos technologies like ATP protection, Sandboxing, and Synchronized Security combine to provide a coordinated defense against today’s zero-day threats,” acknowledges Russell.

Pine Cove Consulting is a big advocate for the concept of Sophos Synchronized Security. Sophos Heartbeat synchronizes next-generation firewall protection with endpoint protection and enables the two technologies to share health and status information in real time. This revolutionary technology accelerates time-to-protection against sophisticated threats. “For example”, Russell says, “when Sophos XG Firewall detects suspicious botnet traffic, Sophos Heartbeat enables the firewall to instantly identify the originating host and even respond automatically, isolating the affected system or limiting access to network resources until it can be investigated and cleaned up”

“When we approach a prospect, we always go with a total solution in mind. Right now, people are exploring how Sophos Security Heartbeat can be used. No one wants infected systems to connect to servers, and Sophos Security Heartbeat makes it easy to spot compromised endpoints accessing servers. We’re really looking forward to seeing the technology used to its full potential at our customer sites,” relates Russell.

Unwavering Performance

Another Sophos XG feature that is widely used among Pine Cove Consulting’s private sector customers is advanced VPN. Businesses appreciate the one-time set-and-forget implementation and the easy process for end-user sign-on.

Reliable firewall performance and high availability are also critical for all Pine Cove customers—especially for larger school districts, which may have from 1,000 to 1,500 power users among its students and staff. To ensure maximum uptime over the long term, Russell took it upon himself to create a sizing calculator, which he uses to scope out a customer’s requirements for optimum coverage. “It’s always better to be on the safe side and ensure a customer’s network security needs are fully met, both now and for the foreseeable future,” articulates Russell.

A Committed Partner

Pine Cove Consulting prides itself on relationship building with customers and vendors. “We don’t like to carry multiple products, nor do we even entertain selling another vendor’s products merely for convenience. With Sophos’ broad scope of security coverage, we don’t see any reason to sell or recommend anything else,” asserts Russell.

Russell has made a personal commitment to immerse himself in all things Sophos — from network to firewall and endpoint to email — and become as highly educated as possible on Sophos technologies.

“In the past, we were trying to be all things to all people and found that we were getting stretched too thin, so we decided to narrow our focus,” Russell elaborates. “We’ve been working diligently to build our expertise in the security area, with Sophos as our vendor of choice. Earlier on, we had some Sophos endpoint installations. It’s been about three years since we made a decision to go full steam ahead with the Sophos XG firewall appliance and other complementary Sophos solutions,” concludes Russell.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS