Sophos MSP Connect helps Dataprise simplify management, boost revenue, and offer comprehensive, unified endpoint protection to its large and diverse client base.

Dataprise is a large managed service provider (MSP) that helps companies throughout the country manage and monitor their IT infrastructures. Serving organizations with 5 to 5,000 endpoints, Dataprise prides itself on being a “one-stop IT shop” and the number one-ranked MSP in the Washington, D.C. area. Tim Foley, Director of Information Security, sums up Dataprise’s mission: “We offload IT and information security services so that our clients can focus on what they do best and can grow their businesses.” Dataprise became a Sophos partner two years ago, and now provides its customers with comprehensive endpoint protection and a powerful defense against ransomware attacks.
Why Sophos MSP Connect

Dataprise was looking for a seamless way to provide a high level of customer satisfaction while increasing the productivity of in-house engineering staff and maximizing profitability. Prior to joining Sophos MSP Connect, Dataprise used traditional antivirus supplemented with Malwarebytes for both its in-house security and for its clients.

As ransomware attacks gained momentum and became the number one security concern of its clients, Dataprise found that it was investing 1,500 to 2,000 hours per year in ransomware cleanup. That translates to 50 hours per ransomware attack, or the equivalent of a security engineer working 30 hours per week with an annual salary of $60,000. Foley saw that the business impact of ransomware on both Dataprise and its clients was unsustainable. Dataprise has a shared equity model for their unlimited service plans—for a fixed monthly dollar amount, Dataprise manages all of a customer's endpoints and users. So when ransomware hits, both Dataprise and its clients share the risk. Dataprise invested its resources in cleanup and restoring files from backup at no cost to the client, while the client bore the risk of downtime and $10,000 to $100,000 in lost revenue.

Foley, who is responsible for product road-mapping, decided it was time to explore other alternatives. He and his team evaluated several endpoint security vendors, and Sophos came through “with flying colors,” beating the competition. Foley was particularly impressed with web control and device control features in Sophos Central Advanced. “I set Sophos Central Advanced to block by default content not suitable for work environments. Some of these sites are loaded with nefarious malware, so if we can block users from going there, we’ll have a more manageable client,” explains Foley.

He and his team then set out to migrate the tens of thousands of client endpoints to Sophos Central Advanced and Sophos Intercept X, which Dataprise is including at no cost to its managed services customers. Using automated processes, they have already migrated 6,500 endpoints and plan to complete the task within the next several months. For clients running Sophos Intercept X, Foley reports that there have been zero ransomware issues.

The Sophos Central Partner Dashboard is tailor-made for an MSP like Dataprise, providing better visibility and eliminating the complexity of managing tens of thousands of client endpoints. Dataprise engineers can access the web-based console anytime, anywhere—even from mobile devices. For Dataprise, the intuitive interface has vastly simplified the process of onboarding new clients and adding new services. “What I like about the portal is that, as we add new Sophos products—like firewall—to our roadmap, we can have everything under one umbrella,” observes Foley. “I am responsible for selecting the right products at the right price point and with the right central management portal for my own group, for the organization as a whole, and for our clients. Price, technology, and ease of use are all factors that we take into consideration when evaluating a vendor, and we felt that Sophos excels in all these areas.”

Benefits of Working with Sophos

Greater profitability

By installing Sophos Intercept X, clients are no longer experiencing downtime caused by ransomware attacks, and Dataprise is saving 1,500 to 2,000 labor hours a year spent on cleanup and data restoration. The Sophos MSP Connect bulk discount and monthly billing is in alignment with the Dataprise MSP service model—there are no upfront costs, so the more services Dataprise sells, the lower its costs. With MSP Connect Flex pricing, Dataprise can control how and where licenses are distributed and can offer competitive pricing that maximizes their margins. Finally, single-agent technology across Sophos Central Advanced, Intercept X, and other products consumes fewer CPU resources, thereby reducing operational overhead.

Greater productivity

Through the intuitive Sophos Central Advanced management platform, Dataprise manages all its clients and all their Sophos products from the single-pane-of-glass, web-based console. By consolidating and simplifying management, Dataprise has reduced in-house administrative overhead. “Thanks to the Sophos Central console, we’ve moved endpoint protection from our service desk to the security operations center (SOC), where it belongs. My SOC team has taken over monitoring and management. Through root cause analysis and USB and peripheral controls, we are experiencing a greater amount of control over our clients endpoints,” explains Foley.

Greater efficiency

By becoming a Sophos MSP Connect Partner, Dataprise has streamlined day-to-day operations and improved business efficiency. By continually investing in R&D and ensuring that all products work together, Sophos helps Dataprise minimize product development cycles and gives the MSP confidence that it can deliver a consistent and advanced level of security. Simplified deployment and easy billing processes also reduce the amount of time Dataprise spends on back-end processes.
Future Plans

Looking ahead, Foley and his team see an opportunity to “increase the resiliency of the attack surface” for Dataprise clients by deploying Sophos XG Firewall and Sophos Synchronized Security, which is powered by Sophos Security Heartbeat™ technology. Sophos Security Heartbeat allows endpoints and firewalls to communicate and share threat insights and information on the health status of endpoints. This capability, along with automated processes, vastly improves detection and remediation across the entire infrastructure. The big advantage of Sophos Synchronized Security is complete visibility to the network. “This single-vendor, fully coordinated approach to security will allow us to know exactly what’s happening on the network at all times,” declares Foley. “From a sales and marketing position, Sophos Synchronized Security makes great sense. With Sophos Synchronized Security, everything is communicating with everything else to provide the best client experience.”

In the coming year, Foley also sees an opportunity to migrate to Sophos an additional 65,000 endpoints not currently under a Dataprise information security service agreement. “We believe that every organization deserves great information technology services and great information security managed services. We are extremely confident about leading with Sophos on these shared equity model service plans. With Sophos Central Advanced and Sophos Intercept X, we’re getting fewer calls about viruses and ransomware, and that trickles down to our clients and their users,” concludes Foley.

‘Price, technology, and ease of use are all factors that we take into consideration when evaluating a vendor, and we felt that Sophos excels in all these areas.’

Tim Foley
Director of Information Security
Dataprise

1,500+

labor hours saved, which, prior to Sophos, had been spent on ransomware cleanup.
- Dataprise

To learn more about Sophos MSP Connect and join the program visit
www.sophos.com/msp