

THE SENSIBLE APPROACH TO IT

Accounting firm sought support for IT,
regulations and cybersecurity

THE DILEMMA

The increasing potential of a breach and pressures from cybersecurity regulations paired with a hectic busy season led accounting and CPA firm RDG+Partners to seek a managed IT provider for its support.

RDG+Partners recognized that its expertise is in accounting, not cybersecurity and IT. With the firm's prudent approach to finance, it looked for a provider to cost-effectively meet all its IT needs. As a result, the firm selected BriteStar for a comprehensive managed IT services offering. The offering from Brite extends beyond basic IT and helpdesk services to include advanced cybersecurity protections.

"Between day-to-day support and ongoing security services, we knew that selecting BriteStar was the sensible decision," John Rizzo, CPA and Managing Partner at RDG+Partners said. "Our industry and access to client information make us easy targets for attacks. With the reliance on technology, we can't afford downtime during the busy season or throughout the year! Our technology cannot impede our services."

THE BRITESTAR SOLUTION

A three-phase, comprehensive approach makes tackling IT and security easy for any organization.

"Implementing our comprehensive service within three phases helps customers like RDG+Partners digest the capabilities and accurately understand the support and coverage they're receiving," Steve Wilmarth, Brite's Sales Director of Managed Services. "This benefits the fast-paced RDG+Partners. The internal IT team can be confident in exactly what's taken off the teams plate."

Proactively Maintain Business Operations

A proactive IT approach was necessary to keep RDG+Partners operational, especially during the busy season. Long hours and critical timelines emphasize the need to minimize technology troubles.

The team gained confidence through BriteStar's proactive planning and management: all individuals receive properly imaged PCs with appropriate access to programs, patches are done in a timely manner and servers are continuously monitored and managed. Once the proactive approach was implemented, ticket volumes and frustrations dramatically decreased.

When issues do arise, BriteStar's 24/7 unlimited helpdesk jumps into action. From simple password resets to facilitating third-party software support, RDG+Partners knows that Brite is always there to resolve technology problems.

“The strategic foresight to partner with a provider is invaluable. Again, just the peace of mind that I know we’re protected; and that the entire Brite team is there for anything is a huge burden off of our team.”

“Having a dedicated team that we can trust and rely on at any time eases the burden. Our entire team knows to contact the helpdesk for any issues,” Rizzo recalled. “As Managing Partner, it’s a peace of mind to know the entire Brite team has our back to keep us up and running.”

The Pressure for Security

Accounting and CPA firms have inherent security risks that require proper management, monitoring and protection of client data and systems. The recent focus on protecting personal, sensitive data required RDG+Partners to adhere to complex cybersecurity regulations like NYS DFS 23 NYCRR 500 and the New York SHIELD Act.

The regulations require network, data, email and endpoint protections along with 24/7 monitoring and management of those tools.

The ability to generate compliance reports quickly and easily was also critical. Brite was able to easily meet all needed requirements and provide detailed documentation, which is reviewed at Quarterly Business Review meetings.

A Good Plan Always Has Backup

We all know that even with the tightest security and proactive planning, there will be a failure at some point - it is inevitable. To protect against natural disasters, systems failures or cyberattacks like ransomware, BriteVault’s Disaster Recovery and Business Continuity solution was deployed.

RDG+Partners quickly realized the benefit of BriteVault when it lost the backbone of the IT infrastructure during a server failure. As the failure was detected, the systems automatically switched over to the backup environment, eliminating any disruptions. Because of the well-executed business continuity plan, employees did not experience downtime and no company data was lost. Upon Brite’s investigation, it was determined to be a server failure and not a cyberattack. The server was repaired, and operations continued.

Rizzo reflected, “The strategic foresight to partner with a provider is invaluable. Again, just the peace of mind that I know we’re protected; and that the entire Brite team is there for anything is a huge burden off of our team.”