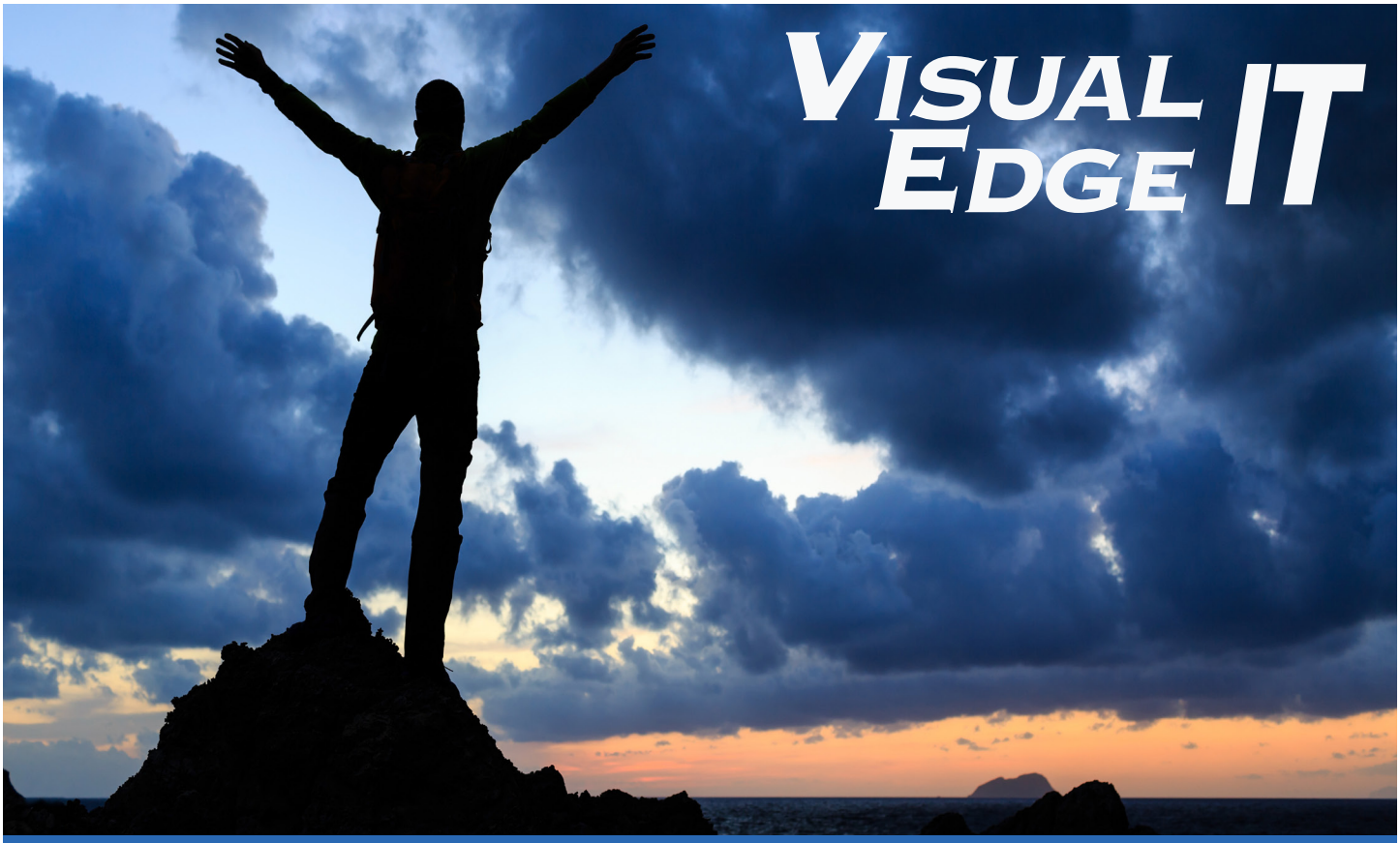

CASE STUDY | TOXICOLOGY LABORATORY

VERTICAL

Healthcare

SOLUTION

Managed IT Services

THE CUSTOMER

The customer is a toxicology laboratory.

THE SITUATION

The customer is looking for a larger, more experienced IT provider to help them avoid another security situation like the ransomware attack they previously experienced.

The ransomware infected their network with multiple viruses and malicious files.

They were unable to recover with their current provider and were left no choice but to pay the ransom.

They are seeking an experienced, knowledgeable IT company to manage and protect their data, and work with on cybersecurity challenges.

THE COLLABORATION

The laboratory interviewed three IT providers and selected Visual Edge IT for our knowledge and expertise in the areas of IT support, current technologies, and data security.

We provided them with managed IT services for help desk and IT support. We also provided several layers of security to their infrastructure that includes advance email protection and advanced endpoint protection.

Additionally, we helped the laboratory create end-user computing standards focused specifically on security policies and procedures.

THE OUTCOME

The laboratory has experienced more peace of mind knowing that their data and network are properly monitored, managed and protected.

A near- and long-term technology roadmap was created to allow the company to plan and budget for additional security and technology going forward.

Onboarding was challenging due to the ransomware clean-up, but the customer is delighted that those challenges have been overcome and with our service.

SECURED DATA AND CLEANED UP NETWORK AFTER A BREACH.

RELATED CONSIDERATIONS

22

EVENTS.

One fifth of organizations experience 22 or more data-loss events a year in which sensitive data is stolen, lost, leaked or destroyed.

$8,500

PER HOUR.

On average, downtime from data-loss events costs small- and medium-sized companies more than $8,500 per hour.

67%

FAILURES.

67% of data loss is caused by equipment or system failures.