SUCCESS STORIES

Crestwood's Cloud Services Team Stops a Ransomware Attack in its Tracks

> "The successful mitigation of the ransomware attack highlighted the importance of having a comprehensive business continuity and disaster recovery (BCDR) strategy, which Crestwood Associates expertly provided."
>
> \- Ben Borger
>
> Director of Cloud Services

LOCATION

Nationwide

APPLICATION

Crestwood's Real-Time Monitoring and Rapid Responsiveness

SOLUTION

Crestwood Associates Cloud Services

The Challenge

Our client in the hospitality industry encountered a ransomware attack. Ransomware attacks can be a significant threat to any organization, but with the right measures in place, they can be effectively mitigated. Ransomware is a type of malware that encrypts the data on a victim's computer or network and demands a ransom for its decryption. It can cause severe damage to an organization's operations, reputation, and finances. It can also expose sensitive information to hackers or public exposure. Ransomware attacks are becoming more frequent and sophisticated, targeting businesses of all sizes and sectors. Thankfully, Crestwood Associates is expert in preventing Ransomware damage before it happens.

The Solution

Crestwood Associates is a skilled and reputable Cloud Service provider, enabling a swift solution mitigating any damage from the ransomware. The process to mitigate and eliminate the attack with our client began with Crestwood's real-time detection of the threat, which triggered an immediate response from the security team. They quickly isolated the affected systems to prevent the spread of the ransomware. Once isolated, the team assessed the damage and determined the most recent clean snapshots of the VMs.

Fortunately, the organization we were working with had a robust backup strategy (by design), with regular snapshots stored securely in a recovery services vault. These snapshots served as a point-in-time copy of the VMs, which included all the data, applications, and system settings. Furthermore, the recovery vault uses Microsoft's new immutable vault property, which prevents backups from being deleted or modified, protecting them from any efforts to destroy them.

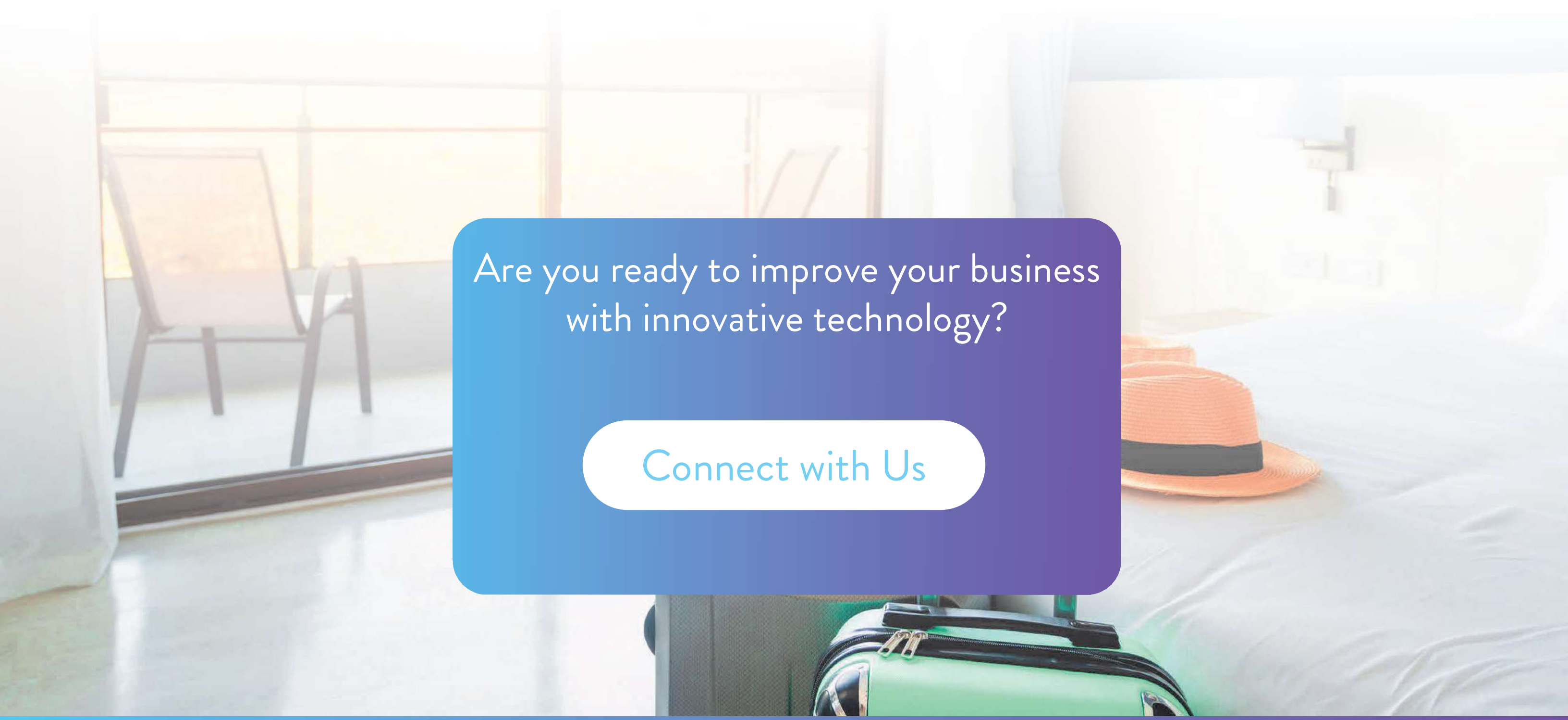
Key Results

- Ransomware attack completely neutralized
- Stopped reignition of Ransomware
- Business Continuity and Disaster Recovery (BCDR) plan succeeded

The Outcome

The successful mitigation of the ransomware attack highlighted the importance of having a comprehensive business continuity and disaster recovery (BCDR) strategy. Crestwood had this in place for the client after an assessment of their IT environment. Further, the use of virtual machine (VM) snapshots and Azure Recovery Services Vault, which is part of every Crestwood Cloud ERP deployment, enabled the IT team to revert the affected systems to a state before the attack occurred, minimizing downtime and data loss, and preventing any need to pay the attackers for decryption or to prevent a data breach.

This experience demonstrated the effectiveness of VM snapshots and a recovery services vault in quickly recovering from such cyber threats and it serves as a reminder for all organizations to regularly review and update their cybersecurity measures, including backup and recovery protocols. By being prepared and having the right tools in place, the business protected themselves against the ever-evolving landscape of cyber threats.



Are you ready to improve your business with innovative technology?

Connect with Us