CUSTOMER CASE STUDY

Summit Hosting

An aggressively growing Quickbooks hosting company is resource constrained and disrupted by ransomware three times in one month

SUMMIT HOSTING™
MANAGED CLOUD SOLUTIONS

- Mid-market hosting company
- Based in Atlanta, Georgia
- 7,000 clients

THE ORGANIZATION

Summit Hosting is a cloud hosting company offering specialized Quickbooks hosting services.

Launched in 1996 as myownASP.com, it grew organically for several years increasing its user count by up to 10 percent each month.

The company rebranded to Summit Hosting in early 2017 as part of an acquisition strategy that more than quadrupled its user base. Today, Summit Hosting has approximately 20,000 users.

CUSTOMER CASE STUDY

Summit Hosting

THE CHALLENGE

Summit Hosting's aggressive growth strategy had left it resource constrained and the company was struggling to manage a diverse set of assets across several locations that made them difficult to secure.

Updates were a particular challenge, explains Brian Wilder, senior network engineer at Summit Hosting. Updates applied to a Windows server could break products for multiple users. Additionally, customers didn't always secure their software effectively, which created potential weak spots in the system. The company was floundering in its attempts to keep systems secure and reliable, says Wilder, explaining that an industry shortage of security professionals had made them prohibitively expensive.

In December 2017, Summit Hosting suffered from a ransomware attack at its Atlanta datacenter over the holidays. When administrative websites stopped working, the small team realized an attack had occurred. "Stuff went down, like a ticketing system that stopped functioning. About then, I started seeing all the files were being encrypted," said Wilder.

The ransomware turned out to be a version of the SamSam strain that cost the city of Atlanta $17 million in 2018. "They took out our backups, so we had to pay $180,000 and then wait 12 hours before obtaining the decryption keys," Wilder said. The company also had to pay another $90,000 to customers in credit for the disruption that occurred.

> **"As a whole, eSentire has been a ten on the scale. They are responsive and help in any way they can."**
>
> **Brian Wilder**
>
> Senior Network Engineer
> Summit Hosting

Summit Hosting

THE SOLUTION

In January 2018, Summit Hosting turned to eSentire for a full security assessment to benchmark and consistently evaluate Summit Hosting's cybersecurity posture across two of its sites in Atlanta and Toronto. eSentire conducted a Risk Assessment and a Malicious Activity Assessment to address any residual from the ransomware attack and to build out a defensive plan by better understanding the security gaps across their environment.

eSentire's Risk Assessment focused on gaps in Summit Hosting's incident response from the recent ransomware attack. A team of security experts were able to:

- collect crucial information to speed up the investigation
- contain and disrupt the threat from doing further harm
- eliminate all traces of the threat
- provide monitoring for re-entry

A unique component of the Risk Assessment was the Malicious Activity Assessment that leveraged eSentire's network security solution. It provided 45 days of continuous network monitoring and analysis of granular forensic data by SOC analysts to identify blind spots in Summit Hosting's environment. Following the engagement, a plan was then put in place to work towards covering the gaps.

eSentire also conducted a detailed technical and procedural security audit that uncovered weaknesses in everything from the smallest procedural detail through to flaws in broader systemic practices. On the technical side, it included complete scans of the company's network and assets to identify vulnerable spots that needed extra protection. On the procedural side, eSentire provided invaluable guidance on key cybersecurity hygiene practices like patching and change management. It also helped Summit Hosting formalize its training processes with top executives through to administrators.

Summit Hosting

The eSentire Solution

eSentire Risk Advisory Services

A build-your-own assessment package, including:

- Risk Assessment
- Malicious Activity Assessment
- Penetration Testing
- Phishing Campaign
- Vulnerability Assessment

eSentire Managed Detection and Response™

esNETWORK™ provides 24x7x365:

- Rapid intrusion detection and response that auto-detects and responds to known and unknown threats with:
  - Real-time blocking of IOCs, signatures, and previously unseen attacks, including phishing, malware, ransomware, and botnets
  - An extensive, proprietary rules library covering 40+ threat categories
  - Highly-customizable rules and policies, including executable white lists, geo-IP, and blocking access to specific sites

While Summit Hosting was working with eSentire, a third site that was not included in the scope of the eSentire project was hit three more times with ransomware despite using another vendor's IDS/IPS solution. Once again, they were forced to pay the ransom, build new servers for customers and give out credits. This further proved the value and need for eSentire's advisory and managed detection and response services.

Summit Hosting

THE RESULT

Following eSentire's Risk Assessment and findings from the Malicious Activity Assessment, Summit Hosting purchased esNETWORK™ to provide 24x7x365 real-time protection utilizing security experts in eSentire's SOC and eSentire's (TTC) Tactical Threat Containment to isolate and block threats on Summit Hosting's behalf. Thanks to eSentire's MDR service, Summit Hosting is in a far better place.

A stricter set of operating procedures has given Summit Hosting peace of mind, meaning Wilder can finally sleep at night without worrying about where the next attack is coming from.

The company updates its servers every quarter and has a robust incident response procedure in place, enabling it to isolate and quarantine virtual machines quickly if eSentire's sensor detects a problem.

"I feel 100 percent better compared to where we were a year ago," says Wilder, adding that he is confident the company will be able to restore uptimes of at least 99.98 percent after a period of instability. For a hosting provider whose entire business is built on trust, that's one business benefit that can't be overestimated.

"

"It was amazing how many threats made it past our firewall in a day that was detected by eSentire's sensor once it went live," Wilder says.

eSentire manages up to 400 cybersecurity incidents every 24 hours for Summit Hosting through investigation and forensic analysis to determine if the threat is a false positive or requires the attention of the team.

eSentire

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-distrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.