

## Providing a premier regional bank with next-generation malware protection

### Challenge:

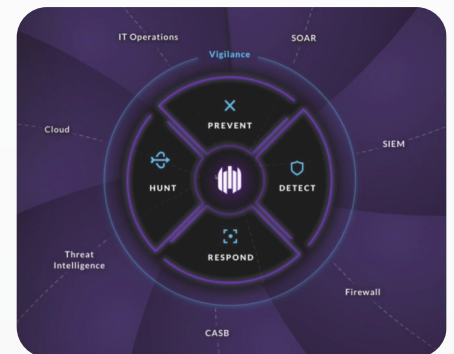
Ransomware is now more widespread than ever. The client suffered a malicious attack due to the failure of its existing endpoint protection solution to detect the threat, with its existing solution also failing to provide a means of recovery.

Data was encrypted by the ransomware and recovery was a painful and lengthy process for the client, with access restricted to critical files, systems and applications.

### Solution:

Bridgenet proposed and implemented a next-generation EPP (Endpoint Protection Platform) with EDR (Endpoint Detection and Response) capability known as S1 (SentinelOne). The solution uses Global Intel with Static AI and Behavioral AI, to detect and block advanced malware.

The S1 solution enabled the client to not only detect and block any complex and advanced malware and security breach attempts, but also to record entire attack storylines for the purpose of security forensics. The solution also enabled the roll back of endpoints to their pre-infected state and the recovery of files encrypted by ransomware.



### Results:



#### Unified Prevention, Detection & Response

- Autonomous decisions and automatic, instant responses
- Global Intel with Static AI and Behavioral AI
- Full forensics and indicators
- Easy pivot to EDR



#### Protection

- Holds up to high velocity and stealthy attacks
- Clean, simple management UX provides context
- Feature parity across OSes



#### Recovery

- Easy reversal of unauthorised changes
- One-click remediation and Windows rollback
- Remote device isolation and triage
- Less re-imaging and less operational work

