Enhanced Security Services for Enterprise

Client Success Story

Client partners with Acumera to secure corporate offices after an extensive ransomware attack

About the Company

After facing challenges in recovering from a ransomware attack, the client opted to employ the Enhanced Security Services (ESS) for Enterprise security suite from Acumera to expand the protection provided to their retail locations. Since the client's retail locations remained unaffected by the orchestrated attack, they recognized the benefits of maintaining a robust defensive posture. This decision extended the proactive protection, monitoring, insight, logging, auditing and 24x7 network security support already proven to be succesful at their retail sites. The ESS security suite uses a zero-trust architecture, which is a security model based on the principle of maintaining strict access controls and default distrust of any system or individual.

After a recent debilitating ransomware attack, the client decided to expand the security services Acumera provides their retail stores to the company's corporate offices — gaining proactive protection, monitoring, insight, logging, auditing and continuous 24x7 network security support.

Challenge

In 2020, one of Acumera's longstanding retail clients fell victim to a ransomware attack at their headquarters. Ransomware, a type of malware, encrypts files on a device, rendering them and the systems dependent on them unusable. Perpetrators then demand a ransom for decryption.

The company attributes this specific attack to a user opening a malicious email, leading to the execution of the Maze ransomware (formerly known as ChaCha). The client's network, typical of many small-to-medium-sized businesses, followed a self-managed, flat topology. Consequently, the compromised endpoint, an employee's PC in this case, had full network access to all other endpoints. This facilitated the rapid spread of the ransomware once the initial PC was compromised.

Within a few hours, a significant portion of the infrastructure was encrypted and effectively offline. The ransomware not only impacted file servers but also moved laterally and vertically, encrypting crucial files on other end-user desktops and servers. Ultimately, numerous key internal systems suffered, significantly affecting the company's daily operations.

Although the retail locations themselves remained uncompromised during the ransomware attack, over 300 corporate systems were affected. The offline status of certain corporate systems disrupted business processes for more than 450 retail locations.

Acumera reviewed the network topology, interviewed team members, and went through an exhaustive discovery process to determine the client’s challenges and goals.

Despite eventually quarantining the offending systems, the company encountered a slow and arduous process in bringing everything back online. Limited technical and security resources made it impossible to restore or rebuild all critical systems within a reasonable timeframe. This resulted in reduced visibility into their operations and a lack of actionable data for guiding business decisions.

Attempts to leverage existing general-purpose IT vendors proved challenging, as they lacked the necessary speed, ownership, and cooperation with other vendors. As a next step, the company sought assistance from an expensive cybersecurity firm for ransom negotiation and forensic processes. Unfortunately, the negotiation was unsuccessful, leading to the initiation of the recovery process.

Subsequent investigations revealed that beyond encrypting critical business data, the ransomware had also exfiltrated information from internal systems. Data exfiltration, a common tactic of cybercriminals, is aimed at extorting additional money at a later date. For businesses with personally identifiable or patient medical information, this poses significant reputation and customer experience risks.

Further evidence emerged of other malware present in the network since 2018, rendering traditional server restores untrustworthy. After weeks of grappling with resource constraints and attempting to remediate the issues independently, the company turned to their trusted security partner, Acumera.

Solution

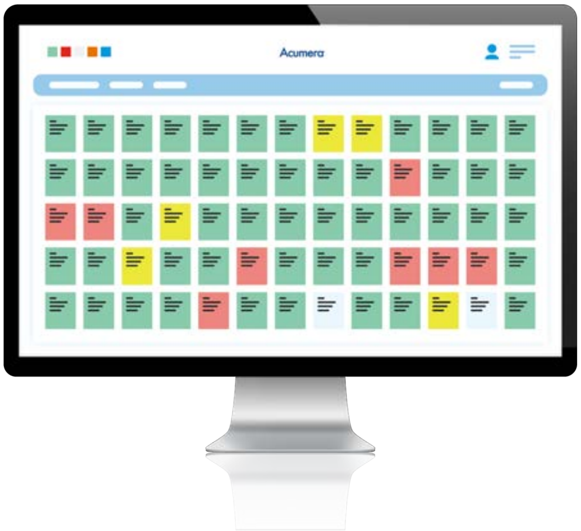
For numerous years, Acumera had been providing managed network security services for the client's retail sites. While the client consistently felt secure about their site security, there had always been a lingering concern regarding the overall cybersecurity resilience of the corporate office. Although the client had previously approached Acumera about implementing its suite of services at their corporate offices, other priorities had delayed the project's progression.

Following the breach, leadership elevated the priority of cybersecurity, and enlisted Acumera to complete a thorough review of the network topology. After interviewing team members, and an exhaustive discovery process, Acumera identified the client's challenges and goals. Collaborating with the company's staff and other technical vendors, Acumera formulated a comprehensive strategy for recovery, migration, and protection.

Built upon the patented MG™ Edge Security Device, Acumera's ESS for Enterprise stands as a defense-in-depth solution grounded in security best practices. This comprehensive approach encompasses various edge computing workloads, including external and internal vulnerability scanning, web filtering, edge and endpoint logging, endpoint detection and response, and endpoint isolation. Covering security from endpoint to edge and every point in between, this suite ensures a robust defense.

To commence with a clean slate and guarantee the absence of back doors into their rebuilt network, the client implemented a parallel network. Systems were only migrated to the new network after being reconstructed. Throughout the recovery process and beyond, the entire original network was treated as hostile and kept outside the security perimeter of the new network. In this enhanced security model, data is permitted to flow outbound from the new network, subjected to inspection for indications of compromise through firewall edge logging and intrusion detection.

Embracing a zero-trust architecture, all devices in the new network are considered hostile and untrusted. Endpoint isolation prevents lateral movement, while network segmentation controls vertical movement through least-privilege access control lists. Endpoint logging and syslogging furnish historical audit information as mandated by various compliance programs. Endpoint detection and response support threat detection, file integrity monitoring, incident response, and compliance for PCs and servers.



AcuVigil™ dashboard for visibility and management

External vulnerability scans aid various compliance programs and identify incorrect configurations before they pose issues. Internal vulnerability scans, employing a vulnerability threat score, prioritize patching based on both Common Vulnerability Scoring System (CVSS) scores and the quantity of affected devices.

Systems on the new network benefit from web browsing protection via category filtering, blocklists, and allowlists, reducing the potential for new malware to connect to control-and-command servers.

As part of the project, multiple legacy solutions were replaced, resulting in a streamlined network fully manageable through the cloud-based AcuVigil™ dashboard by Acumera. The AcuVigil dashboard, with its management-at-scale capability, facilitates configure-once, deploy-everywhere workflows.

Results

Following the implementation of the ESS for Enterprise solution by Acumera, the client has experienced noteworthy efficiency improvements with centralized network and endpoint visibility, monitoring, reporting, and alerting. Furthermore, their technology team is now adept at swiftly detecting and remediating network and security issues, reducing the need for additional staffing through the extensive utilization the 24x7 customer support center at Acumera.

The client, benefiting from management efficiencies through a single-pane-of-glass management platform, is also realizing additional ROI by reallocating internal staff to higher-value initiatives.

Ultimately, the adoption of a zero-trust architecture provides peace of mind to investors and the leadership team, assuring them not only of the protection offered by the ESS for Enterprise security suite for their corporate network but also safeguarding their bottom line and reputation.

About Acumera

Acumera stands as the foremost provider of network operation, visualization, and security services achieved through orchestrating business, networking, and security workloads in the cloud, near the edge, and at the edge. The comprehensive security solutions offered by Acumera extend to securing single-site, multi-site, branch office, and corporate office networks, as well as point-of-sale (POS) systems and IoT devices. This ensures the protection of sensitive data, maximizes uptime, and simplifies compliance measures.

Reasons to Choose Acumera ESS for Enterprise

Helps your IT team

Hand off processes to a team that specializes in securing networks and security monitoring

Safeguards against breaches

Protect your company from breach-related recovery costs of hundreds of dollars per compromised customer record

Keeps your business running

Reduce downtime, save thousands of dollars per hour of lost productivity and reduce reputation risk

Protects employee and customer data

Monitor for data patterns and data exfiltration and ensure privacy compliance (PII, PHI, HIPAA, etc.) with security services provided by Acumera