CLIENT SUCCESS STORY:
Enhanced Security Services Enterprise

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

After a recent debilitating ransomware attack, a client extended Acumera's store-level security services to the company's corporate offices — gaining proactive protection, monitoring, insight, logging, auditing and 24x7x365 network security support.

Acumera®

acumera.net
sales@acumera.net
512.687.7410

Introduction

After struggling to recover from a ransomware attack, the client extended Acumera's store-level security services to their corporate offices, gaining proactive protection, monitoring, insight, logging, auditing and 24x7x365 network security support. Acumera's Enhanced Security Services Enterprise (ESS Enterprise) security suite uses a zero-trust architecture, which is a security model based on the principle of maintaining strict access controls and not trusting any system or anyone by default.

Background

One of Acumera's long-time retail clients was the victim of a ransomware attack at their headquarters in summer 2020. Ransomware is a form of malware designed to encrypt files on a device, rendering these files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

While there are several known entry methods for ransomware, the company believes this particular attack originated with a user opening a malicious email that led to the execution of the Maze (formerly known as ChaCha) ransomware. The client's network was like the type used by many other small-to-medium-sized businesses — a self-managed, flat topology. As a result, the breached endpoint (in this case, an employee's PC) had full network access to all other endpoints. Once the first PC was compromised, the ransomware was able to spread through the network easily.

Within a few hours, much of the infrastructure had been encrypted and was effectively offline. The ransomware affected not only file servers but continued to move both laterally and vertically, encrypting critical files on other end-user desktops and servers. Ultimately, many key internal systems were affected, which impacted the company's daily operations.

While the retail locations themselves were not compromised during the ransomware attack, over 300 corporate systems were affected. However, due to certain corporate systems going offline, some business processes were disrupted for over 450 retail locations.

Alternatives

Although the company was able to eventually quarantine the offending systems, the process of bringing everything back online was slow and tedious. With limited technical and security resources, they found it impossible to restore or rebuild all critical systems in a reasonable time period. This left them with reduced visibility into their operations and limited actionable data to guide the business.

Leveraging their existing general-purpose IT vendors proved difficult, as they did not react with speed, ownership, or with a high degree of cooperation with other vendors. The company's next step was to consult with an expensive cybersecurity firm to assist with the ransom negotiation and forensics process. The negotiation was unsuccessful, and so the recovery process began.

Soon it was discovered that beyond encrypting critical business data, the ransomware had also exfiltrated information from their internal systems. Data exfiltration is a common practice of cybercriminals in order to extort additional money at a future date. For businesses with personally identifiable or patient medical information, this also results in significant reputation and customer experience risk.

Evidence also surfaced of other malware that has been in the network since 2018, which meant that traditional server restores could not be trusted. After weeks of being resource-constrained and trying to remediate the issues themselves, the company turned to their trusted security partner, Acumera.

Proposed Solution

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

Acumera had provided managed network security services for their retail sites for many years. While the client always felt confident with their site security, there had always been a lingering question about the overall cybersecurity strength of the corporate office. The client had even approached Acumera some time earlier about implementing its suite of services at their corporate offices, but other priorities prevented the project from proceeding. After the breach, however, leadership placed a much higher priority on cybersecurity, and Acumera was brought in to assist.

Acumera reviewed the network topology, interviewed team members, and went through an exhaustive discovery process to determine the client's challenges and goals. Working with the company's staff and other technical vendors, Acumera designed a comprehensive recovery, migration and protection strategy. Acumera delivered a custom quote and implementation timeline for their ESS Enterprise service, a suite of managed security services designed for corporate and regional offices.

Implementation

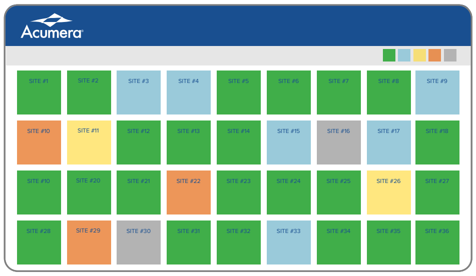
Using the patented MG™ Edge Security Device as its foundation, Acumera's ESS Enterprise is a defense-in-depth solution based on security best practices. It includes a variety of edge computing workloads, including external and internal vulnerability scanning, web filtering, edge and endpoint logging, endpoint detection and response and endpoint isolation. This comprehensive suite of services manages security from endpoint to edge and all points in between.

The client wanted to ensure they were starting with a clean slate and assurance that there were no back doors into their rebuilt network. As such, they implemented a parallel network and only migrated systems to the new network after they were rebuilt. During and after recovery, the entire original network was considered hostile and held outside of the security perimeter of the new network. With this enhanced security model, data is only allowed to flow outbound from the new network, and all traffic is inspected for indications of compromise with both firewall edge logging and intrusion detection.

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

External vulnerability scans support various compliance programs and help detect incorrect configurations before they become problematic. Internal vulnerability scans with a per-vulnerability threat score prioritize patching based not only on Common Vulnerability Scoring System (CVSS) scores but also the quantity of affected devices.

Systems on the new network take advantage of web browsing protected by category filtering, blacklists and whitelists. These technologies greatly reduce the ability for new malware to 'call home' to control-and-command servers. Although appliances such as switches, smart displays and IoT devices don't have interactive users, their internet access is limited to just the sites needed, and some devices, such as printers, are even restricted to only the local network.



🟩 🟦 🟨 🟧 ⬜

🟩 SITE #1	🟩 SITE #2	🟦 SITE #3	🟦 SITE #4	🟩 SITE #5	🟩 SITE #6	🟩 SITE #7	🟩 SITE #8	🟦 SITE #9
🟧 SITE #10	🟨 SITE #11	🟩 SITE #12	🟩 SITE #13	🟩 SITE #14	🟦 SITE #15	⬜ SITE #16	🟦 SITE #17	🟩 SITE #18
🟩 SITE #10	🟩 SITE #20	🟩 SITE #21	🟧 SITE #22	🟩 SITE #23	🟩 SITE #24	🟩 SITE #25	🟨 SITE #26	🟩 SITE #27
🟩 SITE #28	🟧 SITE #29	⬜ SITE #30	🟩 SITE #31	🟩 SITE #32	🟦 SITE #33	🟩 SITE #34	🟩 SITE #35	🟩 SITE #36

AcuVigil™ dashboard for visibility and management

Multiple, best-of-breed legacy solutions were replaced as part of the project, resulting in a simpler network that can fully be managed through Acumera's cloud-based AcuVigil™ dashboard. With management-at-scale capability, the AcuVigil dashboard promotes configure-once, deploy-everywhere workflows. Due to management efficiencies from a single-pane-of-glass management platform, the client is also generating additional ROI by reallocating internal staff to higher-value initiatives.

Conclusion

After deploying Acumera's Enhanced Security Services Enterprise solution, the client has seen significant efficiency increases through centralized network and endpoint visibility, monitoring, reporting and alerting. Moreover, their technology team detects and remediates network and security issues faster than before and has been able to minimize additional staffing needs through the extensive use of Acumera's 24x7x365 network operations center. Finally, by implementing a zero-trust architecture, the investors and leadership team now enjoy peace of mind knowing not only that their corporate network is protected by Acumera's ESS Enterprise security suite but their bottom line and reputation as well.

Reasons to Choose Acumera ESS Enterprise

Helps your IT team	Safeguards against breaches	Keeps your business running	Protects employee and customer data
Hand off processes to a team that specializes in securing networks and security monitoring	Protect your company from breach-related recovery costs of hundreds of dollars per compromised customer record	Reduce downtime, save thousands of dollars per hour of lost productivity and reduce reputation risk	Monitor for data patterns and data exfiltration and ensure privacy compliance (PII, PHI, HIPAA, etc.) with Acumera's security services

About Acumera

Acumera is the leading supplier of network operation, visualization and security services via orchestration of business, networking and security workloads in the cloud, near the edge and at the edge. Acumera fully secures single-site, multi-site, branch office and corporate office networks, point-of-sale (POS) systems, and IoT devices and safeguards sensitive data, maximizes uptime, and simplifies compliance.