Case Study:
Law Enforcement Agency

GDS helps a large sheriff's department strengthen the security of its IT Network and reduce the risk of a potentially devastating cyberattack.

GLOBAL DATA SYSTEMS

Law enforcement agencies, like many organizations in the public sector, face significant cybersecurity threats.

Hackers often target these agencies because they store sensitive data and cannot tolerate the disruption of a cyberattack. Yet many law enforcement agencies lack the skills, tools, and resources to combat today's cyber threats.

A large sheriff's office was attempting to manage its cybersecurity environment using off-the-shelf point products and in-house IT resources. With more than 800 users accessing the agency's network, the IT team was spread thin handling day-to-day administrative and support tasks as well as security events and alerts. They felt the agency would be served more effectively by outsourcing security to a managed services provider (MSP).

The agency asked Global Data Systems to propose a solution. GDS recommended a comprehensive program that emphasized its end-user, email, and advanced infrastructure security services. These fully managed solutions enable the sheriff's office to reduce the burden on its in-house IT team while reducing the risk of a cyberattack.

Challenge

Cyberattacks on law enforcement agencies have escalated in recent years as hackers seek to exploit weaknesses in the agencies' networks. Ransomware attacks are a particular threat because of the high risk of data loss and extended downtime.

A successful attack can threaten an agency's mission and service to the community and have a cascading impact on other critical services. Often, law enforcement networks are interconnected with other computer and communications systems, increasing the risk that an attack can spread throughout local government agencies.

Because organizations are increasingly reluctant to pay the ransom to recover data, cybercriminals are exfiltrating data before its encrypted and threatening to expose it if their demands are not met. If the personnel records of a law enforcement agency were exposed, it would put officers and their families at risk. Cybercriminals have also threatened to release the personal information of crime victims if the agency did not pay the ransom.

A ransomware attack could compromise digital evidence used in an investigation, such as data recovered from a suspect's mobile device. From a legal perspective, this could break the chain of custody such that the evidence cannot be used in court. Even if the data is ultimately recovered, cases can be compromised if prosecutors are unable to prove the evidence was not tampered with.

The sheriff's office recognized that these threats were too great to address with in-house resources. Additionally, the agency was concerned that its cybersecurity toolset had gaps that created vulnerabilities.

Solution

GDS uses industry-leading tools to protect more than 800 endpoints, firewalls, and servers on the sheriff's office network. These tools combine prevention, detection and response capabilities that leverage the power of cloud-based analytics to deliver maximum protection. Definition-based and polymorphic malware detection, file reputation analysis, and machine learning are capable of stopping the most advanced attacks.

All endpoints are protected by definition-based antivirus engines that are constantly updated with the latest threats. Custom, signature-based detection and blacklist enforcement provide additional security. Because the signature database is maintained locally on each endpoint, the solution does not require cloud connectivity for antivirus protection. This is a critical feature for deputies in the field who may not always have access to a reliable Internet connection.

GDS also scans emails coming into the sheriff's office to detect malicious links or attachments that could trigger a cyberattack. Email attachments are compared against a comprehensive database of known threats in real time. Malicious files are quickly and easily quarantined before they enter the agency's network without processor-intensive scanning. Over the three years GDS has managed security for the sheriff's office, hundreds of millions of files have been scanned.

The GDS tools continuously scan active connections, files, and IP addresses to identify malware and other threats. Continuous monitoring helps to uncover threats that have already entered the agency's environment and terminate any applications or processes that exhibit abnormal behavior.

When a threat is detected, it is automatically blocked or quarantined. If a device is compromised, the GDS team is alerted to investigate and take further action. **The GDS Network Operations Center (NOC) and Security Operations Center (SOC) uses powerful tools that provide granular visibility across the environment.** This makes it possible to quickly identify compromised endpoints and track file and device trajectories to determine the scope of the threat. GDS has successfully mitigated thousands of threats for the sheriff's office.

Results

Because all these tools are monitored and managed by the experts at GDS, the sheriff's office does not have to devote IT resources to endpoint and email security. The agency's in-house IT team can focus on other administrative tasks and strategic initiatives.

What's more, **GDS managed security services are fully customizable to meet each organization's specific requirements.**

The sheriff's office needed to give officers and detectives access to several websites that would normally be blocked, and the agency's IT team wanted the ability to manage the whitelist internally. Although GDS does not generally allow customers to make changes to its security appliances, GDS worked with the sheriff's office to develop a shared responsibility strategy that meets the agency's needs.

GDS meets with sheriff's office personnel biweekly to discuss data collected from the security appliances, support tickets that have been issued and resolved, and any concerns the agency may have. From a technical perspective, this gives GDS insight into the agency's operations and helps ensure the highest levels of security.

The GDS Customer Experience (CX) team is also involved in these discussions, documenting open action items, and organizing follow-up. The objective is to deliver the best possible experience for the sheriff's office.

For More Information:

Contact Us:
- getgds.com/contact-us
- linkedin.com/company/getgds

Call Us:
- 888-435-7986

Learn More About This Solution:
- Managed IT Security