ARCTIC WOLF

City of Sparks

PERSONAL | PREDICTABLE | PROTECTION

CASE STUDY

City of Sparks, Nevada

At a Glance

City of Sparks
(cityofsparks.us)
Fifth most populous city in Nevada famously known as a premier destination for special events in the Reno-Tahoe region

Challenges

- Repeated ransomware and phishing attacks that bypassed existing defenses
- Busy IT team lacked in-depth security expertise
- Without budget to build and maintain internal security operations center

Results

- 10X savings compared to building an internal security operations center
- 24x7 monitoring by security experts
- Experienced security team now part of extended staff

> "The Arctic Wolf SOC-as-a-service includes everything Sparks needs for a comprehensive security operations function. We looked at solutions from some of the largest IT security vendors and went with Arctic Wolf because it was easy to purchase and deploy, and was priced in a predictable way. To build the equivalent of the service internally would cost at least 10 times more."
>
> **— Steve Davidek,** IT Manager, City of Sparks, Nevada

Hybrid AI Protects the City of Sparks from Ransomware and Phishing Attacks

Sparks, Nevada is located in the beautiful Truckee Meadows between the Carson and Virginia mountain ranges, an hour's drive from Lake Tahoe. Just outside of Reno, it is the fifth most populous city in Nevada and one of the fastest growing in the state. Sparks is the closest metropolitan area to the Tahoe-Reno Industrial Center, home to Tesla Motors' Gigafactory.

Sparks has a lean IT team that supports the city's administrative offices and public services, including emergency first responders such as the police and fire department. The team is staffed with different functional experts, but lacks a dedicated security expert. Despite having all the essential security defenses in place, Sparks recently experienced repeated cyberattacks. The IT team realized that unless it developed greater security expertise, managing more point security products was not a scalable strategy. The team evaluated building a security operations function in-house versus purchasing the Arctic Wolf SOC-as-a-service. Comparing the two options, Sparks realized that selecting Arctic Wolf brought a 10X savings over doing it internally, once costs of staff, software, and hardware were considered.

Cybercriminals Target First Responders

The Sparks police department experienced a ransomware attack that could have crippled the department if not for the swift action of the IT team. Once the team was alerted to the attack, it sought to identify all compromised endpoints and restore the systems from backups.

Though a crisis was averted, the incident was hugely disruptive, and the team was not sure what changes to implement to protect the police department and the entire Sparks workforce from falling victim to future attacks.

Soon after the ransomware attack, cybercriminals targeted police officers through spearphishing email attacks. Leveraging social media and other publicly available information, the cybercriminals also launched attacks targeting the highest levels of city government. The IT staff realized that it lacked the expertise to investigate these security issues and respond to them in a timely manner.

What frustrated the IT team was that these attacks bypassed its existing defenses from leading firewall-, email security gateway-, and web security gateway-provider Barracuda Networks. It would have been manageable if the defenses were able to detect and contain the attacks, but multiple attacks got through. Each attack was highly disruptive, and the lean IT team was not able to absorb the disruption while still providing the high level of service expected by the city's staff.

Build vs. Buy

The Sparks IT team compared the option of building their own security operations center (SOC) to purchasing a comprehensive service from Arctic Wolf. An internal security operations team would offer a better understanding of Sparks' IT environment and be more responsive.

On the downside 24x7 coverage required a team of several people with extensive security expertise, and a SIEM, which is notoriously expensive to purchase and maintain. Hiring a team of security analysts, purchasing the software, and then getting everything up and running could easily take six to 12 months.

Buying a SOC service was a much more attractive option since it could be deployed quickly and at far less cost than an in-house SOC. A SOC-as-a-service is a comprehensive solution that requires no purchase of software or hardware. It includes a SIEM, set up, and is managed by seasoned security experts who become an extension of the internal IT team. After careful evaluation, the Sparks IT team selected the SOC-as-a-service from Arctic Wolf.

Arctic Wolf with Hybrid AI Delivers

The time to value for Arctic Wolf exceeded expectations within a week of installation. The Sparks IT team was notified of passwords transmitted to websites in the clear, as well as more phishing attacks on police and fire department personnel. The Sparks IT team was also provided specific endpoint mitigation recommendations to quarantine compromised laptops and desktops. This removed the guesswork from how the team addressed security lapses.

One of the key technologies of Arctic Wolf's SOC-as-a-service is Hybrid AI, the combination of human intelligence and machine scale that delivers 10X better threat detection with 5X fewer false positives. Great cybersecurity starts with data, and the volume of data that needs to be processed is now beyond the capacity of human beings. The key to AI is the data it uses to learn, but one of cybersecurity's biggest challenges is handling false positives, i.e., bad data. Therefore, human involvement is critical when AI is used for cybersecurity.

The Arctic Wolf SOC-as-a-service is more than just a detection and response service for the Sparks IT team. The team works hand-in-hand with the Arctic Wolf Concierge Security™ Team (CST), which is considered an extension of Sparks' internal IT team. The CST has helped Sparks close up holes in its firewall and even provided the team data and information to fix an issue with its internet service provider. The CST is not just there for ransomware and phishing attacks, but for all matters related to cybersecurity.

ARCTIC WOLF

SOC2 Type II Certified

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

Contact Us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com