Isolating a Security Incident and Protecting the Network

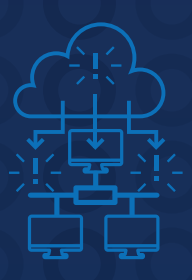
The worst has happened- how do you contain the damage?

A large media company must be accountable to its advertisers, customers and users
TO PROTECT THEIR INFORMATION.

Major data security breaches that make the news damage a company's brand, and can lead to catastrophic financial loss, customer mistrust and legal penalties. Once malware has infiltrated a network, the effects can be incredibly damaging.

NO ORGANIZATION WANTS TO BE THE NEXT HEADLINE,
so when this company found evidence of a possible malware infiltration, it took immediate action.

With this service, Optiv:



Optiv provided immediate incident response services, scouring the network for malicious code.

Once all information was collected, Optiv analyzed it for malware.

After isolating the incident, Optiv provided recommendations to help prevent a future attack.

Optiv's incident response services provided this client with many benefits, including:

Isolated incident:
Optiv stopped the attack and isolated its damage from the network.

Maintained credibility:
by isolating the incident with no data loss, the company kept its reputation intact.

Knowledge:
the client learned how and why the breach happened.

Remediation:
armed with information about the attack, the client could immediately make changes to improve security.

Learn more by downloading the Client Spotlight at www.optiv.com/resources/library or contacting references@optiv.com.