

A photograph of a classical federal government building with a large eagle sculpture on top. The image is overlaid with a semi-transparent teal banner containing text.

## Case Study: Federal Government Sector

**“Since we deployed ArcSight TRM, we have been able to quarantine all cyber-security attacks before any major damage has taken place.”**

Systems Engineer, Federal Government Customer

### Impact Highlights

- Dramatically reduced response times via a clearly defined, auditable response process
- Quarantined all cyber-security attacks before any major damage could occur
- Gained greater command and control of cyber-security response process

### Customer's Challenge

Like any organization with a complex, network-centric environment, this federal government customer struggled with an increasingly challenging and pervasive cyber-security landscape. Once the cyber-security team identified incidents and potential threats on the network, responding was a tedious, time-consuming process.

A senior engineer would typically respond by first consulting a list of identified infected nodes, but by the time he found and quarantined them, additional lists of newly infected nodes had already been created.

“Just keeping track of the network configuration changes we were putting in place to stop an attack was a challenge,” said the systems engineer in charge of network management tools. The customer turned to ArcSight Threat Response Manager™ (TRM) to decrease response time and institute a clearly defined, repeatable and auditable response process.

### The ArcSight Solution

The unique technology behind ArcSight TRM inherently communicates with and leverages existing network infrastructure devices including routers, switches, firewalls, VPNs and WAPs. As a result, the solution does not require any clients or agents to be deployed on the customer's network. The federal government customer was able to easily operate ArcSight TRM without making any changes to its existing network infrastructure and desktop environment.

Moreover, thanks to the agile architecture in ArcSight TRM, the organization was able to place the solution anywhere on its network, enabling a quick and easy deployment. “Putting together the documentation for the implementation was actually more challenging than the implementation itself,” noted the government employee responsible for deploying ArcSight TRM.

Since the implementation, the customer's response process has dramatically improved. Now, infected nodes are located and isolated from the network within seconds, before they have a chance to propagate. With ArcSight TRM, the organization's ability to respond is so effective that all cyber-security incidents are nipped in the bud.



before anything serious can happen. “Since we deployed ArcSight TRM over a year ago, we have been able to quarantine all cyber-security attacks before any major damage has taken place,” said the system engineer.

The customer is also benefiting from the “investigate” feature included with ArcSight TRM. This feature quickly tells the user the exact location and system details of any node on the network. This allows the customer to regularly investigate sources of suspected malicious traffic, enabling the network operations center (NOC) to weed out false positives before actually quarantining nodes.

### The ArcSight Impact

ArcSight TRM has allowed this federal government customer to gain greater command and control of its cyber-security network response process. By reducing the complexity of the response procedure, members of the IT security team are better able to perform their jobs. Senior engineers, for instance, now have the freedom to architect and engineer, rather than spending all their time chasing viruses and worms across the network.

The federal government customer is a strong example of an organization that has embraced new technology to replace manual, labor-intensive processes. The customer has even held several demonstrations for other federal departments to evangelize its new approach to cyber-security incident response.

### About ArcSight

ArcSight, a leader in Security and Network Information Management, delivers mission-critical solutions for security, network and IT operations that enable enterprises to turn operational data into action. ArcSight solutions address today’s complex enterprise networks that span multiple organizations and corporate business initiatives. By comprehensively collecting, analyzing, managing and responding to security and network data, ArcSight solutions mitigate information risk for real-time threat management, compliance reporting and automated network response. ArcSight’s customer base includes leading global enterprises, government agencies and MSSPs.



#### ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA  
[www.arcsight.com](http://www.arcsight.com)  
email: [info@arcsight.com](mailto:info@arcsight.com)

Corporate Headquarters: 408 864 2600  
EMEA Headquarters: +44 870 351 6510  
Asia Pac Headquarters: 852 2166 8302

© 2007 ArcSight, Inc. All rights reserved. ArcSight, ArcSight ESM and ArcSight TRM are trademarks of ArcSight, Inc. All other product and company names may be trademarks or registered trademarks of their respective owners. 03/07