

# State of Oklahoma

## State of Oklahoma Saves Millions of Dollars with Centralized Endpoint Security Solutions from Symantec

The State of Oklahoma needed to standardize endpoint protection across 135 agencies and gain a centralized ability to monitor endpoint security. It chose solutions from Symantec and Intuitive Technology Group, a Symantec Platinum Partner. Results include zero significant disruption from malicious code since deployment, \$2.3 million in projected five-year savings for taxpayers, six person-years in IT staff productivity reclaimed by centralizing security, and on-time deployment for 28,000 endpoints in six months.



**“Consolidating the State of Oklahoma’s spending on IT security solutions and standardizing on Symantec Endpoint Protection will save taxpayers a projected US\$2.3 million over five years.”**

Mark Gower  
Chief Security Officer  
State of Oklahoma

### Transforming services

Paperless, fast, cost-efficient, easy—these are qualities that people want in their government services, and the State of Oklahoma is delivering them. A [long list of awards](#) shows that Oklahoma is emerging as a national leader in eGovernment excellence.



### ORGANIZATION PROFILE

**Site:** [www.ok.gov](http://www.ok.gov)  
**Industry:** Public Sector  
**Headquarters:** Oklahoma City, Oklahoma  
**Employees:** 35,000, including part-time

### KEY CHALLENGES

The State of Oklahoma needed to centralize and standardize endpoint security and gain an organization-wide view of potential security threats.

### SOLUTION

- Symantec Endpoint Protection
- Symantec DeepSight Security Intelligence
- Symantec IT Management Suite
- Symantec Business Critical Support

### BENEFITS

- No significant disruption from malicious code since deployment
- \$2.3 million in projected five-year savings for taxpayers
- Six person-years in IT staff productivity reclaimed by centralizing security
- Six-month target of deployment to 28,000 endpoints accomplished on-time

### SYMANTEC PLATINUM BUSINESS PARTNER

Intuitive Technology Group  
([intuitivetech.com](http://intuitivetech.com))  
Expert Competencies: Endpoint Management, Mobility

One award-winning application helps government staff analyze legislation. Another sends disaster alerts to citizens and helps them report any disaster relief fraud. Another turns the governor's process of making hundreds of appointments to boards and commissions into a paperless digital workflow, saving taxpayer dollars and speeding results.

To support services like these, Oklahoma Chief Security Officer Mark Gower and his team have a mission: secure the infrastructure and information that the government depends on.

It's a daunting challenge. "Oklahoma has 135 state agencies, and there are 30,000 endpoints spread across all 77 of our state's counties," Gower says. "We also need to scan and protect 3,500 servers, about 40 percent of which are virtualized."

Gower's team gathered these details in an initial security assessment. "Security was decentralized," Gower recalls. "Across the 135 agencies, there was a wide variety of antivirus protection, and it was not consistently applied—in some cases there was no protection."

### Gaining a central view

The security team wanted to standardize on a single solution that combined anti-malware, anti-spam, and intrusion prevention, along with application and device control. The team evaluated the state's different solutions and chose Symantec™ Endpoint Protection.

"Some agencies said, 'we already have antivirus,' and we told them that antivirus alone does not offer the level of protection they needed to be custodians of a constituent's data," Gower explains. "The state needed multiple layers of protection that could be centrally monitored. There had never been an end-to-end view showing how security events at one agency could affect another."

Central coordination was critical, Gower adds. "With the application of Symantec Endpoint Protection, we were able to develop what we now call the State of Oklahoma Cyber Command Services. This enables us to have instantaneous real-time views into what's happening from the desktop all the way back to the network layers, and it gives our security operations center (SOC) analysts the ability to identify, detect, and defend all the State IT assets."

In order for endpoints to be well-secured, they also must be well-managed. That's why the State of Oklahoma chose Symantec™ IT Management Suite powered by Altiris™ technology. It enables the IT team to remotely deploy, patch, take inventory and manage the lifecycle of the state's far-flung endpoints.

"If you are going to expect to have some level of security posture for your organization, you have to be able to understand what's on your endpoints," Gower explains. "How do you get patch management? How do you deploy applications? How do you inventory what's out there? These are important questions."



**“I don't believe the State of Oklahoma could have been truly successful without Symantec as a trusted partner that could bring in an integrator such as Intuitive Technology Group. Intuitive does this kind of roll-out daily, and they helped us achieve our mission with a very small impact on the footprint of each site.”**

Mark Gower  
Chief Security Officer  
State of Oklahoma

### Turning worldwide intelligence into protection

Once endpoints are well-managed, antivirus technology isn't enough to defend them, Gower notes because more than half of today's threats are designed to defeat signature-based detection. This is what Symantec has observed in the past year using its Global Intelligence Network, which gets an overview of threats from more than 64.6 million attack sensors that monitor networks worldwide, as well as the opportunity to scan more than 8 billion emails and 1.4 billion web requests a day. Symantec also maintains a database of over 45,000 vulnerabilities covering 15,000 vendors.

Oklahoma taps this network and database by subscribing to Symantec DeepSight™ Security Intelligence. "We have more than 4,500 applications, and there's no way that we could subscribe to 4,500 vendor newsletters to get security information on them," Gower says. "With Symantec DeepSight, we have a trusted partner monitoring for vulnerabilities and recommending how to prioritize our resources for patching or other remediation. We also use DeepSight to evaluate vulnerabilities in any proposed application."

### Reputation and behavior used to shut down threats

Symantec Endpoint Protection directly integrates with the Symantec Global Intelligence Network to provide layers of protection beyond antivirus. One layer is provided by Symantec Insight technology, which uses worldwide user experience to identify a file's reputation and block malicious files based on risk. This effectively protects against rapidly mutating threats and reduces scan overhead by scanning only at-risk files.

Another layer of protection is provided by Symantec SONAR technology, which monitors file behaviors to identify suspicious activity and stop zero-day threats. Having monitored millions of applications, SONAR determines whether a given application's actions are good or bad, stopping bad actions in their tracks. More than half of the overall threats blocked by Symantec in the past year have been stopped by proactive, non-signature based technologies such as these.

"SONAR and Insight give us the ability to triage," Gower says. "They feed back to our central console information on where a threat is and how many different agencies may be impacted by the same threat."

### Detecting advanced persistent threats

The new security infrastructure enabled one of the state's security operations center analysts to detect a particular attack on an agency's web server that would probably not have been detected in the prior security environment. "We were able to identify and mitigate the threat within minutes of its attempt to establish a foothold on that system," Gower says. "It may have been a beachhead for attacking us internally."

Only centralized monitoring from the security operations center along with threat correlation and prioritization made possible by solutions from Symantec and other vendors make this kind of proactive detection and prevention possible, Gower adds. "There has been no significant disruption from malicious code since we deployed Symantec Endpoint Protection," he notes. The new solution now protects more than half of the state's 135 agencies and is being introduced to 15 more each year, with the statewide rollout to be complete in about four years.

### Saving US\$2.3 million and six person-years

"Consolidating the State of Oklahoma's spending on IT security solutions and standardizing on Symantec Endpoint Protection will save taxpayers a projected US\$2.3 million over five years," Gower says.

The initiative also saves IT staff time. In a survey of 1,500 people responsible for state IT, 480 indicated that they had some IT security responsibilities. "We now conduct those same operations with 18 people," Gower says. "So instead of needing to pull them off a mission-critical application for a security event, they can stay focused on their core jobs."

Centralizing security for the state with 18 people reclaims as much as six person-years annually in staff time that can be focused on higher value projects.

### Simplifying deployment with Symantec partners

To get assistance in rolling out the solution, Oklahoma engaged Intuitive Technology Group, a Symantec Platinum Partner.

“For phase one, we had just six months to deploy to 28,000 endpoints or about 80 percent of our total, and we made it,” Gower says.

“We were able to meet our aggressive timeline using the software inventory, removal, and deployment tools in Symantec IT Management Suite and Endpoint Protection to accelerate the implementation.”

Gower continues: “I don’t believe the State of Oklahoma could have been truly successful without Symantec as a trusted partner that could bring in an integrator such as Intuitive Technology Group. With this consolidation, we inherited almost every type of IT environment known to humankind. We would come to an agency without really knowing what environment we would find. Intuitive does this kind of roll-out daily, and they helped us achieve our mission with a very small impact on the footprint of each site.” “I don’t believe the State of Oklahoma could have been truly successful without Symantec as a trusted partner that could bring in an integrator such as Intuitive Technology Group. With this consolidation, we inherited almost every type of IT environment known to humankind. We would come to an agency without really knowing what environment we would find. Intuitive does this kind of roll-out daily, and they helped us achieve our mission with a very small impact on the footprint of each site.”

### IT for the people

There’s a new kind of challenge that IT departments face, Gower notes. “IT is now a utility—users flip the switch, they expect IT services to be there, and they must be secured,” he says. “We need to enable whatever services the state wants to deliver, and strategic partnerships with a company such as Symantec make this possible.”

The benefits of a secure and reliable state IT system can be far-reaching, Gower notes. “School systems, cities, and county governments that struggle to provide their own IT services to their constituents should be able to utilize the state’s resources,” he says, “and that is a goal we are on our way to achieving.”

**“IT is now a utility—users flip the switch, they expect IT services to be there, and they must be secured. Strategic partnerships with a company such as Symantec make this possible.”**

Mark Gower  
Chief Security Officer  
State of Oklahoma

### Intuitive Technology Group

Helping to Secure Data, Improve Productivity, and Provide IT Staffing for Your Business.

Intuitive Technology Group is a Symantec Platinum Partner offering custom IT solutions in cloud, endpoint management, mobility, and security, while enabling customers with professional IT consulting, managed services and IT staffing.

Intuitive’s primary industry focus is on Healthcare, Federal, State and Local Government and Education (FED/SLED), Financial, and Technology sectors. Please visit [www.intuitivetech.com](http://www.intuitivetech.com)

### For more information:

Contact your local Symantec Sales Representative or Business Partner, or please visit: [www.symantec.com/endpointprotection](http://www.symantec.com/endpointprotection)

### Symantec World Headquarters

350 Ellis St.  
Mountain View, CA 94043 USA  
+1 (650) 527 8000  
1 (800) 721 3934