



## Idaho State Tax Commission

### Customer profile

Headquartered in Boise, Idaho, the Idaho State Tax Commission administers Idaho's tax laws

### Industry

State government

### IT environment

The commission's network supports 700 nodes. Of these nodes, ten percent are servers, thirty percent are laptops or tablets, and the remaining nodes are desktops. User endpoints run Microsoft XP, and servers operate with Windows 2003.

### Challenges

A newly deployed network infrastructure required robust security.

### McAfee solution

Idaho State Tax Commission has deployed McAfee Network Security Platform, Network Access Control, Vulnerability Manager, Total Protection (ToPS) for Endpoint Advanced, ePolicy Orchestrator (ePO), and McAfee Site Advisor.

### Results

- Identifies vulnerabilities and blocks threats
- Delivers reliable endpoint protection
- Enables compliance with NIST security guidelines
- Supports commission's "defense in depth" security strategy
- Helps to increase security awareness among network users

## Idaho State Tax Commission Turns to McAfee to Embed Security in New Network Infrastructure

Headquartered in Boise, the Idaho State Tax Commission administers the state's tax laws, maintaining five satellite offices in Twin Falls, Pocatello, Idaho Falls, Lewiston, and Coeur d'Alene, each of which has approximately 20 employees. The headquarters and satellite offices are connected via a T1 line. When Glenn Haar, the Commission's IT Resources Manager, embarked on a network infrastructure upgrade, it involved both hardware and software.

"We ended up replacing every router, switch, and terminating device," explains Haar. "And our strategy was to build security in from the beginning rather than add it on."

Of course, a network project of this scope can be extremely disruptive to everyday business activity. "When you take on a project of this kind, nobody truly understands what is going on behind the scenes," says Haar. "You must ensure that everyone can continue to get their work done. So we decided to build a new network alongside the old one and cut over piece by piece. This tactic has been quite successful in minimizing the impact to our users."

### A McAfee shop in the making

Haar and his team began their security upgrade process by replacing the existing network intrusion detection system with a more comprehensive intrusion prevention system. They evaluated several vendors' products, and ultimately chose McAfee Network Security Platform due to its strength in blocking unwanted and peer-to-peer traffic.

"The next step involved our acquisition of McAfee Network Access Control, (NAC)" comments Haar. "NAC was less expensive than other solutions we evaluated and easier to manage. We also purchased McAfee Vulnerability Manager to identify risk exposures and policy violations. Suddenly we realized that we were becoming a complete McAfee shop."

To further enhance protection, Haar wanted to address endpoint security, and began another evaluation process with multiple vendors. "When I spoke with McAfee, they proposed a suite that made economic sense and also provided growth for future requirements," recalls Haar. The endpoint upgrade was McAfee Total Protection (ToPS) for Endpoint Advanced.

With senior management's support, Haar decided to standardize on McAfee for the new network's security infrastructure. "We could have spent a lot of time evaluating every point product out there," says Haar. "But we decided that standardizing the infrastructure with one vendor made the most sense. All the McAfee products are integrated, and we'll save time and effort in the long run by consolidating with one security vendor."

### Big plans, small steps

Haar has learned to test any new security technology in a small pilot before deploying it across the entire organization. "It just makes sense to deploy to a small group first, make sure they're comfortable with the new software, and then move on to another small group," emphasizes Haar. "You learn a lot with each step in the process. Eventually, you get to the point where the deployment is so clean that no one even realizes you're doing it." Haar also takes care not to deploy anything new between January and April, the Tax Commission's busiest time.

Using that phased deployment scenario, the Commission has deployed McAfee VirusScan® Enterprise and ePolicy Orchestrator (ePO™). The IT group also learned that installing and implementing NAC was not difficult; success was driven by the users embracing the culture change that was introduced through the technology. NAC's enforcement rules tightened the security on the network by requiring all desktops and laptops to be current. "Users found if they pulled their laptops off the network for too long, they would have difficulty gaining access," explains Haar. "They soon realized it was best to sign on and receive updates on a regular basis – this eliminated any potential issues down the road."

"Once we get into the tax season, we shut everything down," says Haar. "First, we don't want to interfere in any way with the work that needs to be done. And second, no one has the time to be trained on anything new."

Haar and his team are also planning a pilot of McAfee Remediation Manager and McAfee Policy Auditor. Those two products will help the agency in its efforts to meet National Institute of Standards and Technology (NIST) guidelines for server configuration.

"We're going to install it in pilot form before full deployment" says Haar. "Our goal is to configure a server to NIST specifications with Remediation Manager and test all user applications in this environment. When the pilot concludes, we'll gradually migrate our 70 servers into a NIST environment. Remediation Manager will give us control of that process."

### Defense in depth

Haar subscribes to a security philosophy that finds its roots in an information security strategy originally developed by the National Security Agency (NSA). The NSA adapted a military strategy that aims to delay rather than prevent the advance of attackers. In its practical application for information security, this entails the use of "defense-in-depth", multiple layers of protection placed throughout an IT infrastructure.

"Defense-in-depth is a very, very old concept," Haar explains. "It's layer after layer of protection. And it's why even though we're primarily a McAfee shop, we run additional products. It gives us a different look at the same things and that's an important component of defense-in-depth."

Complementing Haar's defense-in-depth strategy is a five tier security model—risk assessment, prevention, detection, response, and awareness. McAfee products play a role in every tier. For example, McAfee Vulnerability Manager anchors the risk assessment tier. "If you can't see it" says Haar, "you can't stop it. It's pretty simple." Likewise, McAfee Site Advisor, a product that provides worry-free web browsing and risky web site blocking, has become a powerful tool for boosting awareness.

"Awareness is everyone's responsibility," Haar says. "And McAfee Site Advisor is really one of the few things that we can put in front of a person that helps increase their awareness."

"Information is an asset," Haar concludes, "and securing that asset is simply a cost of doing business. It's an opportunity cost. And if you can't afford to secure your assets, you can't afford to have them."

---

*All the McAfee products are integrated, and we'll save time and effort in the long run by consolidating with one security vendor.*

Glenn Haar  
IT Resources Manager  
Idaho State Tax Commission

---

