Case Study

State of Alaska

Customer profile
Largest, northernmost state in the US.

Industry
State and local government.

IT environment
Approximately 20,000 workstations and almost 5,000 servers spread across three major urban areas, as well as many rural communities.

Challenge
Efficiently and effectively secure citizen data across data centers, endpoints, and networks for 16 state agencies as well as rural citizens—all while cutting security costs and managing future cost projections.

McAfee solutions
Enterprise License Agreement for McAfee solutions, providing desktop, server, data, network, email, and web protection. Solutions include:

- McAfee® ePolicy Orchestrator® software.
- McAfee Endpoint Protection—Advanced Suite.
- McAfee Database Activity Monitoring.
- McAfee Enterprise Mobility Management.
- McAfee Enterprise Security Manager.
- McAfee Total Protection™ for Data.
- McAfee Network Security Platform.
- McAfee Email Gateway and McAfee Web Gateway.
- McAfee SaaS Email Protection.
- McAfee Risk Advisor.
- McAfee Application Control and McAfee Change Control.
- McAfee Management for Optimized Virtual Environments (McAfee MOVE).

Consolidating on McAfee Saves the State of Alaska $3.8 Million

Alaska is the largest US state in area and larger than 18 sovereign countries. It is also the least densely populated of the 50 United States, with approximately 723,000 citizens. In addition to all the standard state government services, the State of Alaska provides communications services—including phone, television, and radio—to the majority of its rural communities. The state's Department of Administration manages the entire statewide area network for all 16 Alaska state agencies as well as sub-agencies and state corporations. Within the Department of Administration, the Alaska State Security Office (SSO), part of the department's Enterprise Technology Services (ETS) group, is responsible for ensuring the security of this network and the approximately 20,000 workstations, 5,000 servers, and terabytes of Alaskan citizens' information associated with it.

Staying Ahead of Constantly Changing Security Landscape With Limited Budget

"Covering such an immense geographical area with extremely remote communities definitely compounds our security challenge," explains Darrell Davis, chief security officer for the State of Alaska. "However, our biggest security obstacle is the same one facing most, if not all, state governments—namely, trying to stay abreast of the ever-morphing security landscape in the face of limited budgets that must be projected 18 to 24 months in advance."

Like many organizations, the State of Alaska chose the "industry-best" path, trying to implement what they believed to be the best of numerous security tools, but Davis and his staff of seven additional SSO full-time employees found it impossible to maintain and keep current these various security systems, let alone obtain real-time, actionable information from them. Consequently, the state began searching for a better security approach. Already consolidating vendors in other areas and pooling resources under ETS to achieve economies of scale, the state wanted to extend this model into the realm of security. In addition, the state placed high priority on centralized management so that, as Alaska SSO Security Analyst Daniel Wolf puts it, "We wouldn't have to continually throw resources at managing a bunch of disparate systems and trying to piece them together to get intelligent information out of them."

A More Cohesive Security Approach and True Force Multiplier

After outlining specific criteria for security functionality, the State of Alaska solicited multiple major security vendors for proposals. In addition to centralized management, factors for augmenting or replacing the state's existing security functionality included: mobile device management, security for virtual environments, database monitoring, application whitelisting and change control, more advanced risk analysis, security information and event management (SIEM), and network access control. After evaluating vendor responses, the state chose to completely overhaul its security approach, replacing their current solution set of solutions from seven vendors with an enterprise license agreement for multiple McAfee® software and hardware solutions. All the McAfee solutions are integrated in a unified security approach through the Security Connected framework and managed centrally with the McAfee® ePolicy Orchestrator® (McAfee ePO™) central management console.

Results

- Saved a projected $3.8 million and improved operational and team efficiency.
- Dramatically improved security posture without increasing headcount.
- Allowed for greater budget predictability with the flexibility to adapt and grow security as needs change.

> *" ... what's distinctive about McAfee is that each of these solutions works in concert with and amplifies the effectiveness of the other solutions—plus, with [McAfee] ePO, they can all be managed with a single pane of glass. The end result is a true force multiplier."*
>
> —Darrell Davis
> Chief Security Officer
> Department of Administration
> State of Alaska

"Each of the major McAfee components in and of itself provides critical security functionality," confirms Davis. "However, what's distinctive about McAfee is that each of these solutions works in concert with and amplifies the effectiveness of the other solutions—plus, with [McAfee] ePO, they can all be managed with a single pane of glass. The end result is a true force multiplier."

Millions of Dollars in Cost Savings, Plus Flexibility and Predictability

"We calculated that partnering with McAfee saves the State of Alaska $3.8 million over what we would have spent during the next three years," confirms Davis. Consolidation of multiple security vendors reduces costs in multiple areas, from contract management through technical administration. For instance, the state no longer has to spend time negotiating contracts with many different security vendors, and the cost of training and maintaining security solutions is considerably reduced. The state also benefits from additional purchasing power; instead of being a small customer to multiple vendors, it is now a large, important customer to a single vendor with McAfee.

"Furthermore, an enterprise license agreement with McAfee enables us to accurately project security expenditures for the next six years, as well as giving us the flexibility to adapt and grow our security as needs change over time," adds Davis. "The ELA also eliminates the time, hassle, and cost of administering proposals every time the state needs to add new security functionality."

"We fully expect to roll out all of our acquired McAfee security solutions, and, thanks to McAfee ePO, to manage them all efficiently, with the same staff we already have in place," attests Davis. Previously the eight full-time employees of the Alaska State Security Office had a difficult time managing less than half that many disparate security systems. "With McAfee, we are able to obtain vastly improved security without having to increase manpower," says Davis.

Enhanced Security Posture through Integration

The integration of McAfee solutions into a cohesive management monitoring and reporting system dramatically improves the State of Alaska's overall security posture across its network, systems, and data. For example, McAfee Network Threat Behavior Analysis software augments the state's McAfee Network Security Platform intrusion prevention appliance so that a security analyst looking at the McAfee ePO console can easily determine the severity and priority of an alert triggered by McAfee Network Security Platform. Add to these two solutions McAfee Vulnerability Manager, and the analyst can immediately discern which systems are vulnerable to the threat and which are not—all from the same console. "Having the three solutions working together in concert expands our perception of a potential threat and puts it into context so that we can prioritize it and quickly respond with the appropriate action—whether that means immediate remediation, mitigation, or doing nothing," describes Alaska SSO security analyst Daniel Wolf.

McAfee Global Threat Intelligence (McAfee GTI), a cloud-based, real-time reputation service, also enhances the data aggregated in McAfee ePO. "Thanks to McAfee GTI, I can take a suspect IP address and find out with just a few clicks in [McAfee] ePO who or what has been associated with that IP address in the past," explains Wolf. Before implementing McAfee solutions, he had to manually track down that type of information. "The upshot of having integrated solutions, [McAfee] GTI, and central management is an increased ability to achieve situational awareness and remediate with countermeasures already in place. We are already using the McAfee solutions to deal with zero-day and other threats before they become major issues," says Wolf.

Long-Term Partner for Long-Term Stability

The State of Alaska has rolled out a handful of McAfee solutions in its data center in Anchorage and is in the process of deploying several more McAfee solutions? As issues arise, SSO administrators have been extremely pleased with McAfee Platinum Support. "Every time we have had an issue, McAfee has responded rapidly and resolved the issue," says Wolf. "McAfee Support engineers have gone beyond assisting with the issue, even taking time to point out various features and operations that enhance the system in question."

"When we went looking for a new security approach, we focused on finding a partner, not just a solution, because long-term stability is absolutely critical, especially for security," concludes Davis. "We wanted a vendor that is mutually vested in securing our enterprise and will give us the attention we need. We believe we have found that kind of partner in McAfee."

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.