CASE STUDY

State Agency Bolsters Endpoint Protection

Security team accelerates time and mitigates risk

California Department of Water Resources

Customer Profile
US state government agency

Industry
Government

IT Environment
16,000 endpoints—4,000 in the department plus 12,000 across 29 other departments

With help from McAfee® Endpoint Security and an adaptive, integrated security approach to securing the threat defense lifecycle, this critical California state agency has dramatically improved its security posture now and in the future.

As the largest department within the California Natural Resources Agency (CNRA), the California Department of Water Resources (DWR) provides technology infrastructure-as-a-service to the entire Agency. DWR Chief Information Security Officer Richard Harmonson and his security team purchase, deploy, and provide multitenancy security solutions across the CNRA's 30 departments and their combined total of 16,000 endpoints.

Protecting the Endpoint Against Cyber Threats

According to Harmonson, nine out of 10 cyber threats experienced by the DWR enter via its users' desktops. "Our previous endpoint protection was adequate but rather two dimensional, the typical antivirus product that we've seen for the past two decades," says Harmonson. "We knew we needed a higher level of protection. We wanted more in-depth security that prevents more incidents—and when an incident does occur, provides the tools to react and remediate faster and more easily."

In addition, the DWR never felt that its legacy antivirus vendor was truly engaged and invested in the organization's success. "This eventually hit home when we had a malware incident and had to hunt down the vendor to help remediate it," notes Harmonson.

Reduced Operational Overhead and an Active Partner

Not long ago DWR decided to displace several of its security vendors with a host of McAfee products, all of which are part of the McAfee integrated security platform. "Compared to integrating a bunch of products from different vendors, the McAfee integrated security ecosystem reduces operational cost, both in dollars and man-hours," notes Harmonson. "A single point of contact for multiple solutions simplifies administration and dramatically reduces time to resolution—that is, if you have an excellent relationship with that vendor."

"We have an innovative, courageous, fast-moving CIO who is not afraid to throw out existing technology and vendors if they are not doing the job they are supposed to do," adds Harmonson. "With McAfee, we felt from the beginning—and it's been validated since—that we have a true, active partner who can help us meet our security objectives, not just pay lip service to them."

Greater Visibility and Less False Positives with McAfee Endpoint Security

Lack of visibility across endpoints and a very high false positive rate with its legacy endpoint protection drove DWR to implement McAfee Endpoint Security first among its McAfee deployments. The DWR information security team initially rolled out McAfee Endpoint Security version 10.5 across all 4,000 end-user physical devices within DWR and will deploy it across the remaining CNRA departments in the coming months, and eventually across virtualized servers as well.

"Visibility and the need to understand what is happening in our environment topped my lengthy list of initiatives," states Harmonson. "Our prior product had a much more limited perspective than McAfee Endpoint Security, which caused it to produce a phenomenal number of false positives. Validating whether each was a real concern or not was extremely time consuming and too frequently we had to call the vendor."

Challenges

- 90% of threats enter through users' desktops
- Safeguard PII and services for California citizens
- Reduce operational burden on security staff

McAfee Solution

- McAfee Advanced Threat Defense
- McAfee Complete Endpoint Threat Protection
- McAfee Endpoint Security
- McAfee Endpoint Threat Defense and Response
- McAfee Professional Services

Results

- Faster response and remediation thanks to better-informed decision making
- Risk mitigated and stronger security posture
- Greater visibility across endpoints and much fewer false positives
- More granular control over endpoint environment
- Highly supportive, trusted security partner

Today, without having to call McAfee or anyone else, Harmonson's team can see exactly what the threat did—for instance, what it changed in the registry or how it modified specific files—and then quickly validate the concern and discern what action, if any, to take. "With McAfee Endpoint Security, we remediate faster, have less business disruption, make better decisions, and protect neighboring workstations and our overall environment—instead of focusing all our attention on an infected workstation while another one gets hit," explains Harmonson.

Improved Protection and Detection Plus Highly Granular Control

"Since we rolled out Endpoint Security, we have been detecting and blocking threats we didn't see before," notes Harmonson. Much of the improvement in detection results from the Real Protect technology in McAfee Endpoint Security. Real Protect uses machine learning rather than manual intervention or signatures to stop difficult-to-detect malware like ransomware, and reduces manual intervention by automatically unmasking, analyzing, and remediating hidden threats. The DWR also uses the Dynamic Application Containment functionality in McAfee Endpoint Security to quarantine suspicious, but not convicted, files in memory and stop potentially malicious changes from executing on the endpoint while the file can be analyzed.

"We now have very granular control over the endpoint," says Jeff Bowen, a security engineer who works for Harmonson. "If you think of endpoint protection as a car," he says, "with McAfee Endpoint Security, we now have the latest model, with the best instrumentation, nicest features, and all the bells and whistles."

Improved Decision Making for Much Faster Response and Remediation

"A couple years ago when a threat entered, we wouldn't hear about it until five or even 10 days afterward, and then we'd have to figure out what to do," recollects Harmonson. "That kind of delay just isn't acceptable anymore. The amount of damage that threats like ransomware can do in a very brief time is significant."

"One of the greatest benefits thus far is the ability to have information we trust so we can make the right decisions in a timely manner and subsequently reduce risk within the organization," states Harmonson. "McAfee Endpoint Security is providing us with more and better information to help us better understand the threats that enter our environment."

According to Harmonson, the DWR used to have to wait 24 hours for its antivirus vendor to create a new signature. Today, with McAfee Endpoint Security, malware's window of opportunity has shrunk tremendously. "We are getting to the point where we can investigate an incident and resolve it within one to four hours," he says.

"McAfee Endpoint Security is definitely a product worth exploring," says Harmonson. "With the layers of protection that it provides, it far exceeds the stereotypical antivirus product. I really appreciate how it provides my staff with the relevant information at their fingertips, helps them understand what happened, accelerates response time, and mitigates risk."

"McAfee Endpoint Security is definitely a product worth exploring. With the layers of protection that it provides, it far exceeds the stereotypical antivirus product. I really appreciate how it provides my staff with the relevant information at their fingertips, helps them understand what happened, accelerates response time, and mitigates risk."

—Richard Harmonson, Chief Information Security Officer, California Department of Water Resources

Roadmap for the Future to Further Reduce Burden on Staff

The California DWR recently began using the McAfee Advanced Threat Defense sandboxing appliance. It also plans to deploy McAfee Threat Intelligence Exchange and McAfee Endpoint Threat Defense and Response to further bolster protection against advanced and unknown persistent threats. McAfee Threat Intelligence Exchange aggregates global and local threat intelligence and shares it among security solutions, such as McAfee Endpoint Security and McAfee Advanced Threat Defense, that are connected via the McAfee Data Exchange Layer (DXL). McAfee Endpoint Threat Defense and Response continuously monitors endpoint processes to uncover hidden threats, automatically prioritize suspicious activity, and provide live and historical threat data to determine the full scope of an attack before using one-click correction across the entire organization.

"These tools will help us be aware when threat actors appear, give us time to react, and prevent further activities of the same nature," states Harmonson. "With them, we hope to create a more adaptive, sustainable threat defense lifecycle that reduces the administrative burden on our staff even further, especially since adding new staff with the right skill set can be a challenge."

"Can't Overemphasize the Partnership"

In addition to McAfee products, DWR relies on McAfee Professional Services—including a McAfee Resident Support Account Manager dedicated to endpoint protection—to augment and support its security staff. "Using McAfee Professional Services has helped 'fast track' our deployments," says Harmonson.

"Over time, you develop relationships with different vendors and some are better than others," he adds. "Our relationship with McAfee has been extremely supportive from the start. I trust our McAfee team and feel that they are working alongside us as true partners, sharing the same objectives. I can't overemphasize the partnership."

McAfee™
Together is power.

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