

Christian Church Homes Gains Tighter Security and More Control with eSoft Internet Security Gateway

Award-winning InstaGate Appliances Shield Residents, Employees and Data against Viruses, Phishing Sites, and Hacker

The Organization:

Christian Church Homes



The Challenge:

Christian Church Homes of Northern California needed an Internet security system to protect the confidential financial information of its residents and to keep its network up and running.

The eSoft Solution:

eSoft provided the organization with more than 50 of its award-winning InstaGate gateways.

The Benefits:

- Intrusion Prevention keeps residents' confidential data safe from hackers.
- Network is protected against malicious software (worms, Trojans and viruses).

The web filtering in eSoft's Web ThreatPak blocks employees and residents from visiting phishing sites and other URLs known to serve up malicious software.

Security Required for Residents' Confidential Data

Christian Church Homes (CCH) has been providing quality housing in caring communities since 1961. A private, non-profit corporation, CCH manages 58 facilities, providing over 5,000 residential units without distinction on the basis of race, color, national origin, sex, religion or familial status. All but one of the organization's facilities feature HUD-subsidized apartments.

In 2006, CCH was outsourcing its security services to an ISP when it was determined that an Internet-security solution was needed internally in order to gain more control over endpoints logging into the network and accessing resources and information from its remote facilities. CCH maintains a database of extensive financial and other confidential information on its subsidized housing residents, and this information needs to be well protected.

"We have a lot of information on people that must be protected from hackers," said Leland Foster, Director of IT at Christian Church Homes. "We also need protection from email and Web-based viruses as well as spyware. Phishing sites and other virus sites are such a huge risk, and our ISP was only doing so much to keep us safe. We needed to do something more to make sure our data and resources were fully protected."

CCH looked at solutions from Barracuda Networks, eSoft and Fortinet. Because Barracuda would only solve the organization's spam issue and Fortinet did not offer specific VPN capabilities the organization needed for its remote sites integrated into one appliance, CCH chose eSoft.

- eSoft VPN Manager makes it simple for CCH to centrally manage its distributed network of InstaGate security appliances and remote users, lowering overall cost of network ownership.

eSoft's Distributed Intelligence Architecture™ quickly identifies new threats and provides rapid, proactive protection against new malware, malicious websites, phishing attacks, and botnet threats.

"Before the InstaGate gateways were installed, our email was going through two different security levels – an outside company conducted the first level of filtering, and then we had a desktop solution as the second tier. When I added the InstaGate, I began catching 25-30 viruses a week—and this is after passing the first two levels."

Leland Foster
Director of IT
Christian Church Homes

Installed Components:

eSoft's [Intrusion Prevention System](#), included with all ThreatPaks, keeps hackers off the protected networks.

CCH deployed eSoft's InstaGate Security Gateway solution with Web and Email ThreatPak capabilities. One InstaGate 604 is deployed at the Oakland headquarters building, and InstaGate 404e gateways are deployed at the organization's residential building sites. InstaGate, which utilizes a high-performance Deep Packet Inspection (DPI) Firewall and IPSec VPN architecture, offers unparalleled protection from dynamic, content-based threats that elude traditional firewalls.

Preventing Spam, Intrusions and Malware

The InstaGate's Intrusion Prevention System keeps hackers outside the network and away from residents' confidential financial and personal information residing on the network. The gateway automatically logs attacks for reporting analysis and alerts an administrator when there's a high priority attack. The InstaGate is updated daily with the latest signatures for blocking new and emerging attacks.

eSoft's Email ThreatPak handles all of CCH's needs for virus protection, email security, content filtering, and spam mitigation. The latest spam-fighting technology is combined with a powerful anti-virus and content scanning engine to provide the organization with comprehensive protection from both external and internal email-borne threats.

"We were protected against the PDF exploit within hours of it being announced," said Foster. "The InstaGate blocked bad PDFs while allowing the clean ones through. I heard about the PDF vulnerability and called eSoft, to learn from them that we had already been protected against it before it was even publicized."

Within the Web ThreatPak is eSoft's Content Filter feature, which scans CCH employees' incoming and outgoing email for keywords, phrases, and patterns that indicate possible policy breaches such as the sending of social security numbers. Offending emails are quarantined for an administrator to inspect.

"Before the InstaGate gateways were installed, our email was going through two different security levels – an outside company conducted the first level of filtering, and then we had a desktop solution as the second tier," said Foster. "When I added the InstaGate, I began catching 25-30 viruses a week—and this is after passing

the first two levels. The others were letting so much through without my knowledge. Now I spend less time chasing viruses, and I worry less about where people are browsing on the Internet."

eSoft's [Email ThreatPak](#) handles all of CCH's needs for email security, content filtering, spam mitigation, phishing email blocking, and email-borne virus protection. The organization is protected against both external and internal email-borne threats.

- eSoft's [Web ThreatPak](#) filters spyware, phishing sites, browser exploits, viruses, and other malicious Internet content while allowing CCH to set and enforce its own Internet usage policies. The large database of spyware, phishing and other URLs is updated automatically with newly categorized websites through eSoft's patented SoftPak Director™ threat response architecture, and the organization can add its own custom URLs to the database.

eSoft's [Content Filter](#) feature scans CCH employees' incoming and outgoing email for keywords, phrases, and patterns that indicate possible policy breaches such as the transmission of social security numbers. Offending emails are quarantined for an administrator to inspect.

More Control and Protection against Malicious Websites

Within eSoft's Web ThreatPak is the Site Filter feature. With flexible group, user, day and time-based policies, Site Filter gives Foster and his IT colleagues complete control of enforcing what sites individual users or groups of users can access at specific times of the day. The solution is integrated with CCH's Active Directory so users are automatically and transparently authenticated and assigned the appropriate web access policy. Detailed reporting then allows a convenient way to summarize and report on actual usage.

"The Web ThreatPak features give us more control granularity, enabling us to have different website filters for different groups," said Foster. "It's easy to use and intuitive, and the integration of Active Directory is very beneficial. The addition of new sites every day is a great asset and helps us keep users off malicious and inappropriate websites."

With the InstaGate, CCH's residents and employees are also protected against phishing scams. "InstaGate blocks phishing sites, which is important to us," said Foster. "We deal with a lot of online banks in this business and the InstaGate automatically blocks users from visiting ever-increasing phishing sites. I can manage the white list myself and manage the quarantine process instead of relying on an outside company to do that. It used to be we'd have to ask a service provider to add a URL to the white list. That request wouldn't be fulfilled for a week or more. Now I can do that myself, bringing full control in-house."

In addition to keeping residents off phishing sites, Site Filter also helps keep CCH employees focused by keeping a database of sites not allowed, including auction, shopping, social networking, and other distracting sites. Finally, CCH has established computer centers for its residents to access the Internet, and eSoft enabled the organization to set up a de-militarized zone (DMZ) so residents can visit approved sites while they're blocked from visiting sites known for fraud, providing them with an extra level of personal data protection.

- eSoft's [VPN Manager](#) makes it simple for CCH to centrally manage its distributed network of InstaGate security appliances and remote users. With a few mouse clicks, CCHs created its VPNs and securely connected its corporate headquarters and far-flung residential buildings. VPN Manager reduces the organization's IT resource requirements and ultimately lowers the overall cost of network ownership.

Real-Time Updates Protect against Newest Threat

eSoft's Distributed Intelligence Architecture™ (DIA) leverages eSoft's patented SoftPak Director™ (SPD) security infrastructure to create a dynamic, two-way communication channel between all eSoft appliances and the SPD. By harnessing the power of eSoft's installed customer base on an opt-in basis to create a collaborative, global threat prevention network, CCH has the power, tools and scale to combat the ever-increasingly sophisticated and coordinated malware attacks on their network. Each eSoft security appliance self-updates all of its signatures constantly through the day and night. Customized reports and mapping features summarize threat activity and provide warning flags, as well as protection suggestions particular to each appliance and network.

"The real-time updating is a tremendous asset—we're always protected against even brand-new threats," said Foster. "I am pleased with eSoft—it offers a robust solution, great pricing, and excellent support."

"The Web ThreatPak features give us more control granularity, enabling us to have different website filters for different groups. The addition of new sites every day is a great asset and helps us keep users off malicious and inappropriate websites."