

Northern Hills Federal Credit Union Keeps Customer Information Safe from Hackers with eSoft UTM Solution

Award-winning InstaGate Shields Credit Union against Intruders and Malware and Enhances Productivity by Blocking Spam

The Organization:

Northern Hills Federal Credit Union



The Challenge:

Northern Hills Federal Credit Union needed an Internet security system to protect its customers' confidential information from hackers and to keep its business running.

Meeting Security Requirements for Credit Union Customers

Northern Hills Federal Credit Union, chartered in 1950, is based in Sturgis, South Dakota and offers its members the convenience of four branch locations. Northern Hills is a \$44 million financial institution serving over 6,000 members.

The eSoft Solution:

eSoft provided the credit union with its award-winning [InstaGate Unified Threat Management \(UTM\)](#).

In 2000, Northern Hills Federal Credit Union began protecting its network with eSoft's InstaGate EX2 Unified Threat Management (UTM) appliance. It had chosen eSoft over some of the industry's leading vendors, including SonicWall and others. In 2007, the credit union upgraded to [eSoft's InstaGate 604 appliance](#) and added the company's [Email](#) and [Web ThreatPaks](#) for comprehensive protection against email- and Internet-borne threats. The credit union worked with eSoft's integration partner, All Net Connections, for the upgrade.

The Benefits:

The credit union's network and resources, including confidential customer information, are safe from hackers, data, and identity thieves.

Malicious software (worms, trojans and viruses) are stopped at the perimeter of the network.

- Intrusion Prevention provides protection against hackers and directly addresses regulatory

"We chose eSoft for its robust set of features as well as the fact that it stays up to date and the operating system is well maintained," said Cindy Griffin, President of the credit union. *"The intrusion prevention feature was the most compelling because nobody's been able to get past the InstaGate in penetration testing. eSoft also offers very good support and is very responsive to our needs. It just made sense to swap out the old InstaGate for a newer model."*

Northern Hills Federal Credit Union has deployed eSoft's [InstaGate Security Gateway](#) solution with [Web](#) and [Email ThreatPak](#) capabilities. 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. eSoft's [SoftPak Director™](#) subscription management provides the credit union with

audit requirements.

New services can be quickly and easily added to the solution as requirements change, using eSoft's patented [SoftPak Director™](#) technology.

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

"Regulations in the financial industry are very strict, and we're fortunate in that we've had good protection from the beginning and haven't suffered any intrusions. We've had some intense IT audits from government agencies and those agencies seem impressed with our eSoft security solution."

**Cindy Griffin
President
Northern Hills Federal
Credit Union**

Installed Components:

eSoft's Intrusion Prevention System keeps hackers — and security auditors — off the protected network.

eSoft's [Email ThreatPak](#) handles all of Northern Hills Federal Credit Union's needs for

unmatched flexibility and responsiveness with the ability to add new security applications, as well as instantly and easily receive ongoing updates and malware signatures.

eSoft offers a robust set of administrative and maintenance features that allow IT managers to implement a sophisticated security solution without extensive training or time investments. eSoft's security applications are designed to be enabled with a simple click of the mouse, configured in a matter of minutes, and provide immediate protection with continuous, automatic updates without administration.

"We work with a national firm that audits our security, and they installed an appliance inside our network that is designed to hack and find open ports and threats and patches that aren't updated," said Griffin. **"They work hard to hammer at our network, and the InstaGate — except for a couple of false positives — responded to this sophisticated technology and came through with flying colors."**

Preventing Intrusions and Malware

The InstaGate's Intrusion Prevention System keeps hackers outside the network. This protects the confidential financial, personal, and corporate information that is present on the credit union's servers and in customer databases. The InstaGate automatically logs attacks for reporting analysis and optionally alerts an administrator when there's an attack of interest such as a high priority attack. The InstaGate's self-updating features mean that it is always updated with the latest signatures for blocking new and emerging attacks.

"Regulations in the financial industry are very strict, and we're fortunate in that we've had good protection from the beginning and haven't suffered any intrusions," said Griffin. **"We hear about some threats and we aren't affected by those. We've had some intense IT audits from government agencies and those agencies seem impressed with our eSoft security solution."**

"The credit union stayed with the eSoft InstaGate solution because it had never been hacked, it's that simple," said Bob Harlan of All Net Connections, eSoft's integration partner. **"I've been working with this product for more than eight years and all of my customers that use the InstaGate are happy with it. They're happy with the features and performance, and they're happy with**

email security, content filtering, spam mitigation, phishing email blocking, and email-borne virus protection. The credit union 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 also allowing Northern Hills Federal Credit Union to set and enforce 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 credit union can add its own custom URLs to the database.

eSoft's [Content Filter](#) feature scans Northern Hills Federal Credit Union 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.

eSoft's support team."

Enhancing Employee Productivity

eSoft's [Email ThreatPak](#) handles all of Northern Hills Federal Credit Union's needs for email security, content filtering, spam mitigation, and virus protection. The latest spam-fighting technology is combined with a powerful anti-virus and content scanning engine to provide the credit union with comprehensive protection from both external and internal email-borne threats.

Within the Email ThreatPak is eSoft's [Content Filter](#) feature, which scans Northern Hills Federal Credit Union 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. Content Filter also gives Northern Hills Federal Credit Union the ability to block email file attachments by type, such as .exe, .scr, and .com.

"Spam was a big problem before eSoft," said Griffin. "Employees were getting quite a bit of it before we deployed the InstaGate 604. It's also great because it requires so little overhead and it's so easy to add sites to the white list. When we hear no complaints from end users about spam, that's the real testimonial — no news is good news."

Updates and Compliance Reports in Real Time

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, Northern Hills Federal Credit Union has the power, tools and scale to combat the 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.

"eSoft's ThreatMap shows us where each threat is

"Our members trust us with their confidential data and they rely on us to protect that information. They assume we're doing our job. With eSoft's security solution, we do exactly that."

coming from, which is crucial information for a financial institution," said Griffin. "The bottom line is that with eSoft we're not fighting viruses or hackers because the InstaGate just works, so we can spend our time elsewhere."

Northern Hills Federal Credit Union remains a happy eSoft customer after eight years and looks forward to many more years of eSoft protection for its resources and data. "Our members trust us with their confidential data and they rely on us to protect that information. They assume we're doing our job," said Griffin. "With eSoft's security solution, we do exactly that."