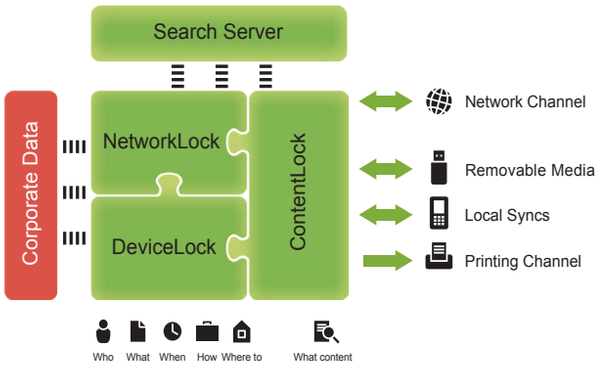
DeviceLock® DLP Case Study

Numerica Credit Union Utilizes DeviceLock to Enforce Endpoint and Network Data Security Controls

Numerica is the fifth largest credit union in the state of Washington with 20 branches throughout the state as well as locations in Northern Idaho. With nearly 115,000 members, Numerica sets its security standards very high in regards to protecting their members' financial and personal data and in ensuring it doesn't expose its network to malicious malware, viruses and potential security breaches.

To meet its compliance requirements as a financial institution as well as its own internal security policies, Numerica is very proactive in its approach to data security. This led the company to explore the use of data leak prevention (DLP) software to ensure both endpoint and network data security. This process culminated in the decision to implement DeviceLock endpoint DLP modules in their organization.

DeviceLock DLP
The Industry Benchmark



The Business Problem

As a financial institution, Numerica is required to comply with a number of regulations regarding the protection and security of private client and financial data including PCI – DSS, Department of Financial Institutions (DFI) and the National Credit Union Administration (NCUA). The company was also aware of the security risk posed by their endpoint computers in terms of the potential loss of data via attached USB thumb drives as well as the introduction of viruses and malware that could result from plugging in an unauthorized USB device into a computer.

As Tony Trunkhill, AVP Network and Security Services at Numerica states: "We were looking to be more proactive in securing our network and protecting our members' data. We had always had administrative controls in place, but wanted a solution that would enhance our technical controls. We take security very seriously and keeping our members safe is a top priority."

Numerica had established a written security policy that prohibited users from plugging in USB devices including thumb drives and other storage devices into their endpoint computers, however they were looking for a solution that provided technical controls to enforce the administrative restrictions. With some Macs in their environment, it was important that the solution supported Apple OS as well.

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

DeviceLock Endpoint DLP Suite 8.0

Peter Stephenson, Technology Editor 9/1/2015

Product Rating

Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★★★
Overall Rating	★★★★★

SC MAG says:

Strengths Too many to list.
Weaknesses None that we found.
Verdict If you want a traditional tool for managing and preventing data leakage at the endpoint, this has got to be your cup of tea. If functionality isn't here you probably don't need it.

Organizations around the world use DeviceLock to secure their endpoints and ensure compliance with increasingly stringent data protection legislation. Trusted by over 70,000 organizations of all types, and deployed on over 7 million devices.

Stop Data Leaks at the Source with DeviceLock

Download a free 30-day trial at: www.devicelock.com/download

Numerica Credit Union Utilizes DeviceLock to Enforce Endpoint and Network Data Security Controls

The Solution

After extensive research for DLP and USB management tools, the company found a few possible solutions, but after a DeviceLock demo, it was apparent that DeviceLock provided the specialized features that were more in line with what Numerica was looking for in a solution.

"Other solutions had DLP and USB management as part of their suite, but not to the level that DeviceLock provides," said Tony Trunkhill.

"We used the trial software by putting it into our test environment and tried to circumvent it. We wanted to get a real feel for the product and the flow before purchasing. We tested DeviceLock from an end user perspective as well as from an administration level and found that it was intuitive, easy to use and solved our problem on both Windows and Macintosh."

"From the time we first demoed DeviceLock to the time we purchased the product was really fast, around 30 days. We encountered a couple of issues while testing, but our network security engineer, working with DeviceLock support, was able to get his questions answered right away and any issues were resolved quickly. After working with DeviceLock support, he said that they were super helpful and had nothing but great things to say about them, so I was really impressed by that."

"Instead of using Group Policy to deploy out to our users, we used an MSI and pushed it out with SCCM and the process worked very well."

The Results

Numerica has received a lot of positive response from both staff and management regarding the DeviceLock rollout. "So far the feedback has been really good and for staff, it's more about awareness. Recently I had someone come to me and say 'I'm trying to use this thumb drive but it's not working,' and we told him that he doesn't have the ability anymore to just plug in any thumb drive. He had to go through the process of getting the device approved. However, our security policy has always been that we don't allow USB drives to be connected to endpoints, so he should have never expected it to work. Now with DeviceLock, we have a solution that basically provides the technical controls to enforce our existing policy."

"I like that DeviceLock keeps users informed of what's happening with customizable pop-up messages. I've seen other products that block devices, but there isn't any dialogue with the end user. With DeviceLock, the user is informed of why the port is blocked or the USB device isn't working because of policy or the fact that the device is not whitelisted and approved. So, I really like that DeviceLock communicates with the end users."

"I report to the CIO, and he's really happy about our implementation of DeviceLock. DLP has always been a priority for him in terms of locking down endpoints to eliminate data loss, to insure people aren't transferring data that they are not supposed to and to eliminate an ingress point for viruses or malware. He's pleased to see us continuing to improve on our already strong security posture and retain complete control over our data and is very supportive in terms of how we plan to evolve the use and application of DeviceLock in our organization."

The Future

"We are currently very happy with the way that DeviceLock is locking down our endpoint devices in terms of port control, but we know that we are not utilizing all the great content and network features of DeviceLock's other modules. We intend on expanding its use into those areas in the future. We are particularly interested in the ContentLock OCR capabilities, since many of the financial documents that we deal with are in a scanned electronic format. Being able to analyze electronic documents via OCR and block access or copying based on policy is something we are very excited about implementing."

- **Context-based Controls –** Block or allow data flows by user, security group membership, file type, device type, network/email protocol, cloud service, hour-of-day, day-of-week, etc.
- **Content-based Controls –** Easily configured content rules and filtering of both "data-in-use" and "data-in-motion" ensures data is not leaking out through endpoints.
- **Advanced Monitoring and Reporting –** Centrally log, shadow-copy, alert and forensically analyze end-user data transfers to devices, ports, printers and network communications.
- **Content Discovery –** Gain visibility and control over sensitive "data-at-rest" stored across the entire network environment to proactively prevent potential data breaches.
- **Extensive Data Handling –** Support for over 5,300 file types, 160 file formats, and on-the-fly OCR in 30 languages to handle data within files, emails, documents, chat sessions, images, compressed archives and scans.
- **Easy Management and Administration –** Native integration via Microsoft Active Directory Group Policy console snap-ins for a highly configurable yet simple to manage endpoint DLP solution for Windows administrators.

Download a free 30-day trial at: devicelock.com/download

AMERICAS
DeviceLock, Inc.
3130 Crow Canyon Place, Suite 215
San Ramon, CA 94583, USA

DeviceLock Canada Inc.
1066 West Hastings Street Ste 2300
Vancouver, BC V6E 3X2, Canada

email: us.sales@devicelock.com
Toll Free: +1 866 668 5625
Phone: +1 925 231 4400
Fax: +1 925 886 2629

UNITED KINGDOM
DeviceLock, Inc.
The 401 Centre, 302 Regent Street
London, W1B 3HH, UK
Toll Free: +44 (0) 800 047 0969
Fax: +44 (0) 207 691 7978

ITALY
DeviceLock, Srl
Via Falcone 7
20123 Milan, Italy
Phone: +39 02 86391432
Fax: +39 02 86391407

GERMANY
DeviceLock Europe, GmbH
Halskestr. 21
40880 Ratingen, Germany
Phone: +49 2102 89211-0
Fax: +49 2102 89211-29

RUSSIA
DeviceLock, Russia
M. Semenovskaya d. 9 st. 9 Office
140, 107023 Moscow, Russia
Phone: +7 495 647-9937

[For more information: www.devicelock.com]