White Paper: **March 2023**

Achieving Compliance with GLBA and Other Regulatory Requirements

How a Credit Union Leveraged the NSX Distributed Firewall with Advanced Threat Prevention to Go Above and Beyond

vmware®

Like all financial institutions operating within the U.S., the United States Senate Federal Credit Union (USSFCU) is required to demonstrate compliance with multiple regulatory regimes. These regimes are intended to protect the safety and soundness of the financial system and ensure that institutions are compliant with consumer protection laws, and demonstrate that they're appropriately protecting customers' private data and the information systems that house it. In addition, as a credit union, USSFCU is subject to rules and regulations that are specifically designed to reduce risks to federal credit union account holders and the National Credit Union Share Insurance Fund.

USSFCU provides banking and financial services to more than 32,000 federal employees, including employees of the United States Supreme Court and the U.S. Senate. Now managing more than $1 billion in assets, USSFCU maintains a strong commitment to keeping its customers' personal data and information secure. However, the credit union must also formally demonstrate compliance with the rules and regulations enforced by the National Credit Union Administration (NCUA), the provisions of the Gramm-Leach-Bliley Act (GLBA; also known as the Financial Services Modernization Act of 1999), and an annual third-party audit against the requirements of the Federal Financial Institutions Examinations Council (FFIEC).

On average, USSFCU undertakes an audit for each compliance regime on an annual basis. NCUA determines the frequency of audits on the basis of a credit union's size; those with over $1 billion in assets under management are reviewed by an NCUA auditor at least once per year. GLBA and FFIEC compliance is ascertained by third-party auditors who are contracted to provide services. In addition, USSFCU's internal risk management team provides ongoing guidance and suggestions for improving the organization's risk profile.

USSFCU wanted to take a modern, software-defined approach to network and infrastructure security, so their IT and security team chose the VMware NSX Distributed Firewall to provide the firewalling and traffic management capabilities needed to meet compliance requirements. Further, USSFCU has implemented the Advanced Threat Prevention (ATP) add-on to the NSX Distributed Firewall. This enables them to go above and beyond the basic network security requirements needed to achieve compliance.

USSFCU must always be ready to show evidence that it is applying appropriate risk management controls at short notice.

Meeting a broad array of compliance requirements

Even though USSFCU is required to meet three distinct sets of regulatory requirements, each with its own audit process and security control objectives, in practice, the three compliance regimes – NCUA, GLBA, and FFIEC – are interrelated. This is the case because individual auditors often ask to see the results of the most recent audit that was conducted, even if that was an examination for a different regulatory requirement.

"The purpose of the audit process is for the government to make sure we're operating in a safe and secure manner in order to protect the overall financial wellness of the system, but each individual auditor can do things a bit differently," says Mark Fournier, Chief Information Officer at USSFCU. "This means that what's examined can vary from year to year and compliance regime to compliance regime. Further, auditors often consult the report from the most recent audit. This can help them determine what to focus on."

It's common for an auditor to choose to investigate an area where controls or documentation were found to be ineffective during the last examination. Because the auditor's aim is to use their time effectively, they'll try to look most deeply into the areas where they believe there are potential control deficiencies. However, every individual audit is different. USSFCU must always be ready to show evidence that it is applying appropriate risk management controls at short notice.

Each compliance regime's audits are conducted slightly differently:

- GLBA audits are conducted by third-party consultants; typically, the auditors are security professionals or employees of an accounting firm or consultancy.
- NCUA auditors are federal employees. Their goal is to assess the credit union's overall risk profile, which encompasses both the technologies it has implemented and the policies and procedures it has put in place. Typically, they'll select a few sub-areas to probe deeply into while also striving to understand the overall security architecture.
- FFIEC audits are also completed by third parties.

Each compliance regime completes one audit annually, so USSFCU fields three compliance audits during each calendar year.

While USSFCU's goal is to maintain clean audits across all three compliance regimes with no adverse findings, the organization also strives to meet the compliance requirements efficiently, with minimal disruption to operations. The less time that security and risk management employees spend hunting for files and logs to document processes and configurations, the more time they have to spend on further enhancing USSFCU's security posture.

Security controls that are both flexible and powerful

Given the complexity of the compliance requirements that USSFCU must meet, it's no surprise that the organization's entire technology infrastructure was designed with risk management in mind. USSFCU's security team cannot limit

The VMware Advanced Threat Prevention package

Included capabilities (see Figure 1):

- **Detection technologies**
  - Distributed IDS/IPS
  - Network sandbox
  - Network traffic analysis (NTA)
- **Network detection and response (NDR)**
  - Aggregation, correlation, and context engines
  - The ability to pull context from sources outside NSX

its attention to just a few applications. Instead, they must ensure that all customer data and financial information is protected through the application of rigorous security controls and ongoing network monitoring, no matter where it's stored or how it flows within the environment.

To mitigate the cybersecurity and data breach risks it faces, USSFCU has implemented a Zero Trust security architecture. In the Zero Trust model, no devices, users, services, applications, or data flows are ever implicitly granted trust. Instead, the security architecture is designed to place a micro-perimeter around each application and its data. Should an attacker ever breach that perimeter, they will gain access only to that application and its data. This limits the damage that a single instance of account or resource compromise can do and ensures that incidents can be rapidly contained.

USSFCU deployed the NSX Distributed Firewall to achieve micro-segmentation across all of their applications and workloads. For an added layer of protection, USSFCU has also enabled NSX Distributed IDS/IPS. This intrusion detection and prevention system was purpose-built for analyzing east-west traffic to detect lateral threat movements. IDS/IPS capabilities are required to meet the regulatory standards to which USSFCU must adhere.

Going above and beyond what's needed to achieve compliance, USSFCU has also enabled Network Sandboxing, which enables its security teams to observe, analyze, detect, and block suspicious traffic as it's traversing the network. This provides a layer of defense against novel attack tactics like never-before-seen malware. In addition, they've also implemented Network Traffic Analysis (NTA) to perform behavioral analyses on east-west traffic as it moves laterally across the network. NTA provides security teams with enhanced visibility and real-time intelligence into what's taking place within their environment. Furthermore, USSFCU has also enabled Network Detection and Response (NDR) capabilities to give security teams yet more visibility, along with the ability to automatically monitor, detect, analyze, and quickly respond to sophisticated threats.

All of the above threat-focused capabilities are available as part of the ATP add-on to the NSX Distributed Firewall. For efficiency in operations, all of these capabilities are managed from the same central console, the NSX Manager. Looking in just one place, analysts and incident responders can quickly understand the scope of a threat and prioritize a response.

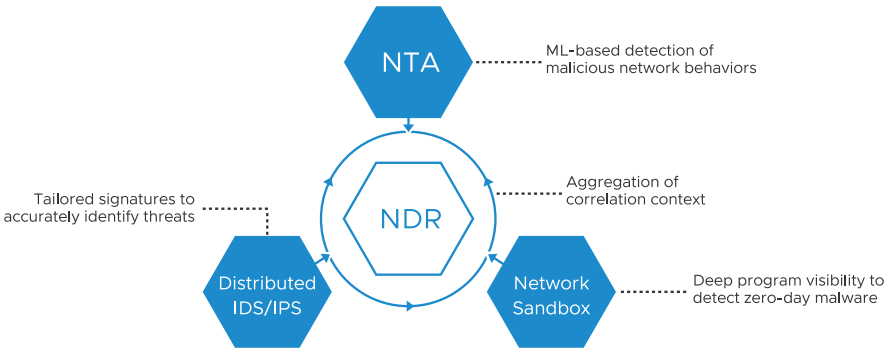

Figure 1: ATP: Multiple detection technologies + NDR

A network architecture designed for efficiency and simplicity

One reason that USSFCU decided to implement the NSX Distributed Firewall was to simplify network engineering. Although USSFCU does rely on an Enterprise Edge hardware firewall, they wanted to avoid hair-pinning traffic to this firewall since traffic hair-pinning consumes network resources unnecessarily and can negatively impact performance. Leveraging the NSX Distributed Firewall enables USSFCU to avoid this hair-pinning.

What's more, the use of the NSX Distributed Firewall also simplifies network switch configuration. In the past, the USSFCU security team needed to manually configure switch access control lists, something that's no longer necessary for the workloads that are protected by the NSX Distributed Firewall.

For these reasons, USSFCU's network architecture is now simpler, more robust, and easier to maintain than it would have been without the NSX Distributed Firewall in place.

The NSX Distributed Firewall stands up to auditors' expectations

Auditors are accustomed to looking for physical network security appliances. In the past, some auditors have been curious about the all-software distributed firewall implementation and were eager to learn more about it. Others have been more interested in the threat detection controls available in the ATP add-on to the NSX Distributed Firewall.

"In one recent audit that we undertook, the auditor had a pretty deep technical focus," says Fournier. "The auditor asked a lot of questions, like 'How do these systems work? What do the interfaces look like? What kinds of data do they collect? What are their reporting capabilities?'" Once the auditor understood what the technology looked like and gained confidence in our distributed firewall implementation, the auditor pivoted to focus on policy and procedures."

This isn't unusual. Auditors who dig deeply into the NSX Distributed Firewall deployment are often impressed by the granularity of control and breadth of network security that can all be managed from a single console.

Typically, auditors will examine the NSX Manager console to get a feel for how the technology works and understand the environment that's being protected. Auditors often check which security policies are deployed from the NSX Manager console.

Most often, they're looking to gain an overview of the traffic flows within the network. They're also trying to understand how firewall rules are configured and which IDS/IPS signatures are deployed. Since there's no appliance hardware to point to, it's the NSX Manager that makes the deployment real for the auditors.

As regulations and compliance requirements evolve and the institution grows, USSFCU will need to prepare to face many more audits and examinations in the months and years to come. With the flexibility and robust security that the NSX Distributed Firewall provides, USSFCU's security and risk management teams feel confident that they can continue to advance their security posture. With the NSX Distributed Firewall's unique architecture, they also have the operational simplicity they need to empower security analysts and incident responders to work smarter and achieve more.

---

1. VMware Inc. interview with Mark Fournier (U.S. Senate Federal Credit Union), 2023
2. National Credit Union Association (NCUA), https://ncua.gov
3. Federal Financial Institutions Examination Council, https://www.ffiec.gov
4. Gramm-Leach-Bliley Act, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
5. Internal Firewalls, VMware Special Edition, https://www.vmware.com/content/microsites/learn/en/656351_REG.html
6. Advanced Threat Prevention with VMware NSX Distributed Firewall, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-advanced-threat-prevention-with-nsx-distributed-firewall.pdf
7. United States Senate Federal Credit Union Makes Security Intrinsic with VMware, 2021 https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/customers/vmw-ussfcu-asset.pdf

Item No: Achieving Compliance with GLBA and Other Regulatory Requirements_JR2 3/23