Fortress

WHITEPAPER

A2V Supplier Security Network for Risk Management

A practical solution for managing third-party risk and regulatory frameworks.

Table of Contents

Executive Summary

2021 surveys found 93% of organizations have been impacted by a cybersecurity breach because of weaknesses in their supply chain[1]. In 66% of reported incidents, attackers compromised these organization by focusing on their supplier code[2]. The frequency and complexity of cyber-attacks on America's critical infrastructure, manufacturing, and defense sectors have accelerated dramatically in the last twelve to eighteen months.

The status quo of looking inward to manage risk and security is no longer an effective means of protecting industry. There is a growing need for a solution which ensures cybersecurity hygiene, information sharing, and supply chain security to enable asset owners to prioritize and react quickly to minimize the impact of threats introduced through third-party technologies.

This paper introduces a unique, scalable solution for simplifying the seek-and-find process of managing third-party security by providing instant access to vendor and product security assessments, continuous monitoring of vendors and products, and remediation via a collaborative supplier security network known as Asset to Vendor Supplier Security Network (A2V). The A2V platform and network combines multiple assessment types, continuous monitoring, tools, and expertise from security professionals to achieve and maintain a secure supply chain while managing multiple security compliance frameworks simultaneously.

A2V helps manage and perform vendor risk assessments, product risk assessments, and verifies the integrity and authenticity of software (e.g., patches), and analyzes software bill of materials. Assessments are customized to the framework of choice to evaluate risk. For example, in the utility sector, A2V facilitates CIP-013 implementation guidance published by NATF3 and NERC4. The platform's continuous monitoring of both vendors and products checks for vulnerabilities, indicators of compromise, software assurance, patch availability information, and more.

The traditional third-party risk assessment process is expensive, inefficient and time-consuming, and often is difficult or impossible for organizations to manage independently due to resource constraints. A2V addresses these issues by facilitating load balancing of costs to ensure a well-developed risk management program is affordable and available for organizations, no matter their size.

A2V's Governance Committee, made up of network members, ensures that the network remains ahead of industry, security, and regulatory requirements.

1. https://www.bluevoyant.com/news/bluevoyant-research-reveals-rise-in-supply-chain-cybersecurity-breaches-as-firms-struggle-to-effectively-monitor-third-party-cyber-risk/
2. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
3. http://www.natf.net/docs/natf/documents/resources/natf-cip-013-1-implementation-guidance.pdf
4. https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013-1-R1%20Implementation%20Guidance.pdf

The digital revolution has created new opportunities, but it has also created new vulnerabilities. Globalization and technological transformation have vastly enhanced the efficiency of supply chains for organizations in every sector but have also contributed to creating vulnerabilities and increased risk exposure.

Many industries have embraced digital transformation, realizing significant benefits in their interactions with vendors and clients. They have also experienced an increased attack surface. They are aware of the risks and the need for strong security. However, these organizations face significant challenges in managing risk across applications and infrastructure.

Challenges in Cyber-Supply Chain Risk Management

The Industrial Internet of Things (IIoT) creates great opportunities for efficiency, but also new vulnerabilities for attackers to exploit. Cybercriminals attempt to exploit these vulnerabilities with the goal of taking down network infrastructure and operations until their demands are met.

Nation states are also attempting to penetrate defenses. However, instead of looking for a payout, their goal is to either gain negotiating leverage, to make a political statement, or to surreptitiously embed themselves in preparation for the possibility of a conflict, at which point they could activate their embedded malware to disable defenses.

In January 2019 the Wall Street Journal[5] reported specific examples of how nation states are using supply chain vendors as a backdoor to attack the power grid. This is the first of two primary attack paths: (1) vendors of the organizations who have fewer resources to put towards cybersecurity, and (2) unpatched vulnerabilities in software.

Adversaries are multiplying, and their ability to exploit supply chain vulnerabilities is growing faster than they can be secured. Unless our methods change, we are fighting a losing battle.

The European Union forecast a 400% increase in the number of software supply chain attacks in 2016, a trend likely to continue.

5. Smith, Rebecca, and Rob Barry. Wall Street Journal. "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It". https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

6. ENISA. ENISA Threat Landscape 2021, p. 3. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Challenges in Vendor Risk Management

Managing vendor risks poses unique security challenges, even for those with mature security organizations.

- **Prioritization of large vendor populations**

  The large population size of supply chain vendors providing equipment, software, and services to your organization makes the task of risk ranking vendors costly and time consuming.

- **Assessing vendors with access to medium and high impact systems**

  Assessments are also time-consuming and costly. As a result, vendors are often only assessed when a new contract compels it, or when an existing contract is up for renewal, rather than on all existing vendors.

- **Non-responsive vendors**

  Vendors who remain "on-call" but who are not currently under contract may resist investing time and labor into completing assessments as they have no financial incentive for doing so, while vendors who are actively serving may not see the point of completing an assessment when their contract is not up for renewal. Internal procurement teams may be reluctant to impose another burden on their vendors for fear of failing to meet their procurement objectives. For these reasons, non-responsive vendors impede achieving risk management goals.

- **Vendor Cyber Remediation**

  Vendors may have challenges achieving security best practices and remediating security findings due to lack of resources. Resources are instead spent on responding to controls assessment requests.

- **Continuous Monitoring**

  Conducting point-in-time assessments leave large gaps of time during which vendors' security posture may change and outsourcing continuous monitoring to service providers can be costly.

- **Supply Chain System of Record**

  Traditional supply chain risk management systems do not meet the unique specifications required to efficiently execute a supply chain risk management program with customizable workflows, document management, approvals, analytics engine, customizable APIs,

> Vendor risk management can be challenging and costly and can be perceived as burdensome by the vendors. These challenges are common amongst critical infrastructure, manufacturing, and defense organizations alike.

Nearly 55% of organizations that suffered a data breach in the last two years cite as the culprit a known vulnerability for which they had not yet patched.[7]

7. Kellerman, Tom and Greg Foss. 2020. Global Incident Response Threat Report. VMware Carbon Black. October. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-global-incident-response-threat-report-the-cybersecurity-tipping-point.pdf

Challenges in Product Risk Management

Managing product risk is a complex challenge that presents its own set of concerns.

Software Assurance

Any software to be used in a secure environment must be verified for its integrity (unaltered from its original source) and authenticity (the identity of the software publisher is confirmed and linked with the software). This is typically a manual process.

Product assessments are complex

Cybersecurity testing on vendor products can ensure secure and reliable operations and inform owners on component provenance. Most industries have done little in the way of product assessments due to the cost.

Vulnerability tools are incomplete

Traditional vulnerability tools only provide vulnerability information if there is a specific CVE (Common Vulnerabilities and Exposures published by MITRE.) Industry professionals are left with only half the picture, because (1) they don't know about vulnerabilities that do not have CVEs, and (2) scanners tend to leave a 50%gap even with a CVE list[8]. Product patch scraping tools focus on automation but generally only provide up to 60% coverage[9], making it time-consuming to identify missing patches. Furthermore, a patch may not even be available, and mitigating controls then have to be researched.

Software Bills of Material (SBOM) Analysis

An effectively prepared and analyzed SBOM can be invaluable in addressing C-SCRM challenges, but the sheer volume of documents and data they generate create their own set of challenges.

Product Security Controls Assessment

Security controls present in a product help secure the assets and the network from attacks, however, understanding what security controls are available for a product and if recommended controls are configured by default on all products can be a time-consuming effort.

Vulnerability risk management can be challenging, costly, and regulatory deadlines create additional urgency.

8. TBA

9. TBA

Regulatory Challenges

New federal rules and regulations are being implemented to defend against and counter cybersecurity incidents, partially in response to recent supply chain attacks against federal networks. Every business should take note as sector regulators may implement similar rules as best practices.

On January 19, 2021, the Department of Commerce issued a rule which allows it to reject contracts for information communications technology and services when the provider originates from an adversarial nation[10]. On May 12th, 2021, The White House released Executive Order (EO) 14028, "Improving the Nation's Cyber-security", requiring IT service providers to share certain breach informaiton and setting standards for software sold to the goverment[11]. Additionally, on May 27th, 2021, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) announced pipeline companies would have more reporting requirements for cyber incidents and regulations[12].

To address emerging supply chain risks to the power grid, the North American Electric Reliability Corporation (NERC) has issued new standards that require organizations to develop a plan for managing cyber risks related to their supply chain. Organizations that fail to have a program in place (with ongoing compliance obligations) can face various levels of penalties ranging as high as $1,000,000 per violation per day. Other sector-specific regulators are likely to follow with their own similar requirements.

1. Duplicative effort

Organizations in the same sector share many of the same assets and vendors. For each organization to conduct the same assessment on a vendor wastes valuable resources for both your organization and the vendor.

2. Prioritization

A big issue for many organizations is a deluge of risk data. How to aggregate, normalize, and make sense of this data is essential to prioritize security resources. Better data informs security teams on how to do their job more efficiently.

3. Cybersecurity costs and staffing

Security team challenges include not just how to secure their assets and network, but how to do it without breaking the bank. Cybersecurity spending is rising, but not as fast as attacks are occurring, or as fast as new regulatory deadlines are approaching. Corollary to budgetary challenges is staffing. Increased demand for trained cybersecurity personnel has made qualified human resources scarce and expensive.

10. https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain, in relation to Executive Order 13873, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" (May 15, 2019) & Executive Order 14034, "Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries" (June 9, 2021)
11. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity
12. https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

A practical solution to C-SCRM risk management

A2V solves many of the challenges facing critical infrastructure, manufacturing, and defense organizations. It resolves issues in both vendor risk and asset or product risk management. It helps organizations achieve regulatory compliance in a timely manner. It reduces burdensome redundancies for organizations and vendors, and it reduces costs for organizations and vendors.

How A2V Helps

The A2V Supplier Security Network is a unique community for information sharing and collaboration which provides clients the ability to fully assess risks, proactively plan, and react if supply chain attacks occur.

Risk Identification and Prioritization

If you have thousands of vendors, where do you start? Data-driven risk ranking uses AI and open-source intelligence to determine the criticality and cyber maturity of supplier assets to quickly prioritize vendors into tiers. These 100% automated reports help organizations get better insight into their vendors at scale and are generally completed within two to three business days.

Validated Assessments

A data-driven vendor assessment can stand on its own or combines a partially automated process with a vendor questionnaire. We work with vendors to complete validated assessments consisting of about 250 questions and validate evidence of remediation when issues arise. Product assessments provide information on the provenance of components and compliance with requirements like the National Defense Authorization Act (NDAA), as well as analysis on product security controls and vulnerabilities.

Continuous Monitoring

Our data and analytics department monitors everything from foreign influence to cyber hygiene, breaches, indicators of compromise, and patch availability information. Regular cyber hygiene scans identify risks present within the public domain, while our File Integrity & Software Assurance (FIA) solution validates file integrity and software assurance and continuously monitors vendors and products to identify known and emerging threats from third-party components, application patches, updates, and more.

Remediation

Fortress provides processes for mitigating risk internally with the vendor, accepting the risk, or validating evidence of remediation after issues arise. We establish how and when controls will be created, and Fortress analysts further follow up with the vendor to finalize resolution. A2V offers secure sharing of risk information.

Software Bills of Materials

A2V uses patented blockchain technology to enable secure sharing to government or downstream consumers of SBOM content as part of our FIA solution. The same mechanism is used to consume supplier SBOMs to provide analysis on (open source) vulnerabilities, outdated components, and insight into component FOCI risk.

Solutions in Cyber-Supply Chain Risk Management (C-SCRM)

As data network and exchange with risk information on 40,000 vendors, millions of assets, and counting, the Asset to Vendor Supplier Security Network (A2V) solves many of the challenges associated with C-SCRM.

This collaborative platform and network acts as a C-SCRM information exchange where members can access a library of thousands of supply chain vendor assessments, product assessments, and cyber vulnerability solutions at significantly lower cost than through independent channels.

Our product assessments provide visibility on vulnerabilities, patch history, and security controls. Provenance reports illuminate risks related to each component in specific equipment, such as foreign influence or control.

A2V increases the security of all members, reduces costs of assessments by up to 50%, and "bends the O&M curve," lowering costs and, in some cases, allowing members to capitalize security costs.

1. **Contribute**

   Member organizations can contribute their completed vendor assessments and validated cyber vulnerability patches to the network or pay a reduced fee to have assessments completed, on both products and vendors.

2. **Share**

   The completed assessments are made available to other organizations at a cost that is projected to save them up to 50% or more of what it would cost them to complete themselves or pay another company.

3. **Reduce Operations and Maintenance (O&M) Costs**

   A2V saves cost due to automation and leveraging network effect sharing information. Assessments can be completed once and shared with many, eliminating redundancies and reducing costs associated with maintaining compliance.

> "Critical infrastructure organizations already share the risk. Now they can share the cost."
>
> - Alex Santos, Fortress CEO & Co-founder

Solutions to Vendor Risk Challenges

The A2V Supplier Security Network resolves many of the challenges vendor risk management teams face.

Risk Ranking Vendor Populations

A2V is pre-populated with the known vendors in an organization's supply chain, with a prediction of the inherent risk of each organization. For example, an OT maintenance provider being a critical risk, versus a travel agency being a low risk. This process utilizes data collection technology, AI, and analytics to make these predictions. A2V members can correlate their vendor list before performing manual inherent risk ranking, gaining insight into their overall risk on day one.

Assessing Vendor Security Controls

Enterprises in the same industry already share the risk, now they can share the cost. By performing assessments and sharing with many, the O&M cost for each organization will be significantly reduced.

Vendor Chasing

Vendors without contractual obligations to comply with may be unmotivated to respond quickly to requests for controls assessments. However, once the assessment is complete, vendors no longer face resource constraints to comply. A2V works with vendors to achieve mutual benefits.

Remediating Control Deficiencies

Just as problematic as non-responsive vendors are unresolved security control deficiencies. The cost efficiencies offered by A2V benefits vendors, helping them remediate deficiencies and show compliance to a wide audience of organizations.

Continuous Operational Monitoring of all Vendors

A2V provides continuous monitoring of all active vendors and cyber assets on the network. Members receive real-time security alerts when any vendor has an incident or new related vulnerabilities are discovered. Alternatively, Fortress and vendors can alert members through the network when they discover vulnerabilities and provide patches or solutions. Monitoring is expanded beyond traditional cybersecurity scanners which include things like application security, configurations, malware, and spam propagation, to include legal, financial, anti-bribery, anti-money laundering (AML), negative news, and regulatory compliance.

System of Record for Supply Chain Risk Management

The platform includes a catalog interface that provides real-time risk intelligence on vendors monitored by A2V. Members can view the catalog with real-time data to see vendor details, vendor products, software and hardware bills of materials (SBOMs and HBOMs) availability, vendor's participation level in A2V, cyber hygiene, breach alerts, M&A alerts, and potential compliance alerts. This includes customizable workflows, document management, approvals, analytics engine, customizable APIs, customizable surveys, rules automation, vendor portal, customizable scoring, and other key features.

A2V Supplier Security Network resolves many of the most pressing vendor risk management challenges, lowering costs for organizations and their vendors.

7. https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-013-1&title=Cyber%20Security%20-%20 Supply%20Chain%20Risk%20Management&jurisdiction=null

Solutions to Product Risk Challenges

The A2V Supplier Security Network resolves many of the challenges faced by IT and OT vulnerability risk management teams.

File Integrity & Software Assurance (FIA) Solution

Fortress FIA automatically verifies patch authenticity (the supplier source) and validates file integrity (that the file is unaltered). FIA uses a distributed ledger that compares file hash values to confirmed values. Further, patches are instantly available for subscribed products. Patches can also be validated back to FIA before deployment. FIA is also guses to share SBOMs.

Product Provenance

Product assessments provide information on the provenance of components for compliance with requirements like the National Defense Authorization Act (NDAA) and Foreign Ownership, Control, or Influence (FOCI) risk, as well as analysis on product security controls and their adherence to risk and regulatory frameworks. NDAA compliance identifies products and vendors that may be prohibited. Provence analysis provides visibility into the origin of components as well as the presence of counterfeit or obsolete components.

Vulnerability and Solution Monitoring

Products monitored in A2V include full vulnerability details, including both CVE and non-CVE information, indicators of compromise, software assurance, patch availability information, as well as organization-specific business context. Threat intelligence is overlaid on the vulnerability data to alert members to vulnerabilities that are actively being exploited.
Monitoring across multiple products simultaneously provides greater viability and insight into supply chain integrity and whether there are appropriate controls in place.

Software Bills of Materials (SBOMs)

A2V through FIA can generate, analyze, and securely share SBOMs. SBOMs allow for better visibility into a product's components and the potential vulnerabilities. Policies like Executive Order 14028 require the implementation of software supply chain risk strategies such as acquiring SBOMs from supply chain vendors.

Product Security Controls

Automated data-driven reports provide visibility into inherent product risk and show at a glance information on what security controls are in place on a product, analysis which can be taken forward into manual validation as well.

How A2V Helps Achieve Regulatory Compliance

A2V enables users to demonstrate compliance and adapt to emerging regulations.

NERC CIP-013 Case Study

Requirement[13]	A2V Solution
R1 Each Responsible Entity shall develop one or more documented supply chain cybersecurity risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include:	Out of the box program policies vetted by member organizations.
1.1 One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cybersecurity risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	All vendor risk service (risk ranking, security controls assessments, vendor chasing, remediation, and continuous monitoring) and product security assessment.
1.2 One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:	Policies include recommended contractual language and master services agreement addendums. Further, members have the option to use Fortress Platform to track the implementation and operation of all CIP-013 requirements.
1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cybersecurity risk to the Responsible Entity;	
1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cybersecurity risk to the Responsible Entity;	
1.2.3. Notification by vendors when remote or on-site access should no longer be granted to vendor representatives;	

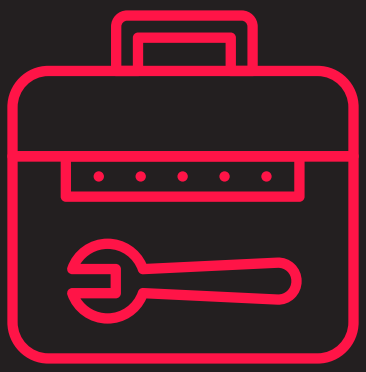
13. https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-013-1&title=Cyber%20Security%20-%20Supply%20Chain%20 Risk%20Management&jurisdiction=null

Requirement[13]	A2V Solution
1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;	Vulnerability and solution monitoring
1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and	File Integrity & Software Assurance (FIA)
1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	(Same as 1.2.1 through 1.2.3 above)

TSA Pipeline Security Guidelines Case Study

Requirement[14]	A2V Solution
7.3. Asset Management Establish and document policies and procedures for assessing and maintaining configuration information, for tracking changes made to the pipeline cyber assets, and for patching/upgrading operating systems and applications. Ensure that the changes do not adversely impact existing cybersecurity controls.	File Integrity & Software Assurance (FIA) for real-time patch integrity and source validation checks, Security Control Assessment, Vendor Chasing
7.3. Risk Assessment Establish a process to identify and evaluate vulnerabilities and compensating security controls.	Vulnerability and solution monitoring, solutions or remediation documentation
7.3. Security Continuous Monitoring Conduct cyber vulnerability assessments as described in your risk assessment process; Utilize independent assessors to conduct pipeline cyber security assessments.	Risk ranking, security controls assessments, remediation, product security assessment, and continuous monitoring

14. https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf



Buy or Build?

Many organizations facing security challenges and regulatory deadlines need to decide: Build or Buy?

Benefits of buying with A2V include:

- Correlation of vendor, asset, and product data – A2V brings it all together.
- Instant program maturity with compliant policies and procedures.
- Quickly scale Cyber-Supply Chain Risk Management (C-SCRM).
- Instant assessment availability.
- Request new and completed validated controls assessments based on your framework of choice to evaluate risk associated with vendors and products.
- A single solution for point-in-time assessments and continuous monitoring.
- Receive continuous monitoring alerts on changes to products and supply chain vendors.
- No added staffing burdens.
- Automate and leverage network effect sharing information.
- Bend the O&M curve: lowering costs and further ability to capitalize costs offset O&M.
- New Software Bills of Materials (SBOM) analysis and reports

FAQs

1. HOW DO I GET ACCESS?

Fortress Information Security is the current operator of the A2V Supplier Security Network exchange and is managing new registrations. For A2V membership information email sales@fortressinfosec.com or visit a2v.fortressinfosec.com.

2. WHY IS A2V ANY BETTER THAN OTHER RISK EXCHANGES?

A2V is the only exchange that offers a complete Cyber-Supply Chain Risk Management (C-SCRM) solution that connects assets, vendors and products. A2V focus is on critical infrastructure, defense, and critical manufacturing and offers comprehensive solutions to address the specific needs of your organization and sector specific needs.

3. IS SECURITY INFORMATION NORMALIZED?

A2V normalizes contributed assessments so that different assessment frameworks are correlated, and members receive a consistent experience.

4. HOW DO MEMBERS PAY FOR SERVICES?

A token system is used to provide simplicity. Token rates are utilized for assessments, risk ranking, and product subscriptions.

5. DO I RETAIN CONTROL OVER MY SECURITY ASSESSMENTS?

Yes, you maintain control over who your assessment is shared with, as written authorization is requested prior to sharing.

6. WHAT INCENTIVES DO VENDORS HAVE TO PARTICIPATE?

By participating in A2V, vendors who serve multiple organizations will save time interacting with each organization individually. Vendors have the opportunity to be seen as responsive partners that are supporting security and compliance needs.

7. WHAT IS THE DIFFERENCE BETWEEN FORTRESS AND A2V?

Fortress operates the A2V Supplier Security Network. A2V is a C-SCRM information exchange enabling vendors to complete an assessment once and, upon authorization, share with other clients.

8. WHO IS DRIVING THE A2V NETWORK?

Members are represented by a Governance Committee that is appointed by the organization members. Fortress Information Security performs operations for A2V.

Summary

The Asset to Vendor Supplier Security Network (A2V) is a platform and network where organizations can collaborate to solve the Cyber-Supply Chain Risk Management (C-SCRM) challenges they face today and prepare for tomorrow. This is an opportunity to make organizations more prepared and resilient against supply chain attacks.

A2V is a unique, scalable solution for achieving and maintaining regulatory requirements and managing multiple security frameworks simultaneously. A2V simplifies the seek-and-find process of managing C-SCRM by providing instant access to security assessment documentation on a multitude of vendors and assets. The A2V platform also provides continuous monitoring, assessments, and expertise from our security professionals.

Bringing Assets and Vendors Together

Many organizations are challenged by the vast network of component providers and manufacturing subsidiaries that make up their operational landscape. A2V helps you make sense of this data and focus on securing your organization. By bring together information from assets, vendors and products A2V automates and standardizes cyber risk assessment, monitoring and management efforts to produce actionable insight and get a holistic view of your security posture. This approach also assists with regulatory and security compliance efforts, saving time and resources.

Continuous monitoring over your entire cyber supply chain of assets and vendors provides real-time visibility into IT and OT vulnerabilities, while mitigating compliance exposure.

Collaborating to Address Supply Chain Security Challenges

A2V offers time and cost savings for both vendors and their clients by reducing the duplicative efforts of completing separate assessment requests.

Fortress created the A2V Supplier Security Network because we believe that security should be accessible to all organizations, big and small. Traditional third-party risk assessment services are a large financial undertaking for any business, and critical industries that lack budget and infrastructure to support initial vetting and continuous monitoring of their vendor network are left vulnerable to breaches.

A2V works with organizations, large and small, to provide a unified C-SCRM solution which load balances costs to ensure that a well-developed risk management program is affordable and available for organizations that support critical infrastructure, defense, and critical manufacturing, no matter their size.

By pre-emptively invoking the need for mutual assistance, organizations can minimize costs and reduce the risk for all. By sharing threat intelligence, best practices, vendor and asset-centric assessments, continuous monitoring and more, progress toward security and compliance can be accelerated.

Fortress guides critical enterprises to discover, prioritize, and monitor cyber and operational supply chain risk.

Find out more at fortressinfosec.com