CyGlass

Solution Brief

Detect and Stop Supply Chain Threats

Delivering Continuous Compliance with CyGlass Network Defense as a Service (NDaaS)

Could you protect your supply chain partners from compromise if your network was attacked?

Digital supply chain ecosystems offer access to larger markets and greater revenues, but organizations must step up their security hygiene and prove continuous compliance to participate, including the ability to meet partner-defined defensive capabilities 24X7.

That is because cyber attackers have penetrated supply chain ecosystems with multiple costly attacks in which organizations have had their entire security defense bypassed due to a partner's weak defenses.

Targeting supply chains allows threat actors to enter a well-defended environment undetected through trusted partner pathways. The attacker can then move laterally to steal valuable data regardless of the strength of perimeter and endpoint defenses, authentication and access control systems, and time and investment in security awareness training. The weakest partner in the supply chain ecosystem has proven to be the backdoor no one expected.

BUSINESS VALUE

Reduce Risk

Reduce vulnerability and threat risk with a universal view of network, directory, and cloud systems.

Participate in Digital Ecosystems

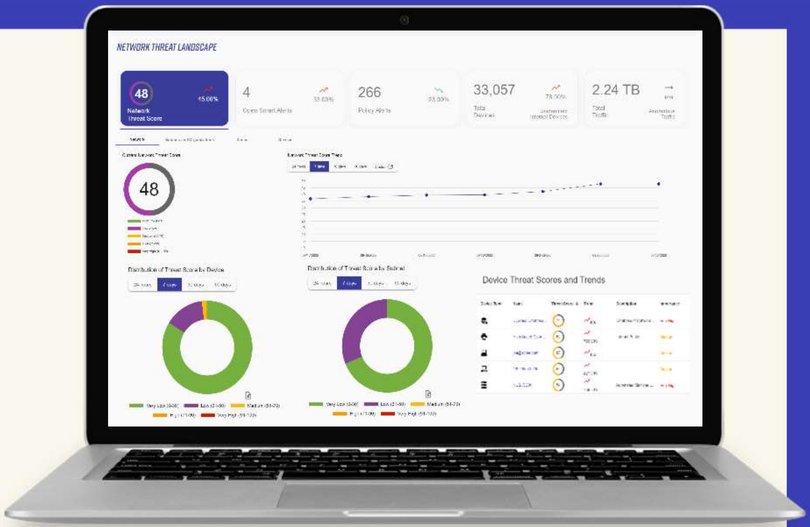
Meet and exceed supply chain ecosystem standards based in NIST 800-53, ISO27001, CMMC, and Cyber Essentials with prebuilt AI driven controls and automated reporting.

Lower TCO

Achieve significant operational efficiencies and cost savings through integrated SECOPS automation and workflows.

Report Security Hygiene

Deploy and automatically monitor and report on integrated security controls for supply chain, regulatory and governmental audits.



The CyGlass continuous risk compliance dashboard delivers a near real-time view of the overall security hygiene of networks, devices, cloud apps, and users.

The Challenge for Mid and Small Companies

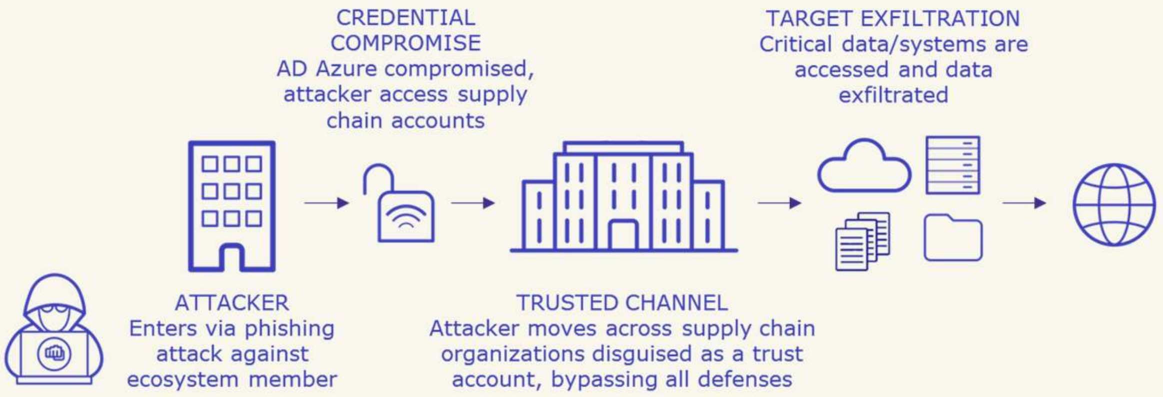
To mitigate the third-party supply chain risk, prominent vendors and ecosystem associations have joined together to set cybersecurity standards that must be met before integrated supply chain contracts are signed. These standards are enforced via stringent audits conducted on a timetable of the auditing parties' choosing, with the implication of failing being contract termination.

Implementing and remaining compliant with these standards creates a significant challenge for resource-constrained companies, who must improve their security hygiene across hybrid networks while managing operations and human costs. They must also demonstrate continuous compliance to enter or remain a part of the supply chain ecosystem. Compliance standards vary significantly from Department of Defense CMMC 2.0 for acquisition and contracting to NIST 800-53 controls used by the motion picture association (MPA) to ISO 27001 rules utilized by payment gateway vendors.

For most organizations, the traditional enterprise security mix of SIEM/EDR/NDR tools is a non-starter, yet they require a solution that can deliver these capabilities, including:

- The automatic discovery of vulnerable assets with the capability to identify and prioritize mitigation based on risk.
- 24X7 threat monitoring and remediation covering event correlation and alerting for compromised credentials, malware, risky activity, IoT threats, and high-risk traffic on network or cloud platforms.
- AI-driven automated threat hunting, investigation, and response with the ability to alert IT teams and offer rapid containment.
- The effective use of AI and automation to overcome staffing and budget constraints while delivering enterprise-class cybersecurity hygiene.
- Continuous security standard compliance with the ability to prove compliant processes and controls on demand utilizing risk and threat dashboards and security process scorecards.

Supply Chain Attack Example


CREDENTIAL COMPROMISE
AD Azure compromised, attacker access supply chain accounts
TARGET EXFILTRATION
Critical data/systems are accessed and data exfiltrated
ATTACKER
Enters via phishing attack against ecosystem member
TRUSTED CHANNEL
Attacker moves across supply chain organizations disguised as a trust account, bypassing all defenses

Supply Chain Attack Proliferation

From attacking software vendors' weak application security to exploiting identity security errors in Microsoft Azure, supply chain attackers use the vulnerabilities of an organization in a supply chain ecosystem to gain silent entry into and attack other, often larger and more valuable organizations. This attack path creates significant risk in the supply chain because while many vendors invest heavily in security, a single weak vendor can, when compromised, undermine many other vendors in the connected ecosystem. Examples of these attacks include: •

- 2018, ASUS, A software supply chain attack that leveraged a malicious version of ASUS Live Update, a utility that automatically updates computer system components. The malicious code included a backdoor trojan that reaches out to a C2 server to download additional payloads. Even though the trojan was widely distributed, this was a targeted data theft attack against ASUS supply chain partners ASUSTEC, Intel, and AzureWare.
- 2020, SolarWinds, A cyberespionage attack using a backdoor placed in legitimate, digitally signed Orion software updates. Then the infected updates were pushed out to thousands of customers, including the Departments of Justice and Homeland Security, and technology giants, including FireEye and Microsoft. The damage from this attack is still unmeasured.
- 2021, ShiftDigital, a CRM/Analysis firm for Volkswagen and Audi, collected 3.3 million individual records of car buyers, including driver's license numbers, names, mailing addresses, email addresses, numbers, and, in some instances, information surrounding the vehicle that was purchased. They promptly left the data unencrypted and unsecured on an internet-facing server for over a year leading to thousands of compromises.
- 2022, Kojima, This small Korean Plastics supplier, suffered a significant data breach in February. The data stolen included sensitive manufacturing plant operations at Toyota to completely shut down operations in Japan to protect their data and systems. Other Toyota subsidiaries were also affected. The initial Kojima compromise is still under investigation.

Secure Your Environment, Prove Compliance & Grow You Business

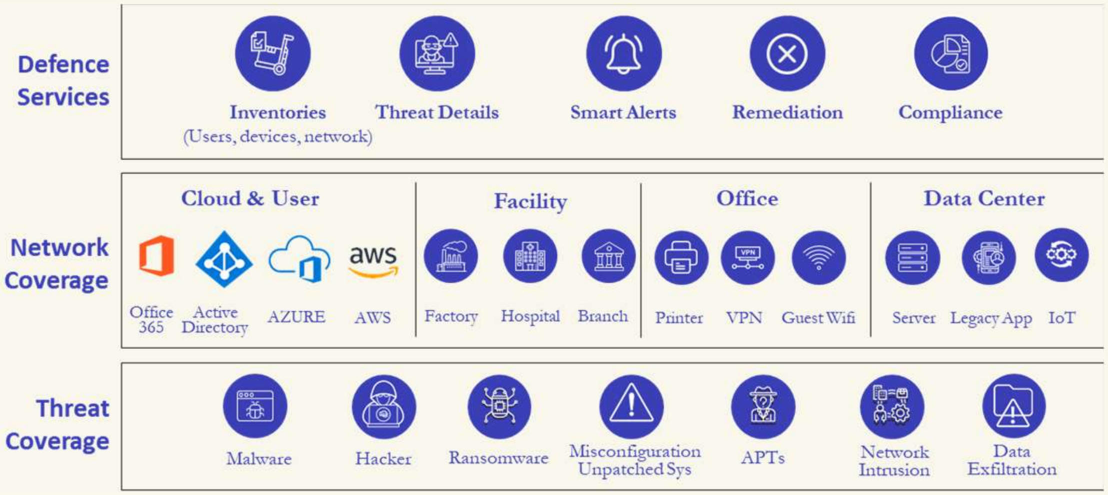
To participate in supply chain ecosystems, organizations must increase their internal defenses by improving system risk monitoring, rapid threat detection and response, and the ability to provide continuous compliance reporting. Uniquely monitoring and analyzing network, cloud, and user events, the CyGlass Network Defense as a Service platform utilizes AI correlated events, detection and risk scoring, and automated remediation designed specifically for resource-limited teams. Universal network visibility dashboards and integrated security and process scorecards allow organizations to prove defensive capabilities to their partners 24X7. With CyGlass, organizations can:

- **Eliminate Network Blind Spots** – 24X7 continuous visibility to cloud, directory, and network systems, including IoT devices, immediately surface vulnerabilities, policy failures, system risk, and anomalous events.
- **Detect Hidden Attacks** – Layered anomaly detection combined with cross-event correlation AI quickly identifies suspicious behavior, while automated remediation controls contain attacks inside your environment.
- **Exceed supply chain ecosystem standards** - Exceed NIST 800-53, ISO27001, Defense Industrial Base (DIB) NIST SP 800-171A, CMMC 2.0, and Cyber Essentials standards with prebuilt AI driven controls and automated reporting.
- **Prove Continuous Compliance** – SecOps process scoreboards, risk dashboards, and multi-view automated threat reports enable teams to prove compliance 24X7.
- **Afford Enterprise Class Network Defense** – A 100% cloud-native platform removes expensive onsite hardware, rapidly deploys in just hours, and reduces TCO for network and cloud threat detection and response by upwards of 70%.

With CyGlass NDaaS, IT and security teams can monitor, detect and contain supply chain attacks that penetrate the networks; rapid alerting and remediating to prevent these attacks from moving across the ecosystem to a partner.

CyGlass NDaaS Solution

Protection from the data center to the cloud



Defence Services

Inventories (Users, devices, network) · Threat Details · Smart Alerts · Remediation · Compliance

Network Coverage

Cloud & User: Office 365 · Active Directory · AZURE · AWS

Facility: Factory · Hospital · Branch

Office: Printer · VPN · Guest Wifi

Data Center: Server · Legacy App · IoT

Threat Coverage

Malware · Hacker · Ransomware · Misconfiguration Unpatched Sys · APTs · Network Intrusion · Data Exfiltration

CyGlass ingests network, cloud, and directory logs via a data collector layer. Data is securely transmitted to the CyGlass Cloud Service, where it is parsed, enriched, and passed to the CyGlass AI Engine. The CyGlass AI engine operates in an AWS Cloud. The AI engine combines unsupervised machine learning and self-learning AI in a big-data architecture complete with an integrated policy engine. This enables rapid deployment of operational, threat, and compliance objectives and controls, which drive relevant analytics. AI models learn from the continuous flow of data mixed with human feedback.

Outputs include data flows to security tools and MDR services, smart alerts, an investigative UI, and a complete set of automatically built threat, network visibility, and compliance reports. Automated remediation is delivered through IP address or Active Directory account blocking.

Case Study: Agriculture Supply Chain

Challenge

Driven by new, more demanding security standards enforced by major supermarkets, this agricultural coop had to upgrade its cybersecurity and compliance capabilities to those standards to maintain lucrative contracts. Based on ISO27001 controls, the enforcement would not be a "point-in-time" review but require demonstrating processes and KPIs to show continuous security compliance.

Solution

CyGlass NDaaS deployed in under an hour and included pre-built controls, dashboards, and reporting for the ISO27001. Dashboards and reports were easily configured to align with the process and KPIs required by the supermarkets simplifying the ability to show continuous compliance.

Results

The agricultural coop maintained all existing contracts representing millions in annual revenue, while the CyGlass completed with a lower total cost of ownership than estimated.

Case Study: Entertainment Production Supply Chain

Challenge

Motion Picture Association (MPA) supply chain participation includes compliance to a set of NIST 800-53 controls, but security audits from many fellow supply chain vendors meant huge variances in compliance requirements. This proved an impossible deliverable for this 3000-employee production company due to resource constraints and cybersecurity tools limitations. Failing any of these audits could impact revenue into the millions.

Solution

CyGlass NDaaS included all required NIST controls out of the box. More importantly, CyGlass integrated reporting allowed the organization to quickly build dashboards and report variations based on the needs of each audit. Costing 66% less than alternatives, CyGlass deployed in under two hours across 42 sites.

Results

Entertainment company compliance for MPA supply chain requirements was met across multiple audits, coming in well under budget with no lost business.

Conclusions

With award-winning artificial intelligence deployed as a 100% cloud-native architecture, CyGlass NDaaS provides cloud, user, and network threat detection and response that is equally as effective and significantly less to operate than appliance-based legacy NDR tools. Explicitly designed for smaller teams with limited resources to use, CyGlass supports threat detection and response and continuous compliance required for smaller organizations to participate in business-critical digital supply chain ecosystems.