CYNERGY

Continuous Automated Validation & Remediation

Proactive and robust cybersecurity begins with efficient attack surface management. Unfortunately, the increased uptake of technologies, cloud infrastructures, and IoT technologies has seen many companies expand their attack surfaces, causing a nightmare for cybersecurity teams. With numerous applications and cloud assets exposed on the internet, most organizations cannot identify, manage, and control their attack surfaces, yet cyber-attacks continue increasing unabated.

The shortcomings of traditional approaches can expose your organization to costly data breaches. In addition, as most companies shift from office-based work strategies to hybrid and remote working arrangements, real-time discovery and management of exposed assets has never been more crucial. Therefore, organizations require modern and proven solutions to identify, track, manage and secure exposed critical assets.

Fortunately, the Cynergy platform is designed to help organizations discover their assets continuously. With Cynergy, organizations can protect exposed assets through automated external asset discovery, vulnerability assessments, validation, prioritization, and automatic risk mitigation. In addition, the Cynergy platform permits you to discover and control externally exposed web, cloud, and network infrastructure assets and detect data leaks.

Cybersecurity teams can use the Cynergy solution to attain organizational-wide visibility of all assets in real-time. The platform provides an automated risk prioritization to your organization's security needs. The AI-based action plan ensures prioritized activities that reduce your organization's security risks while bringing you closer to compliance with regulations.

"Cynergy is a proven solution that helped our company discover assets and attack surfaces that were undetectable using traditional solutions."

Key Benefits

- Fully automated SaaS solution that does not require any integration, customization, etc.
- Continuous Assets Discovery and Monitoring (CIS 1 & 2)
- PCI Compliance (PCI DSS Regulations 10 & 11)
- GDPR Compliance (Leak Monitoring and Security by design)
- Exploitability validation (BOD 22-01)
- Continuous visibility during incident recovery (NIST - Recover)
- Reduce the risk of unknown assets (blind spots/shadow IT)
- Locate and remediate exposures faster & more effectively
- Better prioritize patch and remediation efforts
- Identify misconfigurations & process failures

Cynergy

Real-time company-wide asset discovery to enable real-time attack surface management.

Learn more at
Cynergy.app

Key Capabilities

Continuous Automated Asset Discovery

Enhanced security starts with continuous identification of all assets as they connect to a network in real-time. The biggest impediment to achieving robust security is the inability to detect exposed assets, and attackers are only too happy to compromise them. You do not have to be a victim since the Cynergy platform continuously detects all assets used in your organization. The platform can assist you in identifying publicly exposed cloud interfaces, websites, leaked employee or customer data, and domains.

Automated Validation

The fight against cyber-attacks and data breaches can drain your company's financial and human resources due to continuously emerging vulnerabilities and adversaries' relentless efforts to breach the organization, execute Ransomware and steal your data. You can only win the fight through continuous asset discovery and validation, which calls for an automated solution that assesses and identifies security risks plaguing your assets. In this case, you can use the SaaS Cynergy platform to run automated risk assessments in all your assets and IT environments. The Cynergy solution automatically verifies all new deployments to detect anything that poses a security risk to your organization. In addition, the solution goes above and beyond to highlight cyber vulnerabilities that require your immediate attention to ensure you are vulnerability-free.

AI-Driven Prioritization

The Cynergy platform prioritizes, and acts based on the identified exploitable vulnerabilities. Unfortunately, most organizations employ manual methods to prioritize all detected vulnerabilities, which is time-consuming and ineffective. Therefore, you will want a solution designed to automatically prioritize and implement an action plan to minimize the most severe vulnerabilities. Your security teams can act on the action plan directly from the Cynergy platform, assign various activities, manage tickers, outsource functions to competent experts, and much more.

Automated Remediation

The time from vulnerability discovery to Patching is critical. Therefore, most of the time of cybersecurity teams goes on Patching and Remediation of vulnerabilities. The Cynergy platform provides several automated mitigation capabilities which are intertwined with the validation process. This way, the risky and vulnerable assets are continuously and automatically discovered. The vulnerabilities validated, prioritized, mitigated, and revalidated to make sure you are protected. Reducing vast amounts of time and effort from the security team, and most of all, saving the company from a possible breach, ransomware, or data leak. The mitigation activities are chosen from thousands of possible activities to ensure an effective AI-based mitigation plan. Also, the platform selects each activity based on risk and impact cost reduction to bring your organization closer to complying with relevant regulations and meet all security demands.

Key Use Cases

With the Cynergy platform, you can prevent and mitigate risks from:

- Compromised credentials
- Cloud exposures and misconfiguration
- Human mistakes and omissions such as phishing and data leaks.
- Vulnerable and outdated software
- Unknown open-source software (OSS)
- Targeted cyber-attacks on your organization
- IT risks inherited from M&A activities
- Legacy and shadow IT assets

Key Features

- Continuous Reconnaissance
- Alerts and Notifications
- Evidence Collection
- Exploitability Validation
- Exploit Trends Identification
- Risk Scoring
- SaaS breach validation
- Multi-Factor Authentication
- Messaging Integrations
- Technology Identification
- Test Scheduling

Cynergy helps your team to answer some important questions:

- **Employee Data Leaks – Raising Awareness**
  Do you know your DevOps manager's credentials were leaked from that website?
  Did you know that your developers put the AWS keys in an open GIT site?
- **Web Applications - Securing Agile Development**
  Did you know about that risky feature your development team deployed 2 days ago?
  Did you know about the new vulnerability in WordPress affecting you marketing website?
  Did you ever know that there is a digital marketing campaign, with a website connected to our domain?
- **Cloud – Securing Your Clint's Data**
  Did you know that we have a publicly exposed bucket in Azure/AWS/GCP?
  Did you know that there is a Blob of sensitive data exposed to the world from one of our instances?
- **Infrastructure – Protecting Your IP**
  Is this subdomain hijackable?
  What are all these services running on a server?
  Can somebody breach us if it is exposed?
- **Vulnerability Assessment, Validation and Prioritization** – Helping your team with:
  - Identify what is the actual risk
  - Focus on what needs to be fixed – eliminating unnecessary Change Management processes which take multiple teams time and effort.

To Summarize

Cynergy empowers organizations and digital businesses to get the security baseline based on the regulation they need to meet, NIST, SOC2, ISO27001 HIPPA, etc.
Cynergy arms every asset you have with infrastructure-independent vulnerability identification capabilities.
Allowing visibility and control over Data, Web Applications, API, Cloud and Infrastructure assets.
Our patent-pending advanced technology utilities tailoring the advisory and prioritization of your preparation activities via advanced machine learning.

Coverage Model

Cynergy had crafted this offered coverage model to answer the current needs of Cynergy' clients, according to information received from the client.

Cynergy solution focuses on providing high visibility to organizations by identifying external facing assets security issues, highlighting, and providing mitigations to discovered security issues, implementing a real-time monitoring and alerting mechanisms while analyzing &

identifying vulnerabilities, improving information security awareness among the organization and its employees, and improving information security aspects in the corporate email system.

- Security Dashboard – High Level visibility on vulnerabilities in Web, Cloud, Infrastructure and Employee credentials breach
- Continuous Asset Scanning – All the external assets Web, Infrastructure, Cloud, and Employees are being scanned for possible dynamic changes, due to shadow IT operations
- Automated Validation - Constantly identifying new 1-day exploits used in the wild and validating them against your network.
- Leak Detection – Detection of secrets exposed to git and paste sites.
- 2 Factor Authentication - Enhanced account security for users
- IP whitelisting – Only specific IPs can access the platform
- Ticketing Integration – integration to organization Slack and Jira
- Reporting – of identified issues via sharable reports
- Data Leak Monitoring and Alerting – Daily monitoring of sensitive data leaked in paste sites, git repositories and employee credentials leaked in web, deep-web and darknet.
- Dedicated Customer Success – Dedicated Cynergy team member who serves as a Point of Contact on a 8*5 basis.
- ***Cloud Integration – integrate and scan your AWS accounts
- Enterprise Billing Support

Technical Spec

- **Technologies**
  - Cloud based platform deployed on AWS
  - Multitenant SaaS
  - Open API
  - VueJS 2.0 Frontend
  - NodeJS Backend
  - Python based Backend scripting
  - Go Lang based Backend scripting

- **Features List**

  Dashboard

  - Infrastructure Assets –
    - Subdomains - Total, Monitored and Exposed to Vulnerable

    - Hosts- Exposed ports per host
  - Cloud Assets –
    - Integrated and identified accounts – Total and Configured for testing
    - Cloud Storage – Identified – Private and Publicly exposed
  - Websites –
    - Identified – Monitored and Vulnerable
    - Behind Web Application or not
    - Screenshots per identified service
    - ML based identification
  - Employees –
    - Number of Identified employees
    - Number of Employees which leaked passwords were identified
    - Number of Employees which have social engineering campaigns configured for

Inventory

- Continuous Asset Scanning – All the external assets (Web, Infrastructure, Cloud, and Employees) are being scanned for possible dynamic changes, due to shadow IT operations
- Infrastructure scanning and testing
  - Passive
    - DNS Subdomain enumeration – Based on OSINT
    - Open Ports Enumeration
    - Insecure Open Ports alerting
    - Hijackable Subdomain test
  - Active
    - DNS Subdomain enumeration
    - Open Ports – Full scan on all TCP and UDP ports
    - DNS Zone Transfer
    - Infrastructure Vulnerability Assessment and Exploitability scan
- Web Application Testing
  - Passive
    - SSL/TLS scan
      - Outdated Protocols
      - Certificate Expiration
      - Weak Ciphers
  - Active – Black-Box, non-authenticated test
    - Scanning of URIs
    - Directory and files enumeration
    - Web-Crawling
    - Dangerous files
    - CGI
    - Outdated server software
    - Java Script – Third party Vulnerabilities
    - Angular Client-Side Template Injection
    - Backup Listing
    - Broken JWT Authentication
    - Broken SAML Authentication

- Login vulnerabilities
- Common Files
- Cookie Security
- Cross Site Request Forgery (CSRF)
- Cross-Site Scripting (XSS)
- Default Login Location
- Directory Listing
- DOM Cross-Site Scripting
- File Upload
- Full Path Disclosure (FPD)
- Headers Security Check
- HTML Injection
- HTTP Method Fuzzing
- Http Request Smuggling
- LDAP Injection
- Local File Inclusion (LFI)
- MongoDB injection
- Open Buckets
- Open Database
- OS Command Injection
- Prototype Pollution
- Remote File Inclusion (RFI)
- Secret Tokens
- Server-Side Template Injection (SSTI)
- Server-Side Request Forgery (SSRF)
- SQL injection (SQLI)
- Unvalidated Redirect
- Version Control System
- WordPress Scan
- XML External Entity (XXE)

- Cloud Exposure Testing
    - Cloud account identification using OSINT tools
    - Amazon Web Services (AWS):
        - Open / Protected S3 Buckets
        - awsapps (WorkMail, WorkDocs, Connect, etc.
    - Microsoft Azure:
        - Storage Accounts
        - Open Blob Storage Containers
        - Hosted Databases
        - Virtual Machines
        - Web Apps
    - Google Cloud Platform (GCP):
        - Open / Protected GCP Buckets
        - Open / Protected Firebase Realtime Databases
        - Google App Engine sites
        - Cloud Functions (enumerates project/regions with existing functions & brute-force function names)
        - S3 enumeration
    - Active
        - AWS account configuration test
- Employee Data Testing
    - Passive
        - Employee Email Discovery – OSINT
        - Employee Leaked Credentials Discovery - OSINT
    - Active
        - Password Spraying against SaaS providers
            - WordPress
            - Atlassian
            - GitHub
            - Okta
            - Gmail SMTP & Gmail Web
            - Microsoft EWS
            - Microsoft MSOL

- - - - - Microsoft O365
        - Microsoft OWA
        - Fortify VPN
  - Data Leak Detection
    - Passive
      - Identification of leaked sensitive API keys and Credentials in:
        - Git-sites
        - Paste sites
- 2 Factor Authentication - Based on Google Authenticator and AWS Cognito Services
- IP whitelisting – Only specific IPs can access the platform – Based on AWS CloudFront and AWS Web Application Firewall.
- Ticketing Integration – integration to organization Slack and Jira
- Reporting – of identified issues via sharable reports in CSV format
- Support – usage support 8*5 during work hours – based on human representatives

ASM Evaluation Matrix

Feature	Feature & Capability	Capability	Criteria	Cynergy Answer
Automated Discovery	External Discovery	The solution requires minimal input to begin the discovery process.	Can the solution automatically discover external assets with little to no configuration?	Comply
	Comprehensive discovery	Automatically discover and monitor assets across IPv4 well as data centre and cloud infrastructure.	Does the solution provide broad asset support? Does the solution provide consistent discovery across asset types? Verify the results by taking a sample of known IPv4, IPv6 and external cloud IPs and making sure they were correctly discovered by the platform.	Comply
	Comprehensive discovery	The platform should give you the capability to input IP address ranges to force discovery for more unusual situations.	Note: ASM solutions commonly do not identify all known assets during initial discovery	Comply
	Detailed service discovery	Enumerate detailed service information for discovered assets, including service name and version running on a system. For select services, configuration information also may be available.	Does the solution provide detailed enumeration of discovered services, including name and version, with the capability to check configuration status either directly or through integration?	Comply
	Detailed artifact discovery	Collect detailed artifacts from monitored assets for each scan.	Does the solution collect detailed artifacts on each discovered asset, such as SSL certificates, screenshots and banners?	Comply
	Suppress	The client has the ability Findings and Assets	Does the solution have the ability to supress ta finding and asset so that it will not appear in future scans?	Comply
Continuous monitoring	Ongoing discovery	Discover new assets in an	Does the solution provide ongoing asset discovery? Review	Comply

		ongoing manner, outside of initial discovery.	the vendor’s methodology for updating the asset database for frequency of updates and data sources used. Prioritize those with weekly updates and those that rely on external data sources (passive DNS, certificates, network registrations) beyond user provided data (IP ranges, domains).	
	Change monitoring	User can monitor and track changes, such as newfound assets and new or impactful changes in risk, to their attack surface over time.	Does the solution provide dashboards and alerts to enable change monitoring?	Comply
	Alerting	Automatically alert users to discoveries or changes on their perimeter via email	Does the solution provide email to alert on critical changes?	Comply requires Integration
		Automatically alert users to discoveries or changes in the Application on their perimeter via email	Does the solution provide In-App to alert on critical changes?	Comply
		Automatically alert users to discoveries or changes on their perimeter via API integration to Ticketing	Does the solution provide API to alert on critical changes?	Comply Requires Integration
	Alerting	Immediate alerts for critical issues, such as newly discovered exploitable software	Does the solution provide email, API and in-app mechanisms to alert on critical Vulnerabilities?	Comply Requires Integration
	False positives and noise reduction	Automatically reduce the number of false positives and filter out noise generated	Does the solution limit noise and present highly confident results? Take a sample of 50 assets and verify that: • The discovered asset does, in fact, belong to your	Comply

		by routine changes in dynamic infrastructure.	organization • The discovered asset is active and not simply IP space or an unresolvable domain assigned to your organization • The risk assessment of that asset appears valid	
	Visibility	Show the user the actions the platform takes to validate a finding	Does the platform show the path for validating the finding?	Comply
Risk-based management	External assessment	Automatically provide an external assessment of risk beyond those provided by vulnerability scanners.	Does the solution leverage a multifactor methodology for external risk assessment, including vulnerabilities, asset prevalence, configuration, and local indicators of weakness (expired certs, default pages, test/dev)?	Comply
	Impact scoring	User may input information about business value as well as remediation and workflow status into the system to develop a prioritized assessment of risk.	Does the solution include built-in functionality for users to adjust and manage risk based on business value and workflow status?	Roadmap Features
Enterprise Management	RBAC (role-based access control)	enabling observer-only roles, such as asset owners, to view and comment on critical information in the solution	Does the solution support RBAC control with permissions for write and read-only users?	Roadmap Feature
	Rule-based policy management for triage	Status and workflow tracking	Does the solution provide an easy-to-use interface for policy driven rule development? Can rules be shared internally across the organization?	Roadmap Feature
	SSO (single sign-on)	manage access to the ASM solution website	Does the solution integrate with your SSO policy?	Roadmap Feature
	Ticketing Integration	Ability to open tickets to Jira and Slack	Does the solution have ticketing mechanism integration	Comply Requires Integration

Interoperability and Integrations	Workflow Automation	Supports third-party integrations and custom development using a provided API.	Does the solution provide a robust API with documentation? Validate API by generating an API token and exporting a list of all IPs. Determine whether the product has demonstrated integrations with external third-party tools, such as API for interfacing with SIEMs.	Roadmap Feature
Reporting	CSV reporting	The platform allows to download CSV reports of the Prioritization, Findings and Risk scoring	The platform allows export of the identified assets via a CSV report	Comply
Credential Leak Detection	Detailed information	The platform allows to identify leaked data of employees	The platform allows to identify the credentials leaked for employees and to verify the exposure	Comply
Data leak detection	Detailed information	The platform allows to identify sensitive API leaks	The platform allows to identify the API keys leaked in paste sites and allows to automatically send a request to remove the entries.	Comply
WAF Scanning	Detailed information	Scan Behind WAF	The platform scans if the assets are behind a WAF	Comply
Technology SBOM	Detailed information	Software Bill of Materials	The platform shows a list of all the technologies used by the organization and related CVEs per technology	Comply

Join Cynergy Now!

Discover, Validate, Remediate