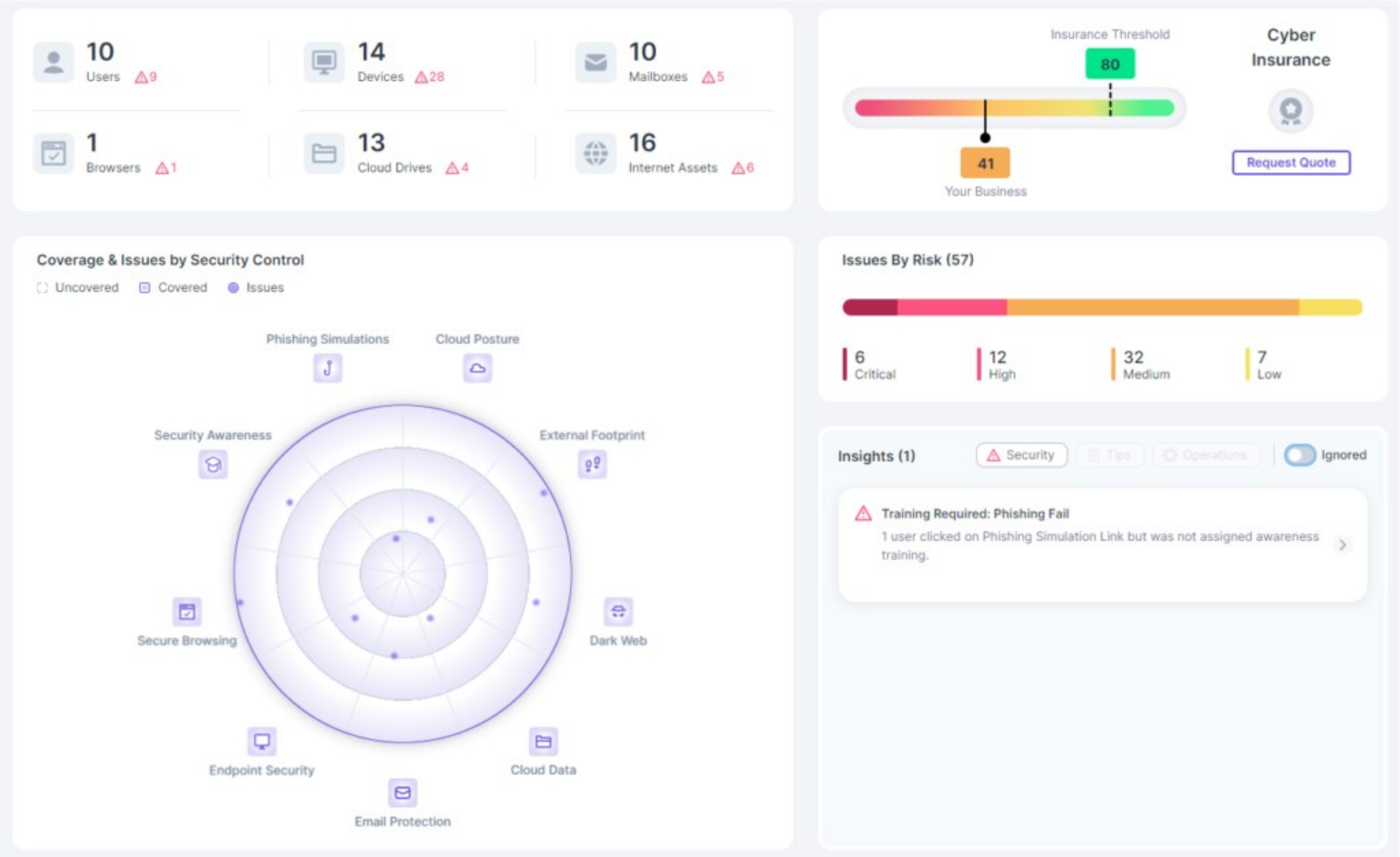
CyberSuite

AIOIntegrations
MANAGED CLOUD SOLUTIONS

CyberSuite 360 Provides Complete Cyber-security Protection

We deliver a solution covering everything from protecting endpoints to training employees. A complete cyber-security solution covers everything from endpoint protection, backup & disaster recovery, device monitoring & management, risk & compliance assessment, 24/7 account activity monitoring, and dark web monitoring.



10 Users ⚠9
14 Devices ⚠28
10 Mailboxes ⚠5
1 Browsers ⚠1
13 Cloud Drives ⚠4
16 Internet Assets ⚠6

Insurance Threshold 80
Your Business 41
Cyber Insurance
Request Quote

Coverage & Issues by Security Control
Uncovered · Covered · Issues

Issues By Risk (57)
6 Critical · 12 High · 32 Medium · 7 Low

Insights (1)
⚠ Training Required: Phishing Fail
1 user clicked on Phishing Simulation Link but was not assigned awareness training.

AI Powered XDR

By using AI at the device level we can catch & prevent zero-day threats from letting hackers into your systems.

Network Security

Continually monitors for abnormal logins and unusual activity to protect against unauthorized access

Awareness Training

Awareness training is one of the most effective breach prevention tools. We educate staff to recognize threats.

Phishing Protection

AIO integrates directly to Microsoft & Google to provide email protection for Phishing and SPAM abuse

Mobile Devices

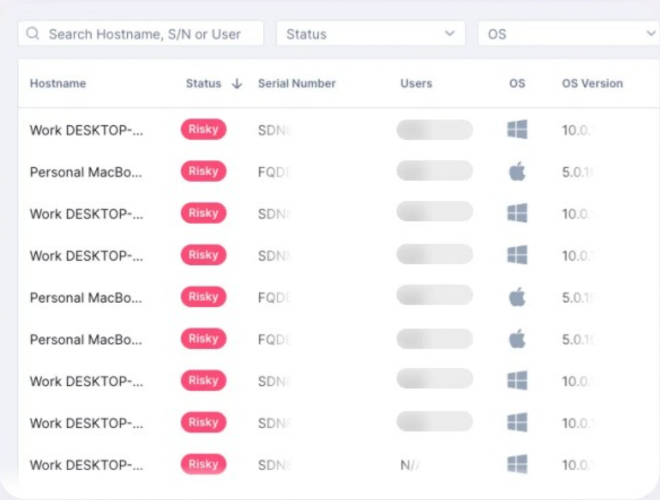
AIO protects all modern Android and Apple SMART Phones & Tablets including Chromebooks

Dark Web Monitoring

Our solution has built-in Dark Web monitoring for all users to monitor for stolen data and credentials

Call (832) 402-1335 or Schedule a Demo at https://get.aiointegrations.com

We manage all elements of Cyber-security through a singular unified backbone based on the most effective tools.



Search Hostname, S/N or User | Status | OS

Hostname	Status	Serial Number	Users	OS	OS Version
Work DESKTOP-...	Risky	SDN			10.0.
Personal MacBo...	Risky	FQD			5.0.1
Work DESKTOP-...	Risky	SDN			10.0.
Work DESKTOP-...	Risky	SDN			10.0.
Personal MacBo...	Risky	FQD			5.0.1
Personal MacBo...	Risky	FQD			5.0.1
Work DESKTOP-...	Risky	SDN			10.0.
Work DESKTOP-...	Risky	SDN			10.0.
Work DESKTOP-...	Risky	SDN	N/		10.0.

Secure All Devices

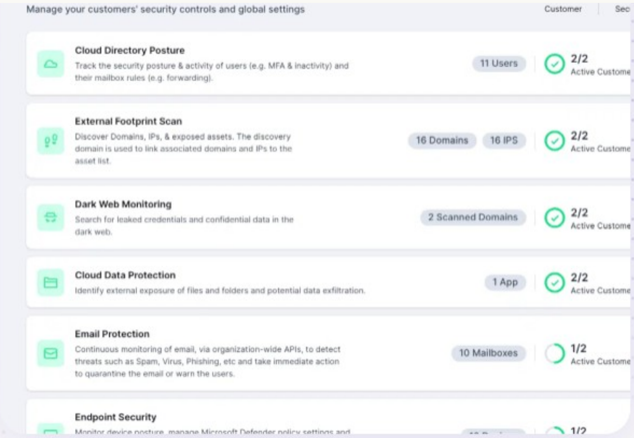
The simplified device management feature offers visibility into devices across an organization, providing vital information on their health status, relevant metrics, threat/risk levels, and existing issues.

This enhances the management of a company's antivirus capabilities and streamlines the process of addressing device-related concerns.

Integrated Security Controls in One Backbone

The Guardz Security Controls are a reflection of the holistic approach to cybersecurity, putting the core safeguards in one place while simplifying the setup and management of these critical controls.

This centralized view of Guardz Security Controls enables hassle-free configuration for each control, ultimately simplifying security implementation and issue resolution in a breeze.



Manage your customers' security controls and global settings

Cloud Directory Posture
Track the security posture & activity of users (e.g. MFA & inactivity) and their mailbox rules (e.g. forwarding).
11 Users — 2/2 Active Custome

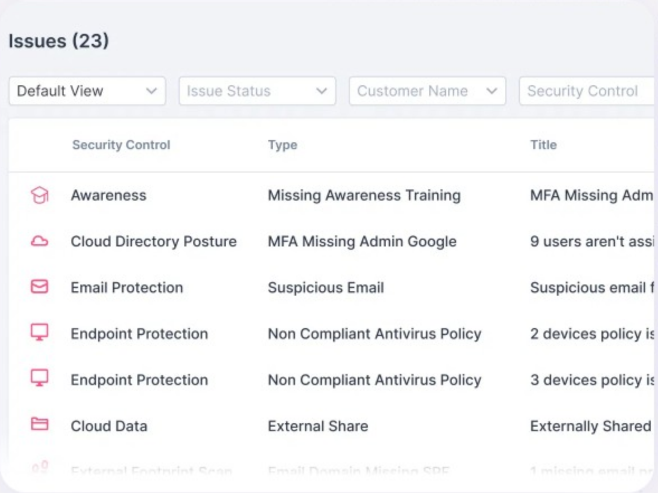
External Footprint Scan
Discover Domains, IPs, & exposed assets. The discovery domain is used to link associated domains and IPs to the asset list.
16 Domains — 16 IPS — 2/2 Active Custome

Dark Web Monitoring
Search for leaked credentials and confidential data in the dark web.
2 Scanned Domains — 2/2 Active Custome

Cloud Data Protection
Identify external exposure of files and folders and potential data exfiltration.
1 App — 2/2 Active Custome

Email Protection
Continuous monitoring of email, via organization-wide APIs, to detect threats such as Spam, Virus, Phishing, etc and take immediate action to quarantine the email or warn the users.
10 Mailboxes — 1/2 Active Custome

Endpoint Security
Monitor device posture, manage Microsoft Defender policy settings and
1/2



Issues (23)

Security Control	Type	Title
Awareness	Missing Awareness Training	MFA Missing Adm
Cloud Directory Posture	MFA Missing Admin Google	9 users aren't assi
Email Protection	Suspicious Email	Suspicious email f
Endpoint Protection	Non Compliant Antivirus Policy	2 devices policy is
Endpoint Protection	Non Compliant Antivirus Policy	3 devices policy is
Cloud Data	External Share	Externally Shared
External Footprint Scan	Email Domain Missing SPF	1 missing email p

Single View of All Issues

Guardz continuously scans for threats across multiple attack vectors and generates issues when a threat is detected. Issues are prioritized by severity of risk and include all the relevant details to trigger automated and manual remediations.

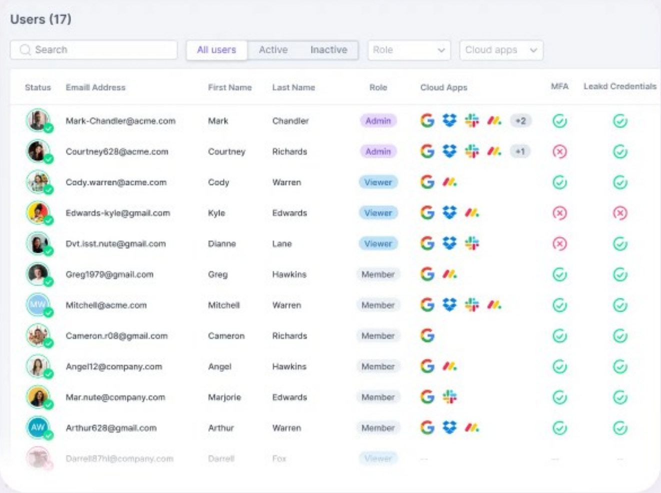
See more specific information about the issue, choose the most suitable remediation, and complete the action to resolve the issue.

Integrated Awareness Training, Simulated Phishing, Email Protection, and Detailed Reporting on Cyber Events & Employee Training

Users are the First Line of Defense

Users are at the center of defining an organization's risk, so Guardz aggregates user-level data to paint a picture of employee risk and its impact on the company.

A company's cloud directory (Google or Microsoft) is the source of the user list and is enriched with data about licensing, role, cloud apps, issue status, related devices, and more.



Users (17)

Status	Emaill Address	First Name	Last Name	Role	Cloud Apps	MFA	Leakd Credentials
✓	Mark-Chandler@acme.com	Mark	Chandler	Admin	G +2	✓	✓
✓	Courtney628@acme.com	Courtney	Richards	Admin	G +1	✗	✓
✓	Cody.warren@acme.com	Cody	Warren	Viewer	G	✓	✓
✓	Edwards-kyle@gmail.com	Kyle	Edwards	Viewer	G	✗	✗
✓	Dvt.isst.nute@gmail.com	Dianne	Lane	Viewer	G	✗	✓
✓	Greg1979@gmail.com	Greg	Hawkins	Member	G	✓	✓
MW ✓	Mitchell@acme.com	Mitchell	Warren	Member	G	✓	✓
✓	Cameron.r08@gmail.com	Cameron	Richards	Member	G	✓	✓
✓	Angel12@company.com	Angel	Hawkins	Member	G	✓	✓
✓	Mar.nute@company.com	Marjorie	Edwards	Member	G	✓	✓
AW ✓	Arthur628@gmail.com	Arthur	Warren	Member	G	✓	✓
	Darrell87hl@company.com	Darrell	Fox	Viewer	--	--	--

Enhanced Phishing Simulations

Real-time Alerts

See in real-time the interactivity between employees and the simulation and gain insight into who passed and who failed

The Power of AI

Instead of dealing with a library of outdated predefined emails, utilize the latest large language model to generate an email based on your custom inputs

Customized Campaigns

Input your preferences based on industry, tone, style, length, and language to generate on-the-fly content to fit a specific audience, and if you are unhappy, regenerate

Automated Scheduling

Utilizing automation, you can schedule the start and end dates for the Phishing Simulation. Upon completion of the simulation, an issue summarizing the results achieved will be generated

Soft Landing

Users who click the link receive a polite yet firm alert, notifying them that they have not passed the simulation. This warning is followed by an awareness training session

POWERED BY

Guardz.

SentinelOne

Gartner — Magic Quadrant™ Leader Four Years in a Row

MITRE ENGENUITY — #1 for Protection Across All MITRE Evaluations

G2 — Industry's Most Awarded Cloud Security Suite