STRATEGY & COMPLIANCE

Secure. Compliant. Cost Effective.

Practical IT, cybersecurity, compliance and risk guidance for Hawaii organizations

Rodney Baba • Chris Aliipule

strategyandcompliance.com

Local relationships. Enterprise-grade thinking. Right-sized execution.

Two complementary leaders. One practical mission.

Strategy and execution come together through a shared commitment to Hawaii organizations.

Chris Aliipule — Technology & Operations

- vCIO and systems engineering leadership
- Infrastructure, cloud, resiliency and IT modernization
- Turns business needs into reliable, supportable technology
- Strong operator who understands cost, continuity and day-to-day realities

Rodney Baba — Security, Risk & Compliance

- vCISO, compliance and security architecture leadership
- CISSP, CCSP and CISM; deep governance and risk experience
- CMMC, NIST, HIPAA, WISP and policy/evidence programs
- Translates complex requirements into clear, sustainable action

Built around Hawaii's business 'ohana

We partner closely, communicate plainly and take ownership of outcomes.

Business-first

Start with goals, risk and constraints—not a product catalog.

Right-sized

Use the smallest effective technology footprint.

LOCAL PARTNERSHIP

Hands-on

Stay engaged from assessment through evidence and improvement.

Trusted

Bring enterprise experience without enterprise bureaucracy.

"Unexpected outcomes" means making IT more efficient, secure, compliant and cost effective—at the same time.

Where we are already helping

Current engagements span regulated and mission-critical organizations.

Healthcare

HIPAA, risk, security operations

Financial & CPA

WISP, client-data protection, evidence

Utilities

Resilience, governance, vendor risk

Nonprofit

Practical controls with limited resources

Architecture & Professional Services

CMMC Level 1/2, FCI/CUI, cloud and client data, CIS, NIST

One model. Adapted to each organization.

CMMC is a core part of our current compliance work

Alongside WISP, we are actively helping architecture and related firms prepare for CMMC Level 1 and Level 2 obligations.

CMMC Level 1

- Protect Federal Contract Information (FCI)
- Establish foundational cyber hygiene
- Prepare for self-assessment and evidence
- Make requirements practical for small teams

CMMC Level 2

- Address CUI and NIST SP 800-171 alignment
- Build SSP, POA&M and evidence workflows
- Coordinate with both On-Prem, Cloud and Enclave workflows
- Coordinate with assessors or enclave providers
- Keep the program sustainable

How we help

- Rapid gap reviews
- Right-sized policies
- Evidence packages
- Governance cadence
- Technology remediation
- Ongoing readiness support

Our message: WISP is one important service line; CMMC Level 1/2 support for architecture and related firms is a major, active part of our customer work.

Sources: DoD CMMC overview; DCSA CMMC guidance. Requirements and implementation timelines continue to evolve; readiness work still matters.

CMMC for architecture & related firms: readiness matters now

DoD cyber requirements are moving into contract expectations; firms handling FCI or CUI need evidence, governance and a repeatable compliance program.

Federal baseline

DFARS/NIST obligations require safeguarding defense information, reporting incidents and maintaining strong security practices.

Dec. 16, 2024

CMMC Program Rule became effective, establishing levels, assessment types, affirmations and evidence expectations.

Nov. 10, 2025

DoD began the CMMC contract phase-in, with Level 1 and Level 2 self-assessment requirements entering applicable solicitations.

Current status

Phase II third-party certification timing is evolving; Phase I self-assessment requirements remain in place, so readiness still matters.

Do not wait for prime-contractor flow-down, SPRS pressure or an assessment request. Build the SSP, POA&M, evidence library and remediation plan now.

Sources: DoD CIO CMMC guidance; 32 CFR Part 170 CMMC Program Rule; DoD CMMC FAQs. Requirements and implementation timelines continue to evolve.

CPA and tax firms: WISP is not optional

The requirement is established; expectations for demonstrable, ongoing compliance are increasing.

Federal baseline

FTC Safeguards Rule requires a written information-security program for covered financial institutions.

2023

Major revised safeguards requirements became effective.

May 13, 2024

Certain covered firms became subject to FTC breach-reporting obligations.

Dec. 6, 2024

IRS again emphasized that tax professionals are legally required to maintain a WISP.

Do not wait for an incident, insurer questionnaire or regulatory review. Build the program—and preserve the evidence—now.

Sources: FTC Safeguards Rule guidance; IRS Tax Tip 2024-93 (Dec. 6, 2024); IRS Publications 5708/5709.

What customer information must be protected?

Think broadly: nonpublic information connected to an identifiable client or taxpayer.

Identity

Social Security numbers, taxpayer IDs, dates of birth, driver-license or passport data

Financial

Income, banking, account, investment, payroll and tax-return information

Access

Passwords, authentication data, security questions and account credentials

Business records

Contracts, invoices, ownership information and other confidential client records

Communications

Email, documents, portals and files containing nonpublic client information

Derived data

Reports, analytics, exports, backups and evidence that reproduce sensitive information

Protection follows the data—from collection and use through storage, sharing, backup and disposal.

From “we should” to Compliant—and audit ready - CMMC/WISP/CIS

A rapid, practical model combining policy, technology, automation and recurring evidence.

1

Evaluate

Inventory data, systems, risks, vendors and existing controls.

2

Design

Create the right-sized policies, roles and remediation roadmap.

3

Implement

Apply security tools, configurations, training and procedures.

4

Evidence

Collect screenshots, reports, logs, approvals and review records.

5

Sustain

Monitor risk, review controls, update evidence and manage exceptions.

Our advantage: reusable compliance tools, automation, AI-assisted workflows and experienced judgment accelerate the first pass—without sacrificing ongoing governance.

Cyber insurance works better when risk is actively managed

Coverage, monitoring and remediation can reinforce one another.

Through relationships with cyber-insurance providers such as Coalition, we can help clients improve security posture, strengthen underwriting readiness and manage total risk cost.

Coalition describes "Active Insurance" as combining cyber coverage, security technology, monitoring and response services.

Why engage Strategy & Compliance?

Because security and compliance should support the business—not overwhelm it.

Lower total cost

Reduce tool sprawl, duplicated services and avoidable consulting overhead.

Business-owner perspective

We understand limited time, limited staff and the need for measurable value.

Faster progress

Use tested methods, templates and automation to move rapidly.

Independent guidance

We recommend what fits—not simply what a vendor wants to sell.

Better readiness

Maintain evidence and operating discipline before an audit or incident.

Faith-informed partnership

Serve with integrity, stewardship, humility and commitment to the customer.

The smallest technology footprint that delivers the biggest practical impact.

Start with a practical evaluation.

We will help you understand where you are, what matters most and what it will take to become—and remain—secure, compliant and audit ready.

1 **Initial conversation**

2 **Focused evaluation**

3 **Prioritized estimate & roadmap**

Rodney Baba • Chris Aliipule

strategyandcompliance.com

Efficient • Secure • Compliant • Cost Effective

STRATEGY & COMPLIANCE

Compliance Assessment Suite

Select a framework to begin or resume an assessment

FRAMEWORKS

CMMC →

CMMC / NIST SP 800-171

Cybersecurity Maturity Model Certification for US defense contractors handling Controlled Unclassified Information.

L1 · L2 · L3 · Enclave support · SPRS scoring · SSP & POA&M

ISO 27001 →

ISO 27001:2022

International Information Security Management System standard. 93 controls across 4 themes. Certification body audit pathway.

93 controls · 4 themes · Annex A · Policy suite

METI CMG →

METI CMG v3.0

Japan METI/IPA Cybersecurity Management Guidelines for Japanese enterprises and supply chain partners.

35 controls · 7 domains · 10 Directions · Japan market

CIS Controls →

CIS Controls v8.1

CIS Critical Security Controls — 18 controls covering basic cyber hygiene across asset management, identity, vulnerability, threat defense, and incident response.

18 controls · 8 groups · IG1/IG2 · Basic Cyber Hygiene

WISP →

WISP — CPA/Tax Practice

Written Information Security Plan for solo and small CPA/tax practices. FTC Safeguards Rule (16 CFR §314) / Gramm-Leach-Bliley Act compliance. Generates your complete WISP plus all required Attachments A–F.

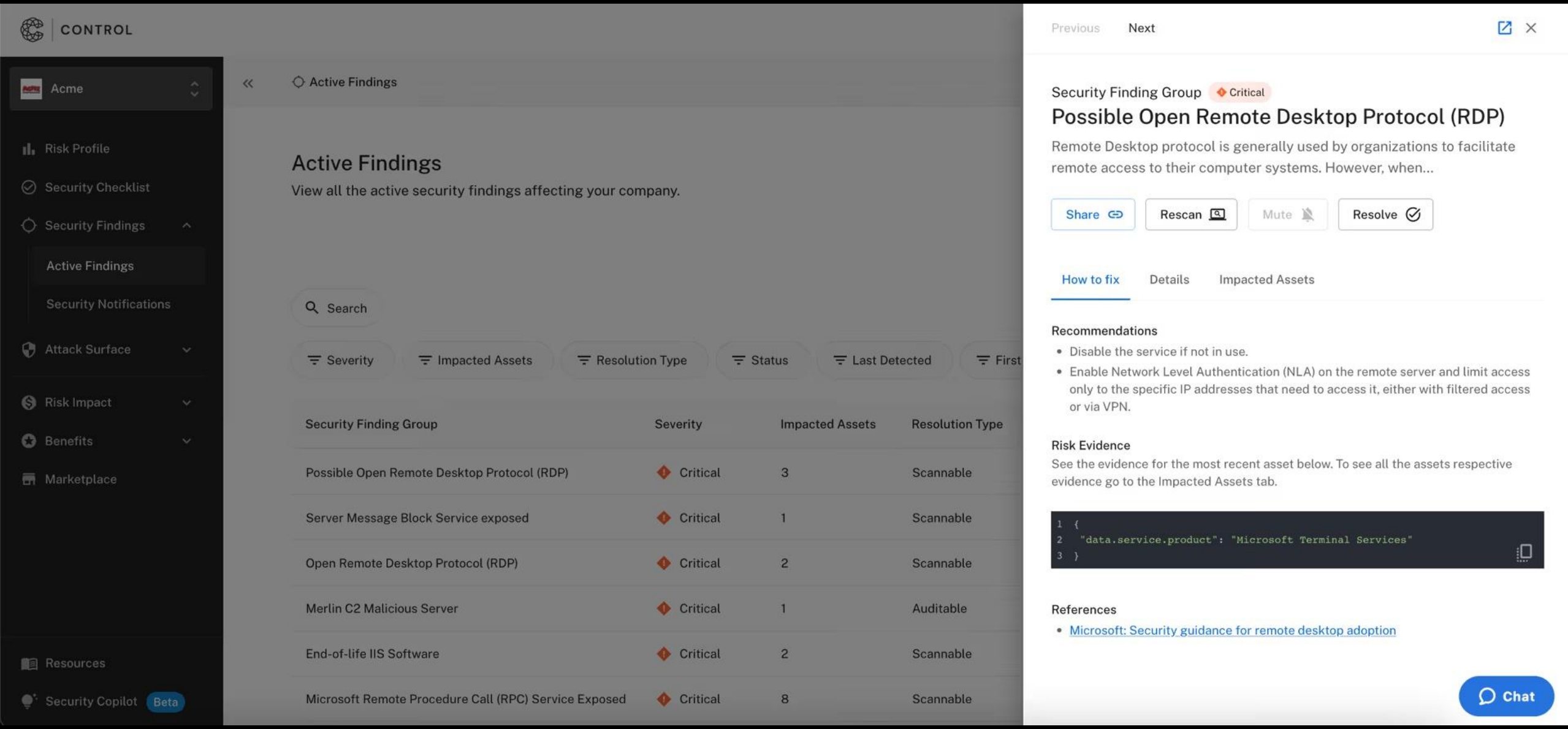
42 controls · 12 domains · 16 CFR §314 · GLBA · IRS Pub. 5708

Resilience →

Operational Resilience

Five-domain Immune System framework covering governance, business continuity, IT disaster recovery, incident response, and cyber controls.

GOV · BCP · ITDR · IRES · CYBER · ISO 22301


CONTROL
Acme
Risk Profile
Security Checklist
Security Findings
Active Findings
Security Notifications
Attack Surface
Risk Impact
Benefits
Marketplace
Resources
Security Copilot
Beta
Active Findings
Active Findings
View all the active security findings affecting your company.
Search
Severity
Impacted Assets
Resolution Type
Status
Last Detected
First
Security Finding Group
Severity
Impacted Assets
Resolution Type
Possible Open Remote Desktop Protocol (RDP)
Critical
3
Scannable
Server Message Block Service exposed
Critical
1
Scannable
Open Remote Desktop Protocol (RDP)
Critical
2
Scannable
Merlin C2 Malicious Server
Critical
1
Auditable
End-of-life IIS Software
Critical
2
Scannable
Microsoft Remote Procedure Call (RPC) Service Exposed
Critical
8
Scannable
Previous
Next
Security Finding Group
Critical
Possible Open Remote Desktop Protocol (RDP)
Remote Desktop protocol is generally used by organizations to facilitate remote access to their computer systems. However, when...
Share
Rescan
Mute
Resolve
How to fix
Details
Impacted Assets
Recommendations
Disable the service if not in use.
Enable Network Level Authentication (NLA) on the remote server and limit access only to the specific IP addresses that need to access it, either with filtered access or via VPN.
Risk Evidence
See the evidence for the most recent asset below. To see all the assets respective evidence go to the Impacted Assets tab.
{
"data.service.product": "Microsoft Terminal Services"
}
References
Microsoft: Security guidance for remote desktop adoption
Chat

Acme

Risk Profile
Security Checklist
Security Findings
Active Findings
Security Notifications
Attack Surface
Risk Impact
Benefits
Marketplace

Resources
Security Copilot Beta

Acme acme.com

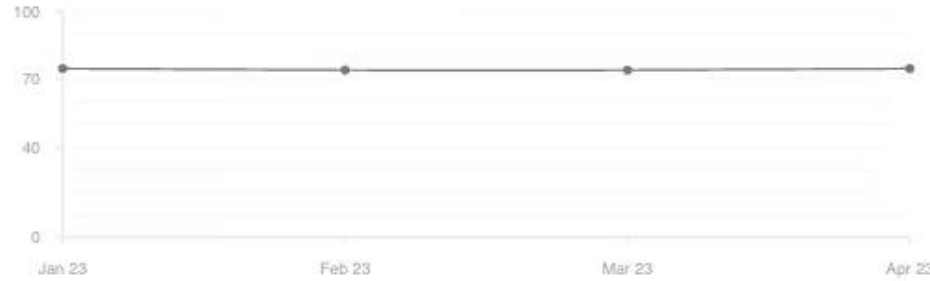
Download Report

Risk Score

Equal to previous scan

Low (<40) Medium (40-70) High (>70)

Risk Score Trend



Your company is at a high risk level!

To improve your Risk Score fix all critical and high security findings and review and update your domains.

Security Findings

Critical (17)

By category

Attack Surface

Assets

Domains See all

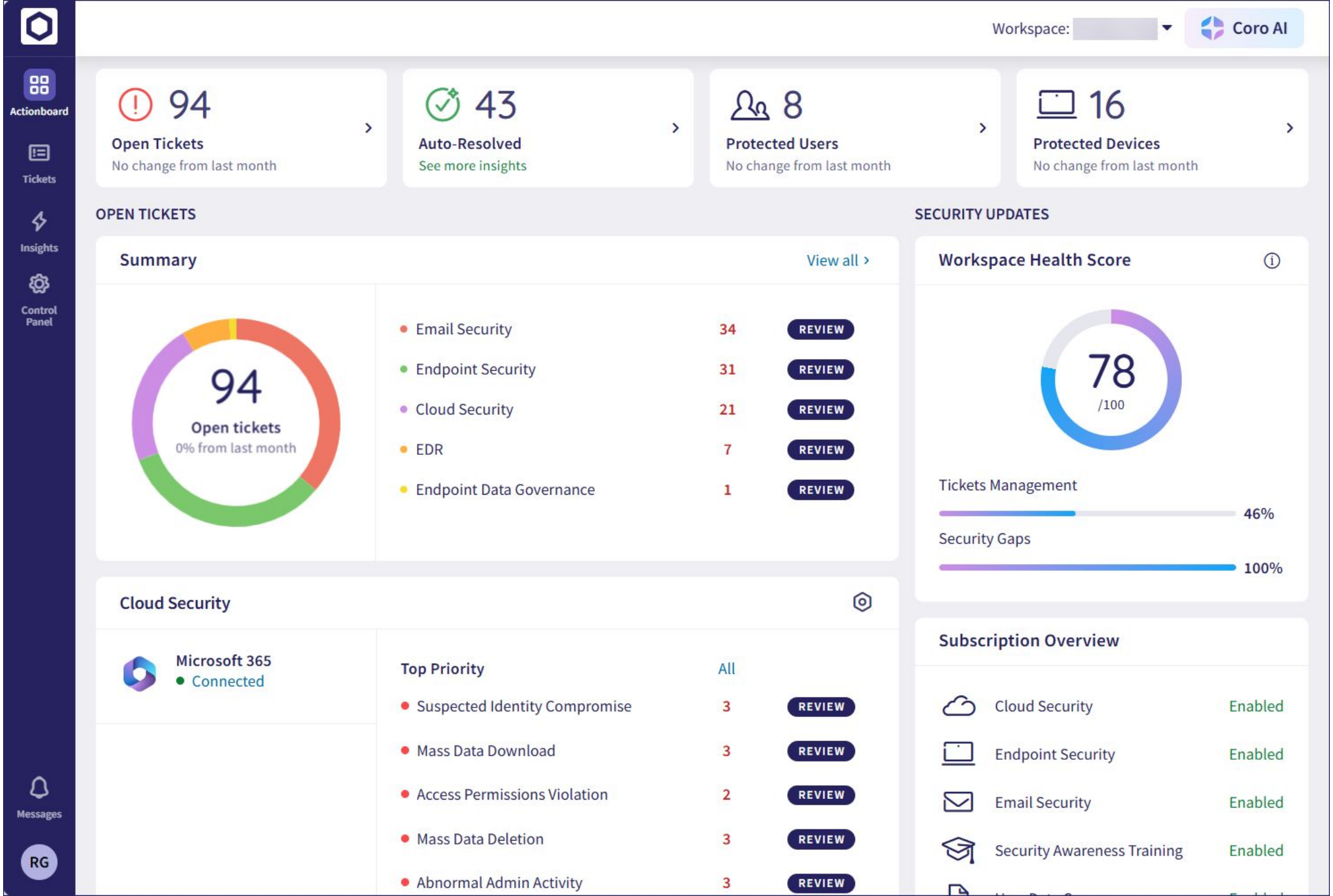
7	7
Impacted	Total

IP Addresses See all

11	28
Impacted	Total

Growth History

Chat


Workspace:
Coro AI
Actionboard
Tickets
Insights
Control Panel
Messages
RG
94
Open Tickets
No change from last month
43
Auto-Resolved
See more insights
8
Protected Users
No change from last month
16
Protected Devices
No change from last month
OPEN TICKETS
Summary
View all
94
Open tickets
0% from last month
Email Security 34 REVIEW
Endpoint Security 31 REVIEW
Cloud Security 21 REVIEW
EDR 7 REVIEW
Endpoint Data Governance 1 REVIEW
Cloud Security
Microsoft 365
Connected
Top Priority
All
Suspected Identity Compromise 3 REVIEW
Mass Data Download 3 REVIEW
Access Permissions Violation 2 REVIEW
Mass Data Deletion 3 REVIEW
Abnormal Admin Activity 3 REVIEW
SECURITY UPDATES
Workspace Health Score
78
/100
Tickets Management
46%
Security Gaps
100%
Subscription Overview
Cloud Security Enabled
Endpoint Security Enabled
Email Security Enabled
Security Awareness Training Enabled

ninjaOne

Search

Dashboard
Search
Configuration
Favorites
- Najera Construction Inc.
- Software Development Inc.
- Clean Teeth DDS

Recent
- Ninja's Mac 51 local
- Dr. Walsh's Workstavtion
- Clean Teeth DDS
- SFP0S02
- SFP0S01
- Software Development Inc.
- Firewall Netflow

DASHBOARD

Getting Started | Organizations | Software | OS Patches | Ticketing | Documentation | Backup

All (7) Healthy (3) Problems (4) Sort By: Status

Filter by Organization Name

Clean Teeth DDS
15 servers, 265 desktops, 3 remote

Best Health Physician Group
2 servers, 22 desktops, 15 remote

Regional Autosales LLC
10 servers, 62 desktops, 5 remote

Software Development LLC
95 servers, 325 desktops, 1 remote

Internal Infrastructure
1 server, 1 VM Host, 25 VM Guests

Najera Construction Inc.
1 server, 4 desktops, 4 cloud

Maine Manufacturing Inc.
6 servers, 116 desktops, 22 cloud

Device Health

Servers	1	
Active	0	Quarantined 0
Failed	0	Pending 3
Failed	0	Pending 2
Devices	5	Cloud 0
Requiring Reboot	1	Install Issues 1
Pending	0	Approved 56
VM Host(s) Down	1	

Devices Running Actions

OS Patch Management
Software Patch Management
Backup Action Antivirus
TeamViewer Virtualization

System Events for the Last Week

Device SFPOS01 update by Peter Bretton

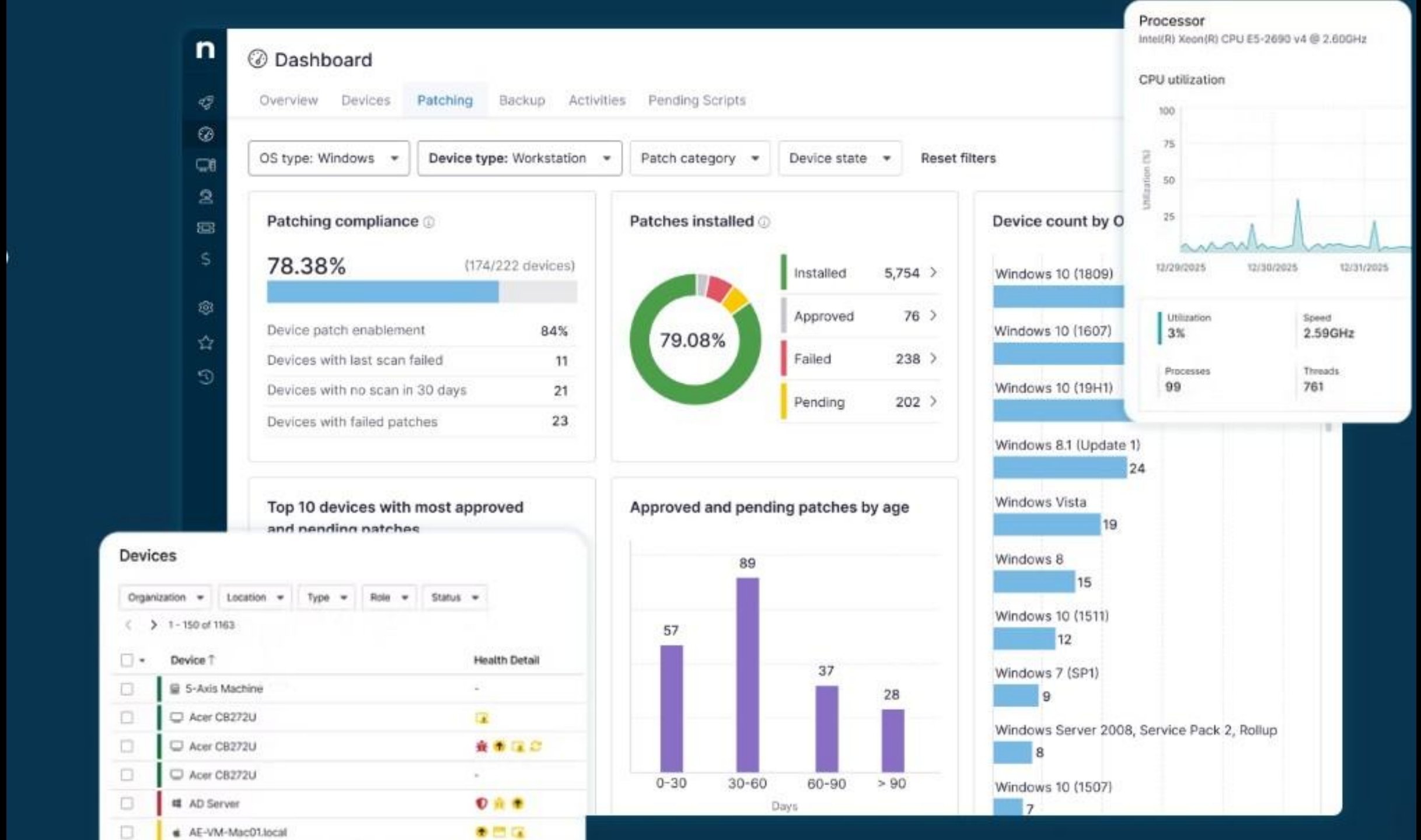
Device Construction Manager JS2 Laptop updated by Peter Breton

Device Construction Manager JS1 Laptop updated by Peter Breton

Device Jonathan's Workstation note deleted by Peter Bretton

Device RAIDSERVER01 updated by Sascha Kabalawi

Device Projects Server note updated by Christopher Serpico.


Dashboard
Overview
Devices
Patching
Backup
Activities
Pending Scripts
OS type: Windows
Device type: Workstation
Patch category
Device state
Reset filters
Patching compliance
78.38%
(174/222 devices)
Device patch enablement 84%
Devices with last scan failed 11
Devices with no scan in 30 days 21
Devices with failed patches 23
Patches installed
79.08%
Installed 5,754
Approved 76
Failed 238
Pending 202
Device count by O
Windows 10 (1809)
Windows 10 (1607)
Windows 10 (19H1)
Windows 8.1 (Update 1) 24
Windows Vista 19
Windows 8 15
Windows 10 (1511) 12
Windows 7 (SP1) 9
Windows Server 2008, Service Pack 2, Rollup 8
Windows 10 (1507) 7
Top 10 devices with most approved and pending patches
Approved and pending patches by age
57
89
37
28
0-30
30-60
60-90
> 90
Days
Processor
Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz
CPU utilization
100
75
50
25
Utilization (%)
12/29/2025
12/30/2025
12/31/2025
Utilization 3%
Speed 2.59GHz
Processes 99
Threads 761
Devices
Organization
Location
Type
Role
Status
1 - 150 of 1163
Device
Health Detail
5-Axis Machine
Acer CB272U
Acer CB272U
Acer CB272U
AD Server
AE-VM-Mac01.local