CYVATAR.AI

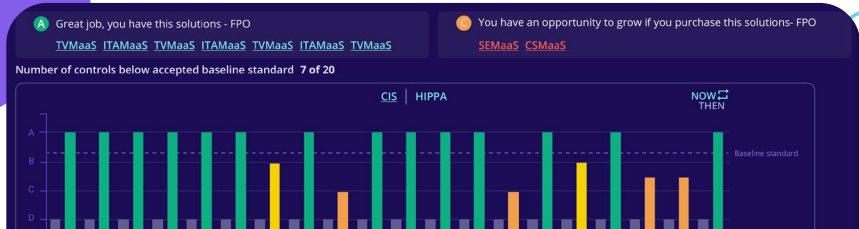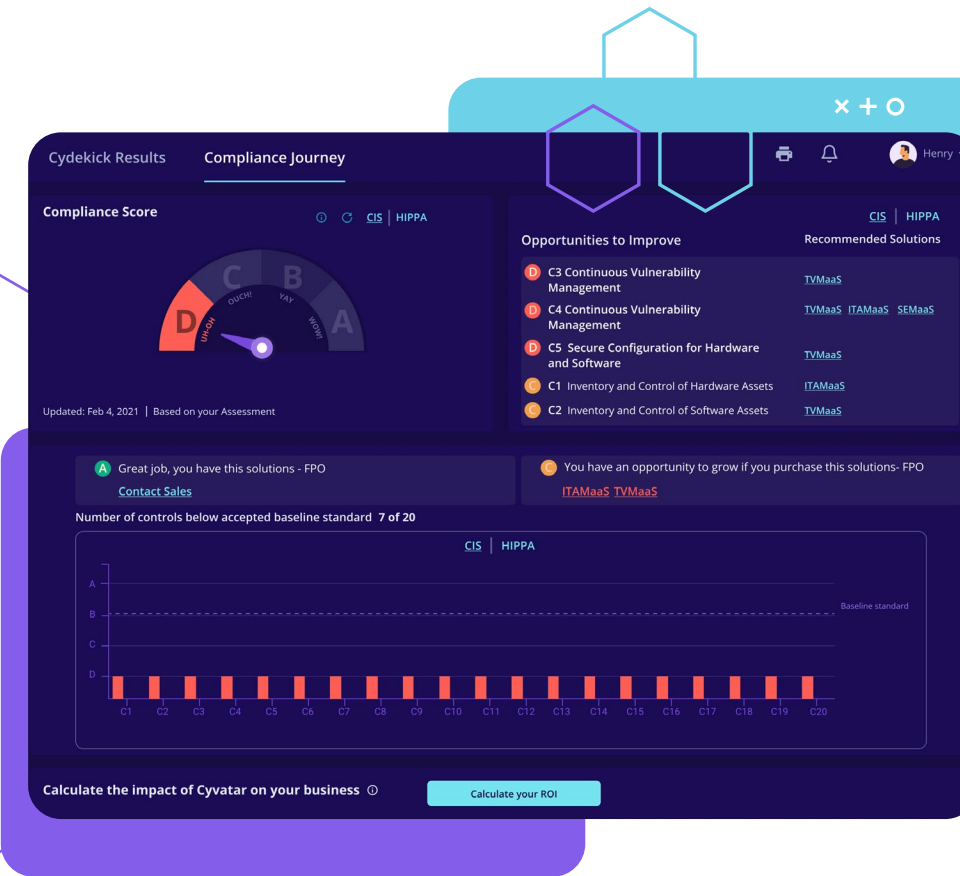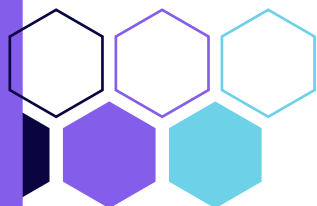# Effortless Cybersecurity for Startups & SMBs.

Cybersecurity Solutions Portfolio & Overview

Table of Contents

About Cyvatar

Cyvatar's cybersecurity-as-a-service and automated security operations platform enables startups and small businesses to effectively deploy and maintain data security while building trust, gaining transparency into operations, and accelerating business growth.

Cybersecurity can seem overwhelming and expensive for small businesses, and many end up deferring it. Cyvatar makes cybersecurity accessible, achievable, and cost-effective for our members by managing and unifying their security technologies, eliminating complex tasks with automation, and reducing risk -- in one simple subscription. We believe businesses of every shape and size deserve access to world-class security outcomes, and we're always ready to deliver. Learn more and get started with effortless cybersecurity at cyvatar.ai.

We believe businesses of every shape and size deserve access to world-class security, and we're always ready to deliver.
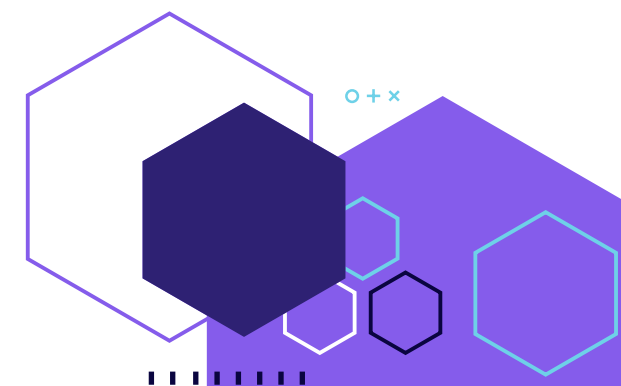
What Can Cyvatar Do for You?

UNIFIED CYBERSECURITY SOLUTION
All your security tools & data in one place. Say goodbye to multiple vendor management and dozens of open tabs.

FULLY MANAGED CYBERSECURITY-AS-A-SERVICE
Access to security solutions, proven processes, and skilled practitioners to run your security strategy.

AUTOMATE SECURITY OPERATIONS
From assessment to installation, configuration, remediation, and continuous maintenance.

BUILD TRUST & TRANSPARENCY
Be in the know of what's happening with your security operations, measure ROI, and streamline compliance.

ACCELERATE SALES & GROW SECURELY
Earn trust with existing and prospective customers by having the proper data security and compliance in place.

Threat & Vulnerability Management

Continuously identify and remediate vulnerabilities across your organization.

When it comes to best practices for cybersecurity, a prevention-based strategy is key. For small businesses, managing vulnerabilities in-house is rarely done comprehensively due to lack of resources and budget, exposing your business to vulnerabilities. Additionally, a single point-in-time penetration test is useless if vulnerabilities aren't remediated timely.

You need continuous monitoring, scanning, and remediation; not to mention penetration testing and meeting compliance requirements.

Assessing and remediating vulnerabilities present in your network can detract focus from your growing business and can be time consuming for your team to manage.

Cyvatar's Threat & Vulnerability Management solution encompasses the entire lifecycle, from product selection to maintenance, with a preventative approach keeping your network secure and your business operational!

CYVATAR'S TVM SOLUTION INCLUDES:

- Solution installation, configuration, assessment, and maintenance
- Continuous vulnerability scanning
- Risk management
- Patch management
- Remediation operations
- Maintenance of the remediated status
- Quarterly automated external network penetration assessments
- Monthly executive reporting

CORE SOLUTION

Secure Endpoint Management

Security solutions that utilize AI and antivirus to secure and lock down entry points of user devices from being exploited by cyberattacks.

In cybersecurity, detecting and responding to threats is not optimal for securing business infrastructure, especially in a ransomware scenario. Once an incident has been detected, it's already too late.

In fact, by 2021, it was estimated that a ransomware attack would occur every 11 seconds (compared to every 14 seconds in 2020). Source: 2020 DBIR

Ransomware is increasing because it works. Most companies are misconfigured on the endpoint, which allows ransomware to execute—the result of a flawed, reactive strategy of detecting and responding to threats.

No cybersecurity company can promise you won't get compromised, but they should offer measurably better security and next-level antivirus solutions that will configure your environment to a preventative state, reducing the threat landscape. A secure endpoint management solution maintains a locked down and preventative state mitigating ransomware or any other malware-based attack.

Cyvatar's Secure Endpoint Management solution brings your company to a proactive, preventative, and locked down state that won't disrupt your business operations.

CYVATAR'S ENDPOINT SECURITY SOLUTION INCLUDES:

- IT asset & endpoint monitoring
- Monitor & remediate zero-day exploits
- Ransomware protection
- Endpoint software installation and configuration on each individual device
- 24/7 Security Operation Center (SOC) monitoring
- Remediation operations
- Maintenance of the remediated status
- Monthly executive reporting

CORE SOLUTION

Cloud SaaS Management

Gain visibility to detect and remediate vulnerabilities. Secure cloud-based applications like Salesforce, Slack, Outlook, AWS, G-Suite, Azure, and more.

Cloud SaaS (software-as-a-service) applications are here to stay and your organization is using them over network-based assets, which puts your business at greater risk than ever. The cybersecurity you need to protect your data simply doesn't come as standard with cloud-based licenses.

It's imperative you ensure only authorized users (and relevant third-party apps) gain access to cloud SaaS tools and your data within them.

Bridge the gap and gain the cloud visibility your organization needs to stay secure with Cyvatar's Cloud Security SaaS Subscription. There's no longer a need to utilize SaaS applications in the dark with proactive ongoing remediation.

Cyvatar solves your cloud security challenges with the right technology, the right services, and continuous management; all within a single subscription.

CYVATAR'S CLOUD SAAS MANAGEMENT SOLUTION INCLUDES:

- Solution installation, configuration, assessment, and maintenance of the remediated status
- Threat Management:
  - ↳ Analyze user behavior to detect account takeover and insider threats
  - ↳ Monitor for malicious integrations to your core SaaS applications
  - ↳ Continuously monitor for threats with AI-powered models and custom detections
  - ↳ Triage quickly with a unified timeline of events across attack stages and applications
- SaaS application posture Management:
  - ↳ Identify and reduce sensitive publicly exposed data
  - ↳ Reduce over-privilege by flagging unused permissions or deviations from a peer group
  - ↳ Save costs by identifying inactive licensed accounts
  - ↳ Optimize configurations across SaaS applications from a single interface
  - ↳ Quantify misconfiguration risk with context on users and activities related to each control
  - ↳ Identify divergence from industry benchmarks and best practice
- Monthly executive reporting

CORE SOLUTION

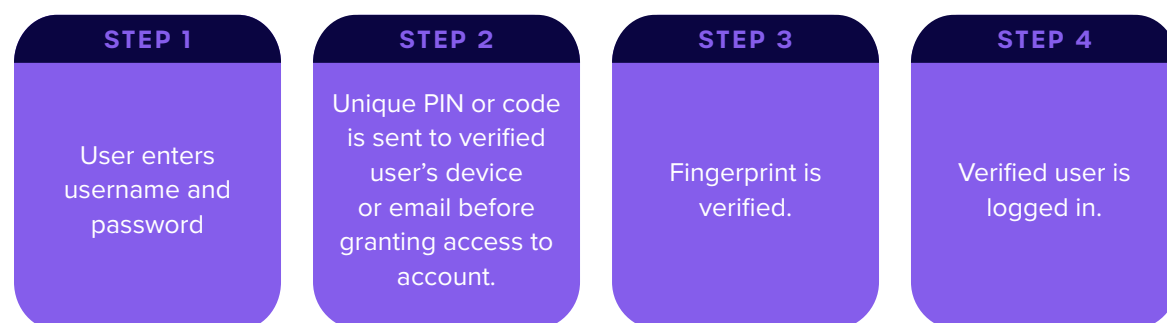# Multi-factor Authentication Management

Multi-layered Secure User Management

Multi-factor Authentication (MFA) is a multi-step authentication method that requires the user to provide two or more verifications to gain access to a device, account, VPN, etc. MFA is a core foundation of strong prevention-based cybersecurity strategy. Instead of just requiring a password, which can easily be compromised, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber attack.

Multifactor authentication credentials fall into any of these three categories:

1. Something you know (like a password or PIN)
2. Something you have (like a phone or smart card)
3. Something you are (like a fingerprint)

EXAMPLE: MFA IN ACTION

STEP 1	STEP 2	STEP 3	STEP 4
User enters username and password	Unique PIN or code is sent to verified user's device or email before granting access to account.	Fingerprint is verified.	Verified user is logged in.

CYVATAR'S MFA SOLUTION INCLUDES:

- Solution installation, configuration, assessment, remediation, and maintenance of remediated state
- Secure cloud Single Sign On (SSO) solution compatible with apps like Outlook 365, Slack, AWS, GSuite, Salesforce, & more
- License management
- Measure and Analyze solution effectiveness
- Monthly executive reporting

CORE SOLUTION

IT Asset Management

Inventory and proactively manage your organization's digital assets, continuously.

If you don't know what assets you have, how can you protect them? But guess what most companies aren't doing? Taking inventory of the assets they have. Asset inventory is your first cybersecurity building block. Most companies lack a central repository that aggregates all assets for ease of reference.

WHAT'S AN ASSET EXACTLY?

An asset can be a multitude of things; it's more than just laptops. An application, a data source, a business unit, cloud instances, and operational infrastructure can all be classified as "assets."

As you can imagine, in a modern organization, assets add up quickly and easily become lost, forgotten, or displaced. Assets encompass far more than just your company computers - they include cloud, remote, and internal assets - and you need to take inventory of both applications and hardware.

IT assets change quickly in the digital age, and you need a cybersecurity partner who can change with them. With continuous cybersecurity asset management, we'll work with you to gain the insight to comprehensively identify and secure your digital assets.

CYVATAR'S CLOUD SAAS MANAGEMENT SOLUTION INCLUDES:

- Agentless, solution installation, configuration, assessment, and maintenance
- Comprehensive Asset Discovery and Inventory
- Identification of devices with missing or malfunctioning agent devices not being scanned for vulnerabilities, managed/unmanaged devices and rogue devices on privileged networks
- Identify endpoint security gaps
- Unify asset inventory and device classification reports
- Configuration Management Database ("CMDB") Reconciliation
- Remediation of any gaps and risks found
- Maintenance of the remediated status
- Monthly executive reporting

Security Awareness Training & Testing

Engaging security curriculum training courses for organizations to adopt and instill cybersecurity into their culture.

Compliance regulations require you to keep your team up to date with regular security awareness training and testing. But when you only offer annual training, what are your employees retaining?

One-time training — even completed annually — doesn't affect real cultural change for your organization's security efforts.

The solution to keeping cybersecurity top of mind for employees is embedding continuous and relevant training which influences sound decision making long term.

Using videos, emails, and posters is just a start. With Cyvatar's Security Awareness Training & Testing, users learn to increase both awareness and knowledge over time with real time training, actionable metrics based on training, and customized modules based on your company's unique culture. Additionally, security and awareness training is managed for you, so you won't need to worry about a thing.

CYVATAR'S SECURITY AWARENESS TRAINING & TESTING INCLUDES:

- Engaging, self-service video content
- Detailed reports to measure employee progress and compliance reports
- Gamified learning such as phishing simulations to create a real-life experience
- Simulated Phishing campaigns and custom content training
- Monthly executive reporting

Email Security Management

Preemptively protect your users against Phishing, Business Email Compromise (BEC), and Email supply chain attacks.

Phishing is one of the most frequent and expensive cyber threats that organizations face. You need a robust email security solution that identifies and blocks attacks before they hit user inboxes, enabling more effective protection against spear phishing, BEC, and other advanced threats that evade existing defenses.

Cyvatar's Email Security Management solution protects your organization from the most common targeted vulnerabilities:

- **Phishing**
  The Verizon 2021 DBIR cites phishing as the most common breach tactic. Through a combination of massive-scale web crawling, small pattern analytics and enhanced detections. Cyvatar's solution stops these attacks before they get into your network.
- **Email supply chain**
  Attackers compromise a vendor's email, observe mail patterns, and intercept existing threads to carry out invoice fraud. Cyvatar's solution analyzes mail threads, message sentiment, and social graphs to stop these sophisticated attacks.
- **BEC and socially engineered threats**
  In BEC, attackers impersonate or compromise trusted entities to steal money and data. Cyvatar's solution analyzes the content and context of email communications to stop these "needle in the haystack" threats.
- **Ransomware & Extortion Emails**
  Gartner estimates that 40% of ransomware attacks originate from email. Cyvatar helps proactively defend against ransomware emails before they reach end users and also removes malicious messages before they spread.

CYVATAR'S EMAIL SECURITY SOLUTION INCLUDES:

- Installation, configuration, assessment, remediation, and continued maintenance
- Enhanced native email security with deep integrations
- Monthly executive report

ADD ON SOLUTION

Incident Response Management Retainer

Every company needs the ability to act fast in the event of a cybersecurity-related emergency situation.

With the number of successful attacks increasing year over year, the world is not winning the war against cybercrime. Cyvatar's security solutions are designed with a preventative approach, but nothing is 100%. To add peace of mind, we offer a world class Incident Response (IR) team ready to respond 24/7.
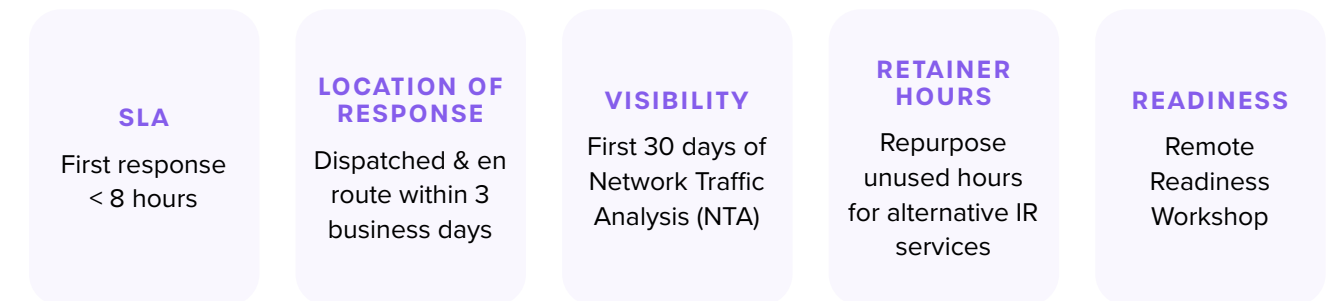
SMBs don't typically justify the cost to have an in-house IR team, or even cybersecurity expert on staff. It's vital for your business to have IR processes and personnel to be equipped with situational awareness beyond just the managed infrastructure of IT, OT, Cloud, and On Prem, otherwise the cost of a breach can be detrimental to a small business.

Cyvatar's Incident Response Retainer Management subscription arms SMBs with resilient and proactive solutions that align our security experts as an extension of your Security/IT team/MSP.

CYVATAR'S INCIDENT RESPONSE MANAGEMENT RETAINER INCLUDES:

- 24/7 emergency response via phone and email escalation paths
- Workshops to understand existing practices in place and improve the readiness state
- Pre-defined terms and agreements with onsite and remote response SLAs that help mitigate impact
- Flexible use of retainer hours to support the organization's needs
- Partner with experts that combine hands-on incident response skills, executive management experience and strategic business acumen

Retainer Offering

SLA	**LOCATION OF RESPONSE**	**VISIBILITY**	**RETAINER HOURS**	**READINESS**
First response < 8 hours	Dispatched & en route within 3 business days	First 30 days of Network Traffic Analysis (NTA)	Repurpose unused hours for alternative IR services	Remote Readiness Workshop

Repurposed Hours

Retainer hours may be repurposed towards any of the following services:

- ✔ Incident Response Maturity Assessment
- ✔ Incident Response Tabletop Exercise
- ✔ Incident Response Plan, Program or Policy Development
- ✔ Response Advisory Services
- ✔ Incident Response Playbook Development
- ✔ OSINT External Analysis

Managed Security Orchestration, Automation, and Response

Collect data inputs to streamline and automate security operations.

SOAR (security orchestration, automation, and response) refers to the collection of security software solutions that collects data from a variety of sources. Through the combination of machine learning, AI, and a human element, the data is analyzed to understand and prioritize security-related incident responses.

Alerts and noise create an overabundance of operational-based tasks that overwhelm security operation teams. This results in broken processes, wasted time, and human error. Critical alerts and vulnerabilities receive slow response time or potentially missed, increasing risk for possible cyberattack.

With a managed SOAR solution, your organization will stay ahead of incidents, receive automated proven processes and workflows, and have issues resolved in record time.

CYVATAR'S MANAGED SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE SOLUTION INCLUDES:

• Solution installation, configuration, assessment, and maintenance
• Logging and monitoring of infrastructure devices, security devices, server logs, web servers, and authentication servers
• Unify security tools and workflows
• Standard and custom playbook implementation
• Optimizes your utilization of resources and human intervention
• Automate manual/repeatable processes
• Remediation of any gaps and risks found
• Maintenance of the remediated status
• Monthly executive reporting

Managed Security Subscription Pricing

Our cybersecurity-as-a-service subscriptions encompass the necessary cyber talent, processes, and technologies into one incredible, all-inclusive monthly subscription.

The plans below are based on companies with 100 employees or less. Custom quotes are available for larger organizations by visiting **cyvatar.ai/contact-us**.

Build Your Own Subscription! Looking for a strategy and solutions that's custom to your business? You can piece together a custom Cyvatar subscription. Learn more on the next page.

CYBERSECURITY **Foundations**	CYBERSECURITY **Prevention**	CYBERSECURITY **Prevention & Cloud**
Implement foundational security, reduce risk, and get continuous remediation.	Automate your cyberattack prevention, reduce risk, get continuous remediation, and keep your business operational.	Prevent cyberattacks, get continuous remediation, lock down and secure cloud applications.
$30/EMPLOYEE /MONTH	**$55**/EMPLOYEE /MONTH	**$80**/EMPLOYEE /MONTH
✔ Threat & Vulnerability Management	✔ Threat & Vulnerability Management	✔ Threat & Vulnerability Management
✘ Secure Endpoint Management	✔ Secure Endpoint Management	✔ Secure Endpoint Management
✘ Cloud SaaS Management	✘ Cloud SaaS Management	✔ Cloud SaaS Management
✔ Cybersecurity Assessment	✔ Cybersecurity Assessment	✔ Cybersecurity Assessment
✔ Monthly External Vulnerability Scan	✔ Monthly External Vulnerability Scan	✔ Monthly External Vulnerability Scan
✔ Cybersecurity Policies	✔ Cybersecurity Policies	✔ Cybersecurity Policies
✔ Business Risk Tool	✔ Business Risk Tool	✔ Business Risk Tool
✔ Continuous Remediation	✔ Continuous Remediation	✔ Continuous Remediation
✘ Cybersecurity Service Guarantee with Cysurance	✔ Cybersecurity Service Guarantee with Cysurance	✔ Cybersecurity Service Guarantee with Cysurance

Build Your Own Security Subscription!

Looking for a strategy that's custom to your business needs?

Cyvatar delivers exceptional cybersecurity-as-a-service and can customize a solution subscription to meet your business needs.

Core solutions are $30 per employee, per month or $25 per employee per month annually.

Reach out to get started!

Contact us for ESM, IRR, and MSOAR pricing.

Core Solutions

- Secure Endpoint Management
- IT Asset Management
- Threat & Vulnerability Management
- Multi-Factor Authentication*
  * Minimum of 25 employees
- Cloud SaaS Management

$30 /EMPLOYEE PER MONTH

$25 /EMPLOYEE PER MONTH FOR ANNUAL SUBSCRIPTIONS

Add Ons

SECURITY AWARENESS TRAINING & TESTING

$5 /EMPLOYEE PER MONTH

CYVATAR.AI

Cyvatar is committed to effortless cybersecurity for everyone. As the industry's first subscription-based, cybersecurity-as-a-service (CSaaS) company, it's our mission to transform the way the security industry builds, sells, and supports cyber solutions. We empower our members to achieve successful outcomes by providing expert practitioners, market-leading technologies, and proven best practices to guarantee business results. Our approach is rooted in a proprietary ICARM (installation, configuration, assessment, remediation, maintenance) methodology that delivers measurable security solutions for superior compliance and cyber-attack prevention, all bundled into a fixed monthly subscription that members can cancel anytime. Cyvatar is headquartered in Irvine, California, with locations around the world. Begin your journey to security confidence at cyvatar.ai and follow us on social media.

FOR MORE INFORMATION ON CYVATAR, VISIT WWW.CYVATAR.AI

@CYVATAR.AI