ShieldForce Secure My Enterprise

For PC, Workstations, Mac, IOS, and Android

- License and secure all your endpoints with **Anti-ransomware protection** and benefit from **1TB of backup storage per device.**
- Get an in-depth **vulnerability assessment** on your endpoints using six (6) key criteria and a **cybersecurity fitness score** between 250 and 850.
- AV and **Anti-malware protection** for your endpoints.
- Eliminate financial/reputational loss due to data leakages by **applying the least privilege principle** for controlling sensitive business data flow.
- leverage your **1TB of backup storage** for file or folder backup.
- Access **unlimited storage** for your Microsoft 365 or Google Workspace backups.
- manage your devices with **device control** and group management of workload.
- Prevent data leakages with **data loss prevention** policies that analyzes and controls data flow across local and network channels.
- Take advantage of 52 weeks of continuous **cybersecurity awareness training** for all your licensed employees.
- Leverage a single, **advanced email security** solution for lightning-fast detection that easy to deploy and manage.
- access additional **1TB of storage for disaster recovery** operations per server or per virtual machine.
- dedicated **public IP address** for disaster recovery operations.

- Achieve **compliance with regulations** (HIPAA, GDPR, PCI-DSS, etc.)
- Get help with phone and web **support** from ShieldForce.

Compatible with Windows 11, Windows 10, Windows 8.1 and the two **most recent** versions of macOS.

Talk with a sales expert

To speak with a sales expert, call 1-307-529-0549. Avaliable Mon to Fri from 8:00AM to 5:00PM Eastern Time.

$400.00 user/month

Annual subscription-auto renews

BUY NOW

Disrupt your Industry while we compliment your cybersecurity strategy

As an Enterprise business, we understand some of your short-term and long-term goals. Delivering value to millions of your customers, unlocking values from your technology investments and generating returns for your shareholders, we also understand you are keen on compliance, regulation, and product innovation. ShieldForce Secure My Enterprise compliments your overall cybersecurity roadmap strategy by protecting your enterprise from financial losses and reputational damage while you keep up the momentum and disrupt your industry.

Cloud Services included

SHIELDFORCE ADVANCED EMAIL SECURITY

SHIELDFORCE ADVANCED MANAGEMENT

SHIELDFORCE ADVANCED SECURITY

SHIELDFORCE ADVANCED BACKUP

SHIELDFORCE ADVANCED DISASTER RECOVER

SHIELDFORCE ADVANCED DATA LOSS PREVENTION

ShieldForce

Features

Automated Patch Management

Keep all Windows and 300+ third party applications up to date. We support more applications than any other Cybersecurity provider in the industry.

APT and zero-day protection

Catch advanced threats that evade conventional defenses with a unique CPU-level technology that detects and blocks attacks at the exploit stage to release

Continuous Data Protection

Save your data between backups and have close to Zero recovery point objective.

Forensic backup

Preserve integrity of evidence collected to be used in legal cases. Capture original data in unaltered state.

Anti-phishing/Anti-spam protection

Minimize email risk for clients with powerful threat Intelligence, signature-based detection, URL reputation. is

URL Filtering

Fourty-four website categories defined, URL Filtering blocks traffic to website categories to which access

Prohibited.

Fail safe patching

Reduce the impact of failed patches on your productivity by automatically backing up workloads before patching them to ensure quick recovery in the case of issues.

Exploit prevention

Detect and prevent malicious processes from exploiting software vulnerabilities on a system.

ShieldForce

Impression (BEC) protection

Prevent payload-less attacks and impersonation attempts Through machine learning algorithms with IP reputation.

Threat Intelligence

Leverage powerful threat intelligence to stop potential or current attacks

Off-host data processing

Reduce CPU and RAM consumption on protected Server by offloading backup management operations to a server with a dedicated agent.

Hardware Inventory

Keep up-to-date information on hardware assets to properly plan replacement. Track changes in hardware assets and generate hardware inventory reports.

Advanced remote desktop and assistance

Seamless access and support for Windows, macOS And Linux workload, saving the time and cost of traveling for an on-site fix, using secure NEAR protocol (ports are not opened).

Cyber scripting: centralized automation

Automate your manual and mundane task with 40+ ready to use scripts that can be fine-tuned and customized.

Runbooks

Runbook lets you automate a failover of one of more Multiple servers, it automatically checks the failover result By pinging the server Ip address and checking the Connection to the port you specify.

IPsec Multisite VPN Support

Multiple sites hosting critical workloads and higher requirements for security, compliance, and bandwidth

ShieldForce

ML-based monitoring and smart alerting

Reduce unplanned downtime and data loss with predictive Monitoring and alerts for 24 metrics / parameters (Hardware, software, services, processes, critical events).

Centralized cyber protection with a single console

Control your TCO, reduce management overhead, and enable better margins with easier service tiering with one Solution that integrates backup, disaster recovery, Cybersecurity, patch management, workload management Management and automation via ML (Machine Learning) based monitoring.

Software Inventory

Discover all software asset on all registered machines, schedule automated scans or on-demand scanning track changes in software Inventory and generate software inventory reports.

Backup Scanning

Backup scanning scans backup stored in cloud storage for Malware. Volume must be with NTFS file system with GPT or MBR partitioning. Cloud backups placed in queue for Execution.

Safe Recovery

Allows you to prevent recurrence of infections by using the integrated antimalware scanning and malware deletion during the recovery process.

Remote wipe

Ability to set Windows 10/11 machine to factory defaults (lost/stolen machine).

Prioritization of incident

Focus on what matters and increase your responsiveness to attacks by leveraging automatic incident alerts that are prioritized based on criticality, so your team can focus on remediating instead of hunting.

Threat containment and quarantining

Remediate attacks by stopping malicious processes and quarantining analyzed threats — blocking them from execution as part of unified, single-click response capabilities.

Endpoint isolation

Stop attacks from spreading and affecting more endpoints – you can isolate affected points from the network to prevent lateral movement.

Recovery, including full reimaging

Ensure clients' businesses always remains up and running and that they can quickly recover data and operability after attacks. With best-of-breed backup and recovery capabilities integrated in our single-click response, you can recover specific files or reimage the whole endpoint.

Disaster recovery failover

Ensure an unmatched level of business continuity with integrated disaster recovery. Automatically switch to a backup, off-site environment in case of attacks that disrupt customers' business continuity.

Remote endpoint connection
Investigate incidents further with a secure remote connection to affected endpoints for troubleshooting and additional analysis purposes.

Forensics backup
Collect evidence for further investigation, reporting, compliance, and legal purposes by gathering forensic information — like memory dumps and process information — and storing it in temper-protected backups.

Patch management

As part of the single-click response to attacks, you can close security gaps to prevent future incident reoccurrence with our integrated patch management for 300+ applications.

Event monitoring and automated correlations

The solution monitors events on an endpoint level and automatically correlates them in attack chain graphs per incident.

Intelligent search for IOCs with focus on emerging threats

Focus on what matters, like indicators-of-compromise (IoC)-related emerging threats from our real-time threat intelligence feeds and automatically search IOCs across all endpoints — instead of scanning hundreds of lines of logs.

Real-time threat intelligence feed

Cyber Protection Operation Centers (CPOC) continuously monitor the cybersecurity landscape and release alerts on potential threats of any kind. Receive real-time alerts on malware, vulnerabilities, natural disasters, and other global events that may affect data protection, so you can prevent them.

Exploit prevention

Prevent advanced attack techniques, including zero-day and fileless attacks, with behavior-based detection heuristics focused on vulnerability exploitation. Acronis' exploit prevention technology specifically detects attempts to take advantage of software vulnerabilities.

Anti-ransomware detection with automatic rollback

Detect and stop ransomware, including advanced sophisticated forms, and automatically roll back any changes caused by the threat or any data that was affected.

Behavior-based detection

Protect clients, their data, and operations against modern threats with award-winning protection to detect typical patterns of malicious behavior and prevent threats from executing.

Unprotected endpoint discovery

Ensure no gaps in your defenses by streamlining the discovery of unprotected endpoints and enabling remote agent installation and service provisioning.

Vulnerability assessments

Monitor endpoints for open vulnerabilities and provide a prioritized view based on vulnerability criticality — enabling you to streamline security configuration management on top of attack detection and response.

Cybersecurity Fitness Score to evaluate the security posture of endpoints

Quickly and easily assess the security posture of endpoints and leverage our guided recommendations to secure customer endpoints. Unlock a unified view of all endpoints along with their #CyberFit Score to streamline security configuration management.

Data classification

Increase your visibility over affected data when investigating attacks by classifying outgoing data from customer endpoints to detect sensitive data exfiltration and stop it with greater efficiency.

File- and system-level backup

Ensure not only endpoints are protected, but also the data residing on them. Leverage best-of-breed, pre-integrated backup capabilities, enabling an unmatched level of data protection and business continuity.

Device and port control

Strengthen data security and prevent leakage of sensitive information via locally connected devices and ports with controls over user access to such local channels, and data operations related to them — even for virtualized sessions.

Automated, tunable allowlisting based on profiling

You can enable monitoring and profiling of your applications to create an automatic allowlist of the most used applications, including custom apps, to save time and avoid resource-draining false positives. You can manually add or remove apps from the allowlist.

Frequently asked questions

We have specific requirements that we would love to discuss so we can take full advantage of ShieldForce and its capabilities.

ShieldForce helps organizations capture its business requirements so they can take full advantage of their subscription. Please fill in the ShieldForce Getting Started Questionnaire and a Customer Success Consultant will get back to you. Alternatively, if you have specific requirements, you can send an email to info@shieldforce.us and we would respond at the speed of an electron, lol.

How many users does ShieldForce My Enterprise support?

ShieldForce Secure My Enterprise supports unlimited users/devices. If you have servers that require high availability disaster recovery services, look at our ShieldForce Disaster Recovery Cloud.

I have already deployed an endpoint detection/prevention solution, why do I still need ShieldForce Secure My Enterprise?

ShieldForce Secure My Enterprise helps you achieve regulatory compliance. An endpoint detection/prevention solution is blind to data leakages, they are not enough to prevent data leaks that have bypassed such defenses. Secondly, most enterprise organizations need additional resources to create the necessary policies to prevent data leakages within the enterprise.

My organization already uses anti-malware/ firewall services. I thought I was protected, why do I need something on top?

Endpoint protection services (anti-malware, firewall) help to stop threats from reaching your network and data. However, they cannot protect you against attempts to exfiltrate your sensitive data – either by threats that have passed your defenses or by malicious or negligent insiders. Only DLP technology can protect against data leaks.

We're utilizing backup and recovery technology in our service stack to protect against data loss. Why do I need to consider DLP technology?

Backup services guarantee your data is stored and recoverable, however, they do not protect sensitive data from being transferred to unauthorized recipients outside or inside the organization. Only DLP technologies like ShieldForce Secure My Enterprise can protect against data leaks.

How does ShieldForce Secure My Enterprise DLP capabilities differ from other providers in the market

ShieldForce Secure My Enterprise automates DLP policy generation, service provisioning and policy configuration. ShieldForce Secure My Enterprise also simplifies complexity to reduce hiring needs. ShieldForce Secure My Enterprise also automatically maps your business processes to DLP policies.

Educate me on the data loss prevention capabilities of ShieldForce

ShieldForce prevents data leaks across local and network channels. ShieldForce blocks risky data flows across local channels like removable storage, printers, redirected mapped drives and redirected clipboards. ShieldForce also blocks risky data flows across network communications like Emails (SMTP, Microsoft outlook (MAPI), IBM Notes), seven instant messengers, sixteen webmail services, twenty-eight file sharing services and twelve social networks.

How can I validate the DLP policy with my IT team or MSP when I do not have technical know-how?

The initial automatically created baseline DLP policy will be presented in any easy-to-understand graphical form. You can easily review and approve or choose to prohibit each sensitive data flow in the initial DLP policy. You don't need security know-how to validate whether a data flow is necessary for your enterprise, you only need to know your business specifics.

Can the implementation of ShieldForce Secure My Enterprise help us meet regulatory requirements?

Yes, ShieldForce Secure my Enterprise data loss prevention capabilities help reduce your cyber insurance premium. It also helps reduce the risk of sensitive data being leaked. Examples of data includes personal identifiable Information (PII), patient health information (PHI), Intellectual Property, Confidential Information, trade secrets and state classified data

What happens when I exceed the 1TB storage allocated per device for my backups?

ShieldForce will automatically allocate the cloud storage you require at a subsidized cost of $0.25/GB/month billed to your credit card on file.

What happens when I exceed the 1TB storage allocated per server/virtual machine for my disaster recovery operations?

ShieldForce Disaster recovery Cloud is different from file/folder backup for workstations, this service is dedicated to servers and virtual machines recovery operations. We will need to understand your enterprise requirements before we provide this service. The following would be required for a successful disaster recovery operation, protected device (your server), backup storage, disaster recovery storage, compute resource and a dedicated IP Address. Additional storage cost is $0.25/GB/month.

What forms of payment can I use?

Enterprise customers have the flexibility to use any form of payment, ShieldForce accepts all forms of Wire transfer, ACH, Fedwire, direct debit, etc.

Pay with all major credit cards, and your subscription amount will appear on your credit card statements. For ShieldForce Secure business plans, you have the option to receive an invoice and, depending on your choice of services, you'll be billed monthly or annually. Receive an email message when your invoice is ready to be viewed and, if a purchase order number is entered when you buy your subscription, that number is included in your invoice.

Where can I view my payments and detailed of my subscription

ShieldForce Customer Center gives you access to your tenant and to manage your subscription.

What payment options are available? Can I pay monthly or annually?

Annual Subscription payments are accepted for Enterprise customers. Enterprise customers are also eligible to receive additional discounts when they subscribe for our 24-month plan and 36-month plan.

Can I cancel my subscription at any time?

You can cancel your subscription at any time, you may be entitled to a partial refund. Please cancelling your subscription leave your enterprise open to various forms of cyber-attacks and data leakages. ShieldForce will not be

held liable for such negligence or human related errors or mistakes as stipulated in the terms and conditions of use document.

What happens to my data if I cancel my subscription?

Your data is yours. If you decide to cancel your ShieldForce Secure subscription, you can download your data – for example, your files, folders on cloud storage -and save it to another device/location. You should save your date before you cancel. After you cancel your subscription, data associated with your ShieldForce Secure account will be avaliable to your tenant administrators (s) in a limited function account for 30 days. After 30 days all associated data will be deleted.

What happens when my subscription expires?

ShieldForce is committed to protecting its customers from financial losses and reputational damage. Your subscription automatically renews upon expiration. All customers are notified via email 30 days, 14 days, and 7 days before expiration.

Where can I find more information about the value, I'm getting with ShieldForce Secure My Enterprise?

Please look at our pricing page here, ShieldForce pricing page and see the loads of great solutions that make ShieldForce awesome. Please feel free to schedule a discovery call here, ShieldForce demo session and one of our super excited Customer Success Consultants will show you the tremendous value your enterprise will get by using ShieldForce Secure My Enterprise.

I represent a government organization in need of data loss prevention services, how can ShieldForce Secure My Enterprise help my agency.

ShieldForce Secure My Enterprise will help prevent your government agency from financial losses and reputational damage. ShieldForce Secure My Enterprise will protect your sensitive data in use in peripheral devices or transferred via network communications. ShieldForce Secure My Enterprise will automatically classify data subject to common regulations. ShieldForce Secure My Enterprise will also automatically create specific DLP policies specific to your organization.

Six (6) types of organizations have been identified that will realize maximum value from ShieldForce Secure My Enterprise.

a) Companies that create, store or work on their workloads with sensitive data are subject to regulations.
b) Companies operating in highly regulated industries.
c) Companies that have suffered a data breach and want to secure their environment and reduce risk.
d) Companies that have/need compliance certifications
e) Companies that are paying/considering a cyber insurance to reduce their liabilities
f) Companies that lack dedicated security staff and expertise.

Can you identify key industries that need ShieldForce Secure My Enterprise and its Robust Data Loss Prevention Capabilities?

The following industries are in urgent need of ShieldForce Secure My Enterprise: financial services, healthcare, legal, IT & Telecommunication, Government, Manufacturing, Education, Retail, Logistics and Wholesale, Energy Utilities.

What is ShieldForce Disaster Recovery Cloud?

This is our Disaster recovery as a service offering specifically designed for all business sizes. We backup your critical servers and virtual machines to the cloud, once we configure your environment, specify the protected device, allocate storage for your backup, allocate additional storage for disaster, allocate compute resources, and specify a dedicated IP address for your server, you are all set.