



Deep Security

SECURITY TODAY

CYBERSECURITY • DEVELOPMENT • HOSTING

Security and technology services built around your business

- **Managed Cybersecurity & Vulnerability Management**
- **Custom Website Design & Development**
- **Internal Business Applications & Portals**
- **Managed Web Hosting, Monitoring & Maintenance**
- **Secure Deployment, Backups & Ongoing Support**

[**SEE CUSTOM DEVELOPMENT & SECURE HOSTING ON PAGE 10**](#)

OUR VISION

Deep Security was founded to meet the needs of **rapidly growing demands** of information security within many industries, primarily driven by recent information security breaches, federal regulations and complex cyber attacks.

OUR GOAL

Ensure organizations **Defense in Depth** is adequately and properly configured in a secure manner. We promote high quality IT hygienic procedures that adhere to HIPAA, ISO 27001 IT Governance and other industry best practice security standards.

WE PROVIDE

Customized security services, solutions to identify and remediate any security issues within your IT infrastructure. We take pride in our recommendations, identifying and addressing gaps in the security stack.

MORE THAN A SERVICE

We provide more than just a **service**, tailored to each client with deep technical knowledge to each environment that we assess.

Deep Security has an in-depth focus and 75+ years of experience within the healthcare vertical as well as several other industries.

MANAGED SECURITY SERVICES

Deep Security's staff of subject matter experts (SME) will execute the most secure methods of remediations and on-going management lifecycle.



Weekly Vulnerability Scanning Internal and External targets



Bi-weekly meetings to review progress on remediation



High Level Security oversight covering several key areas



Weekly Active Directory reviews of Privileged Groups and Policies



SIEM and Daily Incident, Detection and Response services along with Log Correlation



Access review of rights against CISO, CEO, CFO, CTO Level AD users permissions



5 Reasons to use an MSSP

- 01** Using it as an Operational Expense (**Op Ex**) versus a Capital Expense (**Cap Ex**).
- 02** Guaranteed Services **versus** having security staff resign.
- 03** A fraction of the cost ratio instead of hiring 2 mid level security engineers. Ranging from 120-140k per employee with 30k in benefits and training estimated at 300-340k annually.
- 04** Delegating Cybersecurity to an MSSP to Focus on Business.
- 05** Benefiting from Security Experts with a vast number of different environments and infrastructures.

COST CALCULATOR



2 Mid-Level IT
Security Engineers

VS.



Deep
Security

1 year	\$300k - 340k	\$120k with Managed Services
3 years	\$900k - 1.02M	\$360k with Managed Services

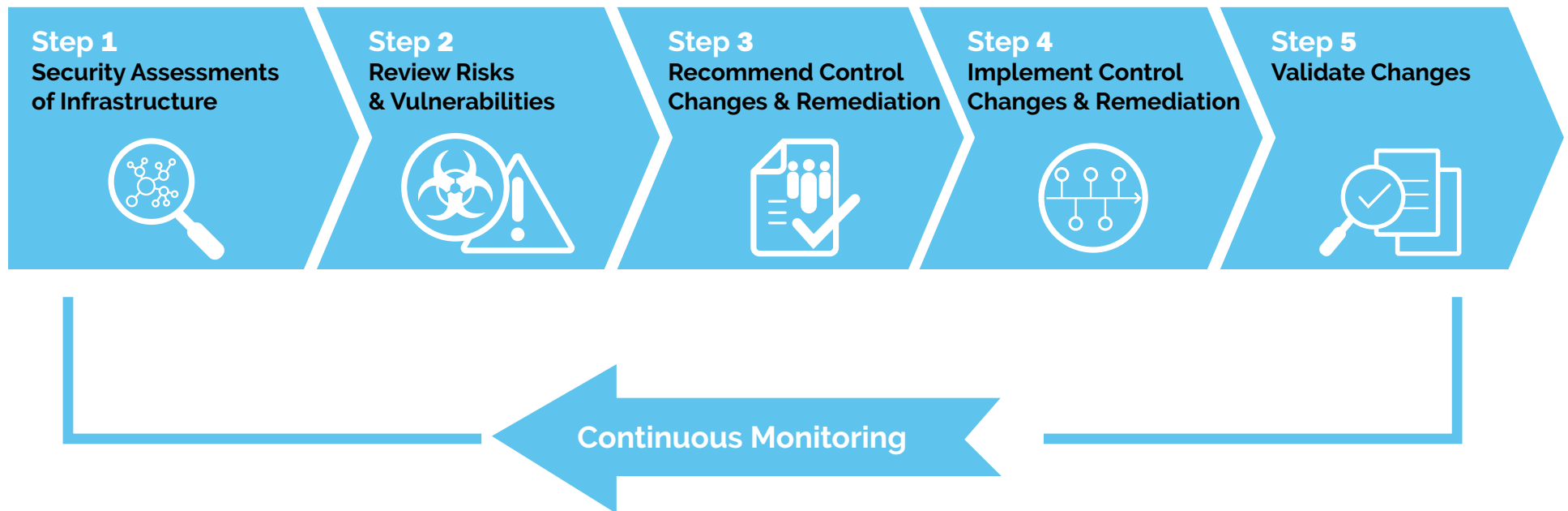
3rd of the costs
(66% savings)

- Active Directory Assessments
- Cloud Security Assessments
- Vulnerability Assessments
- GAP Assessments
- Firewall Security Assessments
- Firewall/IDS/IPS Troubleshooting
- Penetration/Web App Testing
- Physical Penetration Testing
- Phishing Campaigns
- 3rd Party Risk Assessments
- Internal Auditing Review
- Password Cracking Services

ADDITIONAL SERVICES



RISK METHODOLOGY



BUILT TO SCALE

Practical cybersecurity services aligned to your size, risk profile, regulatory obligations and business priorities.

SMALL BUSINESS

Essential Protection

Gain experienced security support without the cost of building a full internal security team.

- External vulnerability scanning and prioritized remediation
- Microsoft 365, identity and privileged-access reviews
- Phishing readiness and security awareness support
- Incident response planning and executive reporting
- Flexible advisory hours as your needs grow

MIDSIZE BUSINESS

Managed Defense

Extend your IT team with repeatable controls, continuous oversight and security expertise.

- Internal and external vulnerability management
- SIEM monitoring, alert triage and incident coordination
- Cloud, firewall and Active Directory assessments
- Third-party risk and compliance gap assessments
- Security roadmap, metrics and leadership reviews

LARGE ENTERPRISE

Enterprise Assurance

Add specialized capacity, independent validation and governance across complex environments.

- Enterprise attack-surface and risk-based testing
- Penetration testing and web application assessments
- Control validation across business units and cloud estates
- Executive and board-level risk reporting
- Co-managed programs supporting internal security teams

Start where the risk is highest. Expand coverage as your environment, workforce and compliance needs evolve.

PROTECTING CRITICAL BUSINESS

Every engagement is tailored to the information, systems and operational realities that matter most to your organization.

LAW FIRMS & LEGAL SERVICES

Protect confidential client communications, matter data and privileged information while strengthening third-party, remote-access and incident-response practices.

- Client confidentiality and data protection
- Email, identity and document-management security
- Vendor and e-discovery risk
- Cyber insurance and client security questionnaires

CORPORATE ENVIRONMENTS

Build consistent security across offices, remote teams, cloud platforms, subsidiaries and critical business applications.

- Enterprise identity and access governance
- Cloud and network security validation
- Security program maturity and control testing
- Executive metrics and remediation accountability

HEALTHCARE & REGULATED ORGANIZATIONS

Apply deep healthcare experience and risk-based guidance to environments subject to HIPAA and other contractual or regulatory expectations.

- HIPAA security risk assessments
- Technical safeguard validation
- Risk register and remediation planning
- Audit-ready evidence and leadership reporting

SMALL OFFICES & STARTUPS

Deep Security helps small teams build a reliable, secure technology foundation - without requiring a full-time internal security staff.

WE SUPPORT THE WAY SMALL BUSINESSES WORK

Whether you operate a printing company, medical office, dental practice, professional office or new startup, we work with you to make sure essential systems are configured correctly, protected and ready to support daily operations.

SECURE EMAIL & COMMUNICATION

Email is a primary source of communication for customers, patients, vendors and employees - and one of the most common paths for cyberattacks.

- Microsoft 365 and Google Workspace security
- Multi-factor authentication and account protection
- Anti-phishing, spam and impersonation controls
- Secure email configuration, including SPF, DKIM and DMARC
- Mailbox access, forwarding and administrator reviews
- Backup, retention and recovery guidance

A STRONG FOUNDATION FROM DAY ONE

We help organize and secure the technology your business depends on, then provide practical support as your team and customer base grow.

- Device, user and administrator account setup
- Secure Wi-Fi, firewall and remote-access configuration
- Endpoint protection, patching and vulnerability reviews
- File sharing, cloud storage and access permissions
- Data backup and business continuity planning
- Security policies, employee guidance and vendor coordination

RIGHT-SIZED SUPPORT. CLEAR PRIORITIES. ROOM TO GROW.

Start with a setup review, a focused email security assessment or ongoing managed support. We explain risks in plain language, help correct issues and provide a practical plan that fits your business and budget.

REQUEST A SMALL BUSINESS CONSULTATION

FROM ASSESSMENT TO ONGOING DEFENSE

Choose a focused project, ongoing managed coverage or a co-managed model that strengthens your existing team.

01

ASSESS

Establish a clear view of risk through vulnerability, cloud, identity, firewall, application and compliance assessments.

02

PRIORITIZE

Translate findings into a practical remediation roadmap based on business impact, exploitability and available resources.

03

IMPROVE

Support control changes, hardening, troubleshooting, testing and documentation with experienced security professionals.

04

MONITOR

Maintain visibility with recurring scanning, SIEM oversight, access reviews, reporting and regular progress meetings.

A SECURITY PROGRAM DESIGNED AROUND YOUR BUSINESS

Request a consultation to define the right starting point, scope and service

[DEEPSECURITY.IO](https://deepsecurity.io)



REQUEST AN ASSESSMENT

www.DeepSecurity.io

CONTACT US DIRECTLY

For any consulting engagements
or questions about services

EMAIL

Info@DeepSecurity.io

CUSTOM DEVELOPMENT / SECURE HOSTING

CUSTOM WEBSITES & INTERNAL APPLICATIONS

We design, build, secure, host, and maintain digital services made for your business.

01

CUSTOM WEBSITE DEVELOPMENT

Professional public websites, service portals, landing pages, integrations, and responsive user experiences.

02

INTERNAL BUSINESS APPLICATIONS

Custom dashboards, workflow tools, reporting, access controls, automation, and operational portals.

03

HOSTING & LIFECYCLE SUPPORT

Domains, production deployment, monitoring, updates, performance, backups, security, and ongoing support.

DEFINE → BUILD → SECURE → HOST → SUPPORT

Schedule a consultation with Deep Security.

deepsecurity.io

Info@DeepSecurity.io

CONTINUOUS EXPOSURE REDUCTION

MANAGED VULNERABILITY MANAGEMENT

Turn recurring discovery into prioritized remediation, measurable progress, and executive visibility.

01

DISCOVER & VALIDATE

Continuously identify vulnerabilities across endpoints, servers, networks, cloud workloads, and applications.

02

PRIORITIZE & REMEDIATE

Rank findings by exploitability and business impact, assign owners, validate fixes, and manage exceptions.

03

LEADING SECURITY PLATFORMS

Support for Tenable, Qualys, Rapid7, Microsoft Defender Vulnerability Management, CrowdStrike Spotlight, and Greenbone.

DISCOVER → PRIORITIZE → REMEDIATE → VERIFY

Schedule a consultation with Deep Security.

deepsecurity.io

Info@DeepSecurity.io