

Sidechain Services Overview

IT management, cybersecurity, and physical security.

Sidechain brings together the services you need to operate, secure, and improve your technology environment and workplace. We manage IT infrastructure, protect employee devices and email, provide 24/7 security monitoring, install security cameras, and help secure your offices and sensitive data. Sidechain is a trusted security partner to Fortune 1000 companies, and we have provided IT and cybersecurity services for Zoom, Molina Healthcare, AT&T, Walmart, IBM, Google, and more.



IT operations

INFRASTRUCTURE &
ENDPOINTS



24/7 monitoring

NIGHTS, WEEKENDS,
HOLIDAYS



Office security

CAMERAS & PREMISES



Data protection

ENCRYPTION & RECOVERY

SUPPORTING ORGANIZATIONS IN

BANKING

HEALTHCARE

RETAIL

MORTGAGE & LENDING

OTHER REGULATED INDUSTRIES

“

Sidechain's team are great communicators, they know their products, and they're knowledgeable. They're also just nice people, the kind of people you want to work with.

CHRIS K. · CIO

“

Sidechain brought expertise and innovation to bear in a niche area for sensitive data encryption. Their work is of exceptionally high quality, and I recommend Sidechain without hesitation.

JAMES V. · EXECUTIVE SOFTWARE ARCHITECT

— ONE COORDINATED RELATIONSHIP

Operations and security, managed together.

For mid-market organizations, these responsibilities are closely connected. We bring the disciplines together so your team can address operational needs and security requirements within one service relationship. Our background in enterprise encryption, key management, and secure infrastructure adds specialist depth to everyday technology operations.

**Reliability**

Depends on well-managed, well-maintained infrastructure.

**Security**

Depends on protected devices, trustworthy email, secure offices, and 24/7 monitoring.

**Recovery**

Depends on protected backups and a tested restore process.

SERVICE COVERAGE AT A GLANCE

SERVICE AREA	WHAT WE HELP YOU ACCOMPLISH	PG
IT management & infrastructure	Keep systems maintained, monitored, and ready to support the business.	03
Office security & cameras	Improve visibility across your premises and secure workplace technology.	04
24/7 security monitoring	Investigate threats around the clock and coordinate response.	05
Endpoint & email protection	Protect employee devices and inboxes from common attacks.	06
Microsoft 365 & identity	Strengthen access, email, collaboration, and business information.	07
Backup & recovery	Protect critical information and establish a practical path to recovery.	07
Encryption & key management	Protect sensitive data across applications, infrastructure, and cloud.	08
Private cloud & secure hosting	Run business and security workloads in managed infrastructure.	08
Assessments & compliance	Understand risk, prioritize improvements, and document your posture.	09
Penetration testing	Test how weaknesses could be exploited, with clear remediation guidance.	10
Professional services & DevOps	Deliver migrations, upgrades, integrations, and dependable releases.	10

IT MANAGEMENT & INFRASTRUCTURE OPERATIONS

The systems your business relies on, well maintained.

We manage the systems your business depends on, combining ongoing maintenance with the engineering needed to resolve problems and support change. Your internal team keeps strategic ownership while we take responsibility for everything else.



Servers and Cloud Services

Administration, configuration, maintenance, and troubleshooting for servers, virtual machines, and cloud services, including compute, storage, and network resources.



Employee devices

Monitoring and management for workstations, laptops, and servers, including device health, security-agent deployment, and routine maintenance.



Office networks & firewalls

Network configuration and hardening, firewall management, and secure remote access, with business systems, guest Wi-Fi, and security equipment kept separate.



Patching & remediation

Operating system and application updates, with vulnerability fixes prioritized by risk and business impact.



Monitoring & planning

Infrastructure monitoring, alert investigation, and issue resolution, plus resource planning so capacity keeps pace with the business.



Documentation & coordination

Technical documentation and coordination of infrastructure changes with your application teams and technology vendors.

BUSINESS VALUE

A maintained technology environment, clearer responsibility for operational issues, and access to engineering expertise as your needs change.

— OFFICE SECURITY, CAMERAS & PHYSICAL SECURITY

Protect the places where your people work.

Office security combines practical physical safeguards with secure networks and well-configured camera systems. You get better visibility into your premises and a clearer way to review events, with cameras managed as part of your broader IT environment.



Site planning

Security planning around entrances, shared areas, equipment locations, and the spaces you need to protect.



Camera installation

Camera selection, placement planning, onsite installation, and configuration for the agreed site coverage.



Recording & retention

Video recording, authorized viewing access, and footage retention set around your operational requirements.



Secure remote viewing

Secure remote access to camera systems for authorized personnel.



Network separation

Cameras and other connected security equipment kept on restricted, separate networks.



Physical access review

Review of access practices for offices, network closets, and server areas, with recommendations to close gaps.



Ongoing support

Camera system troubleshooting, configuration changes, and maintenance under the agreed service scope.



Facilities coordination

Physical security requirements coordinated with your IT environment and the people responsible for facilities.

BUSINESS VALUE

Better visibility into office activity and security events, with camera systems and workplace technology managed as part of one environment.

AROUND-THE-CLOCK SECURITY MONITORING

Security oversight that continues when the office closes.

Our 24/7 monitoring keeps attention on covered security events beyond the working day. We bring together endpoint alerts and relevant system, identity, email, and network activity to find what needs investigation, then connect detection to escalation and action.

● OVERNIGHT

● WEEKENDS

● HOLIDAYS

HOW AN EVENT IS HANDLED

- | | | |
|----|--------------------------------|---|
| 01 | Collect | Security logs from covered systems and tools are gathered in one place, with detections tuned to improve visibility and reduce noise. |
| 02 | Detect | Continuous monitoring for threats across the systems and security tools included in your service. |
| 03 | Investigate | Alerts are reviewed and prioritized based on the affected assets and potential business impact. |
| 04 | Escalate | Your agreed contacts are reached through established response procedures, including after hours. |
| 05 | Contain & remediate | Containment and cleanup are coordinated within the permissions and responsibilities set for your environment. |
| 06 | Report & improve | Security summaries, incident findings, and improvement priorities for your technical team and leadership. |



Prepared before an incident. We maintain escalation paths and incident response plans, connected to your backup and recovery preparations. Covered systems, escalation contacts, and response responsibilities are defined for each engagement.

BUSINESS VALUE

Security oversight that continues when the office closes, with a defined connection between detection, investigation, escalation, and action.

— ENDPOINT PROTECTION & EMAIL SECURITY

Protect the devices and inboxes your employees use every day.

Laptops and inboxes are common ways into a business. We combine preventive controls with people who investigate and act on what the tools detect, so a single compromised device or account doesn't become a wider incident.



Endpoint protection

Protection for employee laptops, workstations, and servers, in the office or working remotely.

- ✓ Deploy and manage endpoint detection and response (EDR) tools across covered devices.
- ✓ Monitor for malware, ransomware, suspicious processes, and unauthorized activity.
- ✓ Investigate alerts and isolate affected devices when warranted and authorized.
- ✓ Track agent health and coverage gaps so unprotected devices get addressed.
- ✓ Apply patches and prioritize vulnerabilities that increase exposure.
- ✓ Coordinate cleanup and return to normal operation with your IT team.



Email & phishing protection

Technical controls and employee awareness working together against credential theft, impersonation, and payment fraud.

- ✓ Configure and manage email filtering and anti-phishing protections.
- ✓ Reduce spoofing of your domain with SPF, DKIM, and DMARC authentication.
- ✓ Block malicious links and attachments using your email platform's capabilities.
- ✓ Address business email compromise: impersonation, suspicious forwarding, and unauthorized mailbox access.
- ✓ Security awareness training so employees recognize and report suspicious messages.
- ✓ Investigate reported phishing and remediate affected accounts or devices.

★ Endpoint and email alerts feed directly into 24/7 security monitoring (page 05).

BUSINESS VALUE

Protection that follows covered devices and layers of defense for a common entry point, supported by people who investigate what the tools detect and a clear path for employees to raise concerns.

MICROSOFT 365 & IDENTITY SECURITY

Use the security you already pay for, and close the gaps that matter.

We review how Microsoft 365 is configured and help you address the access, email, and data-sharing risks that affect everyday work. Assessment and implementation can be scoped as separate engagements.

- ✓ **Security audits** covering identity, email and collaboration, threat protection, data protection, governance, and licensing.
- ✓ **Access controls** including multifactor authentication, Conditional Access, privileged roles, and guest access.
- ✓ **Sharing and data protection** across Teams, SharePoint, and OneDrive, including labels and retention.
- ✓ **Oversight** of security alerts, audit logging, app permissions, and administrative practices.
- ✓ **Prioritized recommendations** based on Microsoft Secure Score and your available licensing.
- ✓ **Remediation** of agreed findings and configuration improvements, scoped separately.

BUSINESS VALUE

Better visibility into how your collaboration environment is protected, with a practical plan to address important gaps.

BACKUP, RECOVERY & CONTINUITY READINESS

A tested path back when something goes wrong.

We help you protect important information and prepare to restore it after accidental deletion, equipment failure, or a security incident. Scope, retention, recovery priorities, and testing are defined around the systems your business depends on.

- ✓ Managed backup for agreed server, virtual machine, and data workloads.
- ✓ Backup job monitoring, failure investigation, and remediation.
- ✓ Off-site backup and replication designed around each workload.
- ✓ Scheduled restore testing and documented recovery procedures.
- ✓ Retention planning, access controls, and encryption for backup data.



Sidechain Data Vault for M365

Backup and recovery for Exchange, SharePoint, OneDrive, and Teams: automated backups, granular recovery, health reporting, and storage on private infrastructure. Geo-redundant options are available where the service design requires them.

BUSINESS VALUE

A defined recovery approach supported by protected copies, operational oversight, and validation that data can be restored.

ENCRIPTION, KEY MANAGEMENT & TOKENIZATION

Data security is a core Sidechain differentiator.

We design, deploy, and operate the controls that protect sensitive information such as customer, patient, and payment data, and the encryption keys that protection depends on.



Encryption

Protection for data at rest and in transit across on-premises, cloud, and hybrid environments.



Key management

Enterprise and cloud key management, hardware security modules, and Bring or Hold Your Own Key designs where the platform supports them.



Tokenization

Implementation and integration, including batch transformation and validation of tokenization and detokenization workflows.

THALES CIPHERTRUST

THALES LUNA

ENTRUST

UTIMACO

FORTANIX

AWS KMS

AZURE KEY VAULT

GOOGLE CLOUD KMS

BUSINESS VALUE

Specialist protection for sensitive data and the encryption infrastructure behind it.

PRIVATE CLOUD & SECURE HOSTING

Managed infrastructure, on your terms.

For organizations that need control over their hosting environment, we provide and manage private cloud infrastructure from the hardware layer through day-to-day operations.

- ✓ Private cloud design, deployment, and management.
- ✓ Compute, virtualization, storage, and network capacity planning.
- ✓ Hardware security module hosting and colocation.
- ✓ Hosting and administration of business application infrastructure.
- ✓ Secure hosting for key managers, PKI, privileged access, and logging systems.
- ✓ Data center design, migrations, implementation, and monitoring.

BUSINESS VALUE

Experienced operators and managed infrastructure, with the deployment model aligned to your operational, security, and data-location requirements.

SECURITY ASSESSMENTS & COMPLIANCE SUPPORT

A clear view of risk, and what to fix first.

We help leadership understand current exposure and give technical teams a prioritized improvement plan. Assessments can focus on one platform, a set of controls, or the broader security program, with follow-on remediation available.

**Cyber Security Health Check**

A review across common areas of exposure. A practical starting point.

**Vulnerability assessment**

Risk-prioritized findings and a remediation roadmap.

**Cyber risk evaluation**

People, process, and technology reviewed together.

**HIPAA security risk assessment**

For healthcare organizations and their business associates.

**Microsoft 365 Security Audit**

Executive summary, technical findings, and a debrief with your team.

FRAMEWORKS WE SUPPORT

FRAMEWORK	COMMONLY RELEVANT TO
HIPAA	Healthcare organizations and business associates handling patient information
PCI DSS	Retailers and any organization that stores, processes, or transmits payment card data
Financial-sector requirements	Banks, mortgage companies, and wealth management firms under state and federal security rules
SOC 2	Organizations responding to customer due diligence on how they protect data
NIST CSF	Any organization that wants a structured way to measure and improve its program

Deliverables include risk registers, findings reports, and recommendations for leadership discussions, customer due diligence, and audit preparation.

BUSINESS VALUE

An actionable sequence of improvements, supported by documentation your stakeholders can review. Our work supports your compliance program; certification and audit opinions remain with the appropriate independent parties.

PENETRATION TESTING & APPLICATION SECURITY

Find exploitable weaknesses before an adversary does.

We test agreed systems and applications the way an attacker would, combining manual investigation with automated tools. Every finding explains the exposure and how to address it.

**External network testing**

Internet-facing infrastructure, as an outside attacker sees it.

**Internal network testing**

What an attacker could reach from inside, within an agreed scope.

**Web application testing**

Authentication, authorization, injection, and business logic weaknesses.

**AI agent & copilot assessments**

Prompt injection, data exposure, excessive permissions, and the actions an agent can take.

DELIVERABLES

Severity-rated findings, supporting evidence, and prioritized remediation guidance your teams can act on.

PROFESSIONAL SERVICES & DEVOPS

Engineering capacity for the projects that matter.

We deliver the engineering projects that improve how technology is deployed and operated, from a specific technical problem to a system taken from design through implementation and ongoing management.

- ✓ Infrastructure and security architecture, implementation, and integration.
- ✓ Data center design and build, including equipment planning and deployment.
- ✓ Release automation, environment separation, and secrets management.
- ✓ Platform upgrades, migrations, configuration changes, and remediation projects.
- ✓ DevOps process design and delivery pipelines, including Azure DevOps.
- ✓ Runbooks, documentation, and operational handoff, or ongoing management.

BUSINESS VALUE

Additional delivery capacity for important projects, with attention to how the resulting systems will be maintained after launch.

— HOW WE WORK WITH YOUR ORGANIZATION

Start with one service area. Expand as your needs change.

You can engage us for ongoing management, extend your internal team's capabilities, or bring us in for a defined project. The service mix is defined around your environment, your existing team, and your business priorities.

ONGOING**Managed services**

Assign defined operational and security responsibilities to Sidechain, with scope, reporting, escalation, and service expectations set for your environment.

BEST FOR Organizations that want day-to-day IT and security handled by a dedicated team.

CO-MANAGED**Support for your internal team**

Add infrastructure engineering, security operations, data protection, or specialist encryption expertise where you need more capacity or depth.

BEST FOR IT teams that want backup, after-hours coverage, or specialist skills.

PROJECT**Focused projects & assessments**

Start with a specific objective: evaluate risk, test an application, improve Microsoft 365 security, migrate infrastructure, deploy encryption, or build a release pipeline.

BEST FOR A defined need, a deadline, or an audit or due-diligence request.

CONNECTED**From findings to implementation**

Connect assessment results to separately scoped remediation and ongoing management, keeping the work tied to the risks that prompted it.

BEST FOR Turning an assessment into measurable, managed improvement.

Discuss your requirements.

Tell us what you operate today, where your team needs support, and what you need to improve. We'll help define the combination of managed services and project work that fits your organization.

✉ info@sidechainsecurity.com

☎ +1 (503) 389-3174

🌐 sidechainsecurity.com

[START A CONVERSATION](#)