CYBERSECURITY SOLUTIONS & SERVICES

68% OF BUSINESS LEADERS FEEL THEIR CYBERSECURITY RISKS ARE INCREASING[1]

30% OF DATA BREACHES INVOLVE INTERNAL ACTORS[2]

207 DAYS THE AVERAGE TIME TO IDENTIFY A BREACH IN 2020[3]

The cybersecurity landscape is increasing in complexity every year. With thousands of security controls available to purchase, how do you determine which tools are best for your organization? We believe that effective security starts with understanding the risk landscape of your business. Our customer-focused consultative approach enables us to take the time to understand your environment and business needs and work cooperatively to develop a roadmap that moves the needle on reducing risk for your organization.

With the average cost of a data breach skyrocketing in 2020 to $3.86 million for SMBs[4] and a whopping $116 million per breach for publicly traded companies[5] the need for an effective security program and improved risk posture is a business necessity now more than ever.

Our team of cybersecurity industry veterans have assisted thousands of companies across all industry verticals develop security programs and security controls that are tailormade to the organization's business needs.

GDT's 3 Ds of Cybersecurity

DEFINE
DESIGN
DELIVER

We've developed an approach that assists our customers with their Cybersecurity needs from concept to production

[1] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
[2] https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
[3] https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
[4] https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
[5] https://www.complianceweek.com/cyber-security/report-average-data-breach-costs-public-companies-116m/29037.article

CYBERSECURITY
SOLUTIONS
& SERVICES

DEFINE

A sure way to miss your target is to fail to define your destination. In cybersecurity, that could mean spending too much on what might be perceived to be the "squeaky wheel" but end up failing to solve for your ultimate objective.

vCISO

Don't have a CISO or your cybersecurity executive is overwhelmed? Our cybersecurity executive consultants help your organization meet its strategic objectives with a flexible engagement model.

Security Tools Rationalization

We assist in assessing and solidifying your standard technology stack, identify overlaps, and look for ways to consolidate and optimize spend.

Third-Party Services and Access

Third party software and access present real risk to organizations and recent breaches are evidence of this. We lead our clients in implementing a program to control, monitor, and assess their Third-Party Service Providers.

OUR SERVICES

Executive Consulting
- Virtual CISO (vCISO)
- Decision Support Matrix/Planning

Cyber Risk Management
- GRC as a Service
- GRC Programs & Platforms
- Third Party Risk Management

Security Best Practices
- Security Playbooks, Governance Planning & Documentation
- Policy / Procedure Planning & Documentation

Architecture
- Secure Cloud Architecture
- Cybersecurity Infrastructure
- NGFW Assessments/Best Practice Review

Resilience
- Disaster Recovery Planning
- Business Continuity Planning
- Incident Response Planning
- Third Party Risk Management

Security & Privacy Readiness Reviews
- FFIEC/GLBA
- HIPAA/HITECH
- CCPA/GDPR
- CDPA/NYSHIELD
- FISMA/FedRAMP
- CUI/FAR
- CDI/DFARS
- SOC1ITGC/SOC2

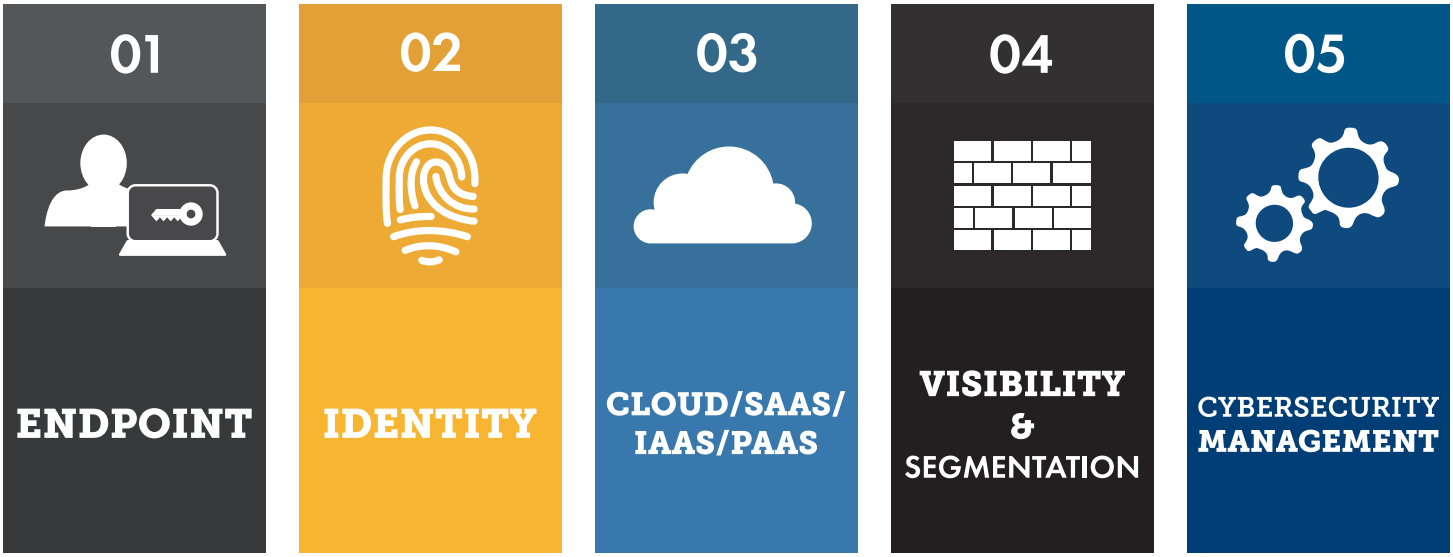
Security & Privacy Standards Implementation
- PCI DSS
- ISO 27000
- NIST CSF/800-53R4 NIST RMF/800-53R5
- NYShield/NYCRR 500
- HIPAA/HITRUST

CYBERSECURITY
SOLUTIONS
& SERVICES

DESIGN

Modern cybersecurity goes way beyond the firewall or even the network and requires a holistic view of the applications, infrastructure, data, processes, and people operating within an organization.

At GDT we've worked to simplify security by breaking it down into 5 fundamental pillars.



Optimally cybersecurity is "shifted to the left" as much as possible and becomes an integrated part of infrastructure design, application development, and IT/business operations. "Bolting on" security is often costly and a recipe for increased effort and complexity. GDT provides a unique value to clients by providing experts in both traditional IT infrastructure and true cybersecurity that will help ensure the solutions and services provided integrate security as a fundamental principle.

DESIGN COMPETENCIES

- SASE/Remote Work/ZTNA
- Endpoint Protection
- Identity & Access Management (IAM)
- Privileged Access Management (PAM)
- SaaS Security/CASB
- Secure Cloud Architecture/Cloud Security
- Data Loss Prevention
- SIEM
- DevSecOps
- IoT Security
- NGFW
- Network Access Control
- Vulnerability Management
- Patch Management
- Micro segmentation/Zero Trust Architecture
- Security for SD-WAN
- Secure SD-Branch
- SOAR
- MFA & SSO
- Email Security

OUR SERVICES

Cybersecurity Assessment

- Cybersecurity Architecture Assessment Workshop
- Cybersecurity Tools Rationalization
- Firewall Rules Assessment
- Cloud Security Assessment

CYBERSECURITY
SOLUTIONS
& SERVICES

DELIVER

We deploy, monitor, manage, and test your cybersecurity infrastructure designs.

NGFW Implementation
Health checks, installation, and monitoring, supported by a team of highly trained experts.

SASE Implementation
Secure your employees and data no matter where they are.

Identity Solutions
NAC, IAM, PAM, MFA, SSO, we cover all the identity acronyms to ensure your identity infrastructure stays secure.

Security Architecture Assessment
Deep dive design workshops to help you evaluate your existing security posture and identify vulnerabilities, inefficiencies, and compliance violations.

OUR SERVICES

Managed Services
- Managed SIEM
- Managed Firewall
- Managed SOC
- Managed Detection & Response

Testing and Simulation
- Vulnerability Testing
- Penetration Testing
- Social Engineering, Physical Security Testing
- Adversarial Simulations (Red Team)
- Tabletop Exercises

Response
- Incident Response
- Breach Assessment

Implementation
- NGFW
- Endpoint Protection
- SASE
- IAM/PAM
- SaaS Security/CASB
- Secure SD-WAN
- Secure SD-Branch
- Network Access Control Systems
- Secure WiFi
- MFA & SSO
- Email Security
- Micro Segmentation/Zero Trust Architecture