CORP INFO TECH

CORPORATE INFORMATION TECHNOLOGIES

MANAGED FIREWALL

DOCUMENT VERSION 2022.09.001

About Us

Corporate Information Technologies (CorpInfoTech) is a full-service information systems management outsourcing and Information Security risk assessment and advisory firm headquartered in Charlotte, NC. Our Information Security team consists of professional penetration testers, technologists, certified assessors, and risk managers that use a team-based approach to deliver a comprehensive assessment product that addresses practical, technical, regulatory, and operational elements collectively.

CorpInfoTech has extensive experience in defense, energy, critical manufacturing, fintech/finsec, banking, and sensitive logistics industries. Certified and accredited by the leading industry organizations including ISC^2, ISSA, Cyber-AB, and SIRA. Members of CorpInfoTech's cybersecurity team hold seats on working groups within the Internet Engineering Task Force (IETF), Center for Internet Security (CIS), and Information Security Systems Association (ISSA).

We actively contribute to the cybersecurity community as a whole and have helped develop and promote the Center for Internet Security (CIS) Critical Security Controls (CSC), a set of pragmatic key cybersecurity security control areas. Our security staff maintain active and relevant information technology and information security certifications that include specialties in ethical hacking, IT governance, network security, cloud security, and Linux/Windows systems administration.

Critical Security Controls

To better align business, technology, security, and risk stakeholders, CorpInfoTech has adopted the Center for Internet Security's (CIS) Critical Security Controls ("CSC") Framework as a universal reference standard within its assessment and information security consulting practices. This framework, derived from National Institute of Standards and Technology (NIST) controls, aligns well with many common security standards including those used by the United States Department of Defense (DoD) and constituent members of the Defense Industrial Base (DIB).

The CIS Controls are recognized within formally regulated industries that are required to comply with external regulatory oversight including that enforced by FINRA, SEC, and FFIEC Information Security guidelines within the financial services industry, HIPAA within the healthcare industry, and PCI-DSS requirements within the payments and retail industries. Using the CIS Security Controls Framework permits audit-friendly cross-reference and compliance with multiple dimensions of compliance within a single organization across many stakeholders.

One Lens, Tailored Solutions

Effective cybersecurity requires constant monitoring and adaption to change based on threats. Outdated cybersecurity technology equipment that is not constantly monitored, maintained, and updated to meet the ever-changing demands of those threats offers ineffective protection. Erroneous or aged configurations that do not reflect the current state of security give hackers and cybercriminals an easy path around your defenses.

CorpInfoTech’s highly trained and experienced team of security professionals based in our Charlotte, NC, Security Operations Fusion Center configure, deploy, manage, and monitor your next-generation connectivity and defense solution to protect your business from cyber threats and keep it connected using state-of-the-art cloud-aware technology. Our highly certified and experienced analysts combine Machine Learning (ML), Artificial Intelligence (AI), and human intelligence to identify and arrest threats. As the state of the security changes, our security personnel proactively adapt your boundary defenses to keep their configuration optimal and at the cutting edge.

Extended Managed Detection and Response (MDR/XDR)

Our Managed NG-Boundary Defense service is a perimeter security and network protection offering that safeguards corporate networks, cloud environments, and beyond to end-users wherever their “office” may be. Using comprehensive inspection and monitoring of your network traffic for cyber threats allow us to quickly identify and respond when threats are found to immediately take action to contain and neutralize them, often before they can impact your business.

Going well beyond blocking suspicious IP addresses and using signature-based detection techniques, we perform full-stack inspection up to and including network applications. Our security fusion center incorporates multiple commercial, governmental, and international threat sharing platforms to broadly identify potential threats. These threat intelligence sources represent information from multiple Information Sharing and Analysis Organizations (ISAOs) and Information Sharing and Analysis Centers (ISACs) including the Multi-State (MS-ISAC), Financial Serviced ISAC (FS-ISAC), Information Technology ISAC (IT-ISAC), and all major cloud platform providers (Google GCP, Amazon AWS, and Microsoft Azure). Using these vast resources, we are able to identify potential threats earlier and arrest their progression through the Cyber Kill Chain more quickly.

Consistent quality across geographically diverse sites

Inconsistencies within the configuration and protection characteristics across deployed firewall systems is a common attack vector used by cybercriminals. Whether it’s inconsistent versions of (vulnerable) software or inconsistent configuration, attackers have long used this as a method to slip by an organization’s defenses. Manually updating and enforcing configuration standards across a number of firewall appliances is a tedious and time-consuming job, which is why it is so often found to be a contributing factor in successful attacks.

Utilizing our decades of experience to inform the methods and mechanisms of firewall fleet management, CorpInfoTech uses an standards-based and modeled work management process to ensure uniformity and consistent deployment and performance quality standards. Using the National Institutes of Standards and Technologies (NIST) Cyber Security Framework (CSF) and the more refined lens of the Center for Internet Security Controls as the lens for effective cybersecurity controls, we bring the knowledge and experience of thousands of cybersecurity professionals in the broader community into the equation. Through these standard frameworks, we are able to deliver standards-based and broadly compliant enterprise-grade security for a fraction of the cost of deploying similar capabilities internally.

Stakeholder Visibility

In the recent past, the delineation between the corporate network boundary and less secure or cloud networks have become more blurry than ever before. As technology and the nature of work have evolved, these boundaries are less clearly defined while an increased importance on the role of controlling communications and protecting your business from threats at the network boundary have grown. In the past firewalls were the go-to technology to implement security and block unwanted network traffic. Today the dynamic nature of the corporate network boundary requires these systems to not only block increasingly advanced threats but also provide secure remote VPN access, self-healing connections to cloud service providers, and prioritize your network traffic to align with business priorities.

Visibility – Receive detailed reporting that goes beyond network threats and extends into application usage, social media usage, and comprehensive inventories of dynamic network boundaries (such as VPN, Cloud Services, and Mobile/5G). Fully customized technical, stakeholder, and executive reporting is included in this solution.

Optimized Access – We deliver industry-leading Gartner Magic Quadrant™ Software Defined Wide Area Network (SD-WAN) capabilities as part of this solution. Ensure critical business applications are always connected using the most secure and economical means. Dynamic automated service-level monitoring provides self-optimizing, self-healing connectivity across the most complex of network architecture.

Maximize Productivity – Identify network behavior and applications that are detracting from performance and productivity. By identifying and controlling traffic at the application-layer patterns of behavior that are time-draining or violate corporate standards and policies can be controlled.

Control data egress – Control and protect sensitive information from unauthorized transmission. Compatible with sophisticated pattern matching, digital watermarking, and origin-controlled data loss prevention technologies, this solution allows for further control of authorized data transmission while increasing visibility of the data types transiting network boundaries.

Service Description

Our service was created from the ground-up to provide the most effective cybersecurity controls that incorporate advanced connectivity technologies like SD-WAN and Extended Detection and Response (XDR) capabilities that are natively cloud-aware and optimized. Incorporating advanced technologies with enterprise-grade Next-Generation Firewall (NGFW), deep integration with Identity and Access Management (IAM) systems, Virtual Private Network (VPN) technologies, robust threat indicator sharing, and modern cryptography to keep your private data secure, our managed next-generation connectivity product was formed.

<u>This service includes the following features</u>:

- ✓ 24/7 health monitoring
- ✓ Dedicated US-based security professionals
- ✓ Customized device configuration and tuning
- ✓ Updates and patch management
- ✓ Centralized log collection and analysis
- ✓ Centralized log retention and reporting
- ✓ All required Licensing
- ✓ Hardware assurance and advanced replacement
- ✓ Configuration backup and storage
- ✓ Configuration change-management / control

- ✓ Managed network detection and response
- ✓ Comprehensive traffic analysis and screening for threats / indicators of compromise
- ✓ SD-WAN
- ✓ Anti-virus
- ✓ Web filtering
- ✓ Application control
- ✓ Intrusion prevention
- ✓ SSL deep packet inspection
- ✓ Web application firewall
- ✓ Data leak prevention
- ✓ Traffic shaping
- ✓ Policy scheduling
- ✓ Site to site IPsec Virtual Private Networking
- ✓ User-level traffic and behavioral attribution (using Microsoft Active directory integration)
- ✓ End-user Virtual Private Network (VPN) access
- ✓ 4G/5G failover

CorpInfoTech's Managed Connectivity solutions are offered using a shared responsibility model in two service editions to ensure the service is "right sized" for your business' needs. Our *Core* service provides smaller organizations with the enterprise-class protection and security features that are focused on arresting adversaries at the network perimeter. While our *Secure* service provides all the features offered under *Core* while extending logging, telemetry, and remote-access capabilities required by larger or more sophisticated organizations.

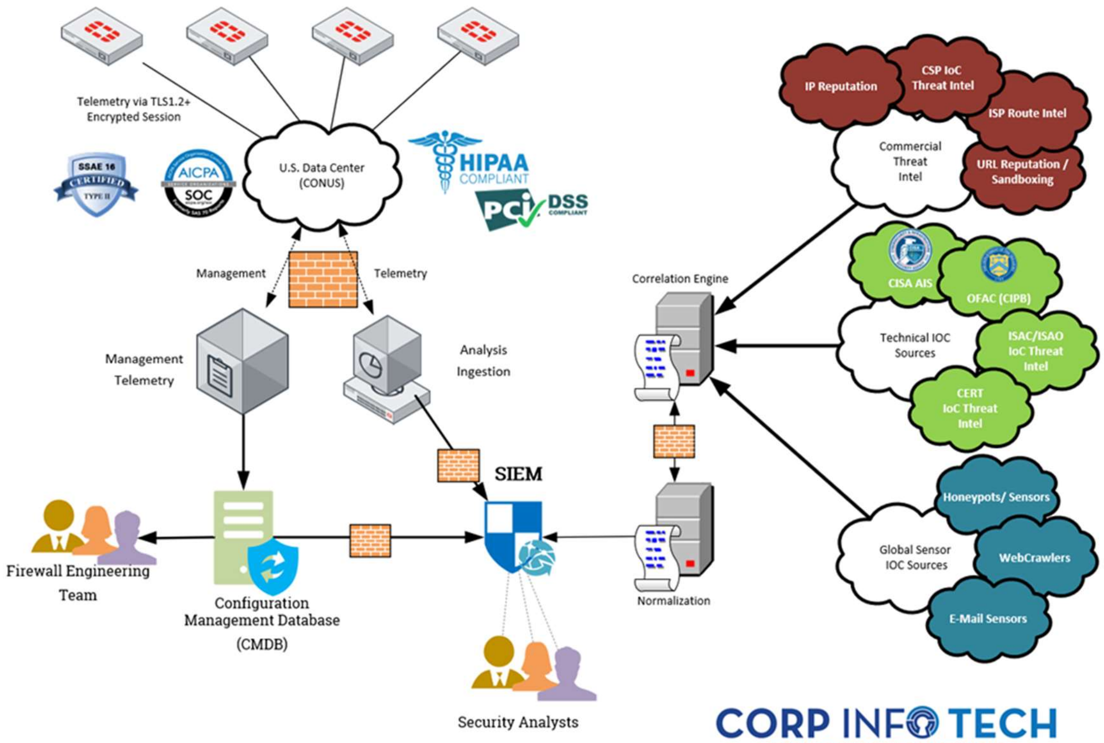
Service Features

	Core	Secure		Core	Secure
Administrative Features			***Managed Features***		
PCI Compliant Solution	-	✓	**247x7x365 Emergency Support**	✓	✓
HIPAA Compliant Solution (with executed BPA)	-	✓	Managed Extended Detection and Response (MDR/XDR)	✓	✓
NIST 800-171 Compliant Solution	✓	✓	Centrally managed risk-based security policies	✓	✓
Priority Hardware Failure Replacement Coverage	-	✓	Active Network Behavioral Analytics	-	✓
Next-Business Day Hardware Failure Replacement Coverage	✓	-	Managed Adversarial Detection & Response	-	✓
Firewall Configuration Management & Backup	✓	✓	Traffic analysis using AI + threat intelligence	-	✓
Firmware Compatibility Research	✓	✓	Monthly Network Boundary Vulnerability Scan	+	✓
Maintenance Features			***Technical Features***		
24x7 Firewall Monitoring	✓	✓	Layer 3 Routing (OSPF, BGP, RIP)	✓	✓
Managed Firmware Upgrades	✓	✓	SSL-VPN for Remote Users	-	✓
Firewall Vulnerability Patching	✓	✓	Site-to-Site IPSEC VPN Tunnels	✓	✓
Firewall Security Hardening	✓	✓	Virtual LAN Extension Support (VXLAN)		✓
BoundaryPerspective(TM) Security Reporting		✓	Network Anti-Malware Scanning (AML/AV)	✓	✓
Customized Operational Reports	✓	✓	Intrusion Detection & Prevention (IDS/IPS)	✓	✓
Log Retention	60 Days	90 Days	Network Application Filtering (Application Control)	✓	✓
Configuration Backup	60 Days	90 Days	Web Content Filtering	✓	✓
			SSL Traffic Inspection (SSL DPI)	✓	✓
Governance Features			Web Application Firewall (WAF)	-	✓
BoundaryPerspective(TM) Security Posture Reports	✓	✓	Software Defined WAN (SD-WAN)	✓	✓
Customized Technical & Security Reports	✓	✓	Time-Based Security Policies	-	✓
Customized Executive-Level Reports	✓	✓	Active Directory User-Based Security Policies	-	✓
Administrative Change-Control Reports	✓	✓	Threat Intelligence	✓	✓
Data Loss Prevention (PII, SSN, HIPAA/EHR Control)	Opt.	✓	***Add-On Features***		
			Wireless Network Control & Management	+	Opt.
			Layer 3 Ethernet Switch	+	Opt.
			4G/5G Failover	+	✓
			Third-party support	+	✓

Service Architecture

Our service architecture uses secure TLS 1.2 / TLS 1.3 management, monitoring, and mechanisms to collect technical telemetry from managed firewall devices. We continuously ingest telemetry and system activity from each device into our privately owned and operated **SSAE 16 Type 1 and Type 2**, **PCI-DSS** Compliant, **HIPAA** Compliant datacenter located within the Continental United Stated (CONUS). All data is encrypted in motion and at-rest using Federal Information Processing Standard (**FIPS**) 140-2 compliant encryption algorithms. Included in this telemetry are numerous technical operational metrics including intrusion detection, anti-virus, application detection, SD-WAN, and network-level information activity.

CorpInfoTech then uses this information to identify traffic or network activity that warrants deeper investigation using numerous commercial, governmental, and privately derived anonymized threat intelligence sharing sources. Our unique threat scoring systems correlate traffic-based and telemetry-based observables with a network of over three million sensors deployed globally. This includes multiple platforms, honeypots, early-warning sensors, and proprietary web crawlers that all combine to deliver high-fidelity threat intelligence of the global cyber space. Aggregately, our clients are secured with the threat sharing resources of over 200 global programs that includes all major Cloud Service Providers (CSPs), strategic technology vendors, multiple national Computer Emergency Response Teams (CERTs), major Internet Service Providers (ISPs), and numerous Information Sharing and Analysis Centers (ISACs).



CORP INFO TECH
CORPORATE INFORMATION TECHNOLOGIES

GET IN TOUCH

704-392-3031
Info@corp-intech.com
www.corp-infotech.com

ONE PARTNER.
TOTAL
CYBERSECURITY.