








## Security Matrix

      							
Technology Solutions Required: Cloud Access Security Broker (CASB), Dark Web Monitoring, Data Loss Prevention (DLP), DDoS Mitigation, Email Security, Incident Response (IR), Managed Patching, Penetration Test, Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA)		✓ (10/10)	○ (9/10)	○ (9/10)	○ (8/10)	○ (8/10)	○ (5/10)
Provider	link to provider's Pathfinder profile	<a href="#">Quest</a>	<a href="#">Dataprise</a>	<a href="#">Ntirety</a>	<a href="#">CBTS</a>	<a href="#">Securus Communications</a>	<a href="#">TierPoint</a>
Primary Line of Business	main service the provider offers	System Integrator	MSP & MSSP	Cloud & MSSP	MSP & MSSP	Carrier	Cloud
# Employees	number of in-house employees	250	500	450	2,000	16	800
Year Company Established	year founded	1982	1995	1998	1995	2012	1999
Year Security First Offered	year the company first offered cybersecurity services	1990	2014	2002	2010	2012	pending
Elevator Pitch	provider's value prop	Quest certified cybersecurity experts work directly with customer executive teams, department managers and key stakeholders to analyze security posture and make appropriate recommendations in developing/supporting a comprehensive digital security program.	Dataprise is a nationwide MSP delivering best-in-class EDR/XDR/MDR complemented by managed service desk, infra/cloud, and DRaaS solutions. We support SMB and Mid-Market clients with tools based on Microsoft technologies and built in a client's own tenant.	With over 20 years of experience, Ntirety is the only company that embeds compliant security throughout your IT and company culture. Protect the entirety of your enterprise through a comprehensive compliant security solution from a single relationship.	CBTS is 20 years old, with 2k employees and \$1B revenue. 60% of revenue is from MSP and MSSP services. We provide security for 1k North American companies, across SASE, SSE, MDR, EDR, Patching, DRaaS, BaaS, VCISO, and Security Consulting.	We leverage extensive experience and security experts to design a solution to fit your needs. We are vendor-agnostic, but specialize in Fortinet, Cisco, and Juniper. The process starts with a pen test & gap analysis, and leads to full SOC instigation.	TierPoint solves complex IT problems so you can focus on business outcomes. We build our solutions around security, not the other way around. Our engineers use a proactive, security-first approach to ensure data security by design.
Common Packages	name & description of provider's most commonly sold products & services.	1. CyberDefense Suite: endpoint protection, email security, FW/IDS/IPS, monitoring, & vulnerability scanning 2. EPaaS: endpoint protection & MDR 3. Free Cybersecurity Workshop 4. Managed FW / IPS / IDS 5. SIEM-as-a-Service	1. Managed Cybersecurity Advanced: 24x7 managed EDR solution with pen tests, continuous vulnerability assessments, dark web scanning, phishing and cyber awareness training, and live metrics dashboard 2. Managed Cybersecurity Premier: includes everything in Advanced plus, cloud-native SIEM and SOAR 3. Managed XDR: next-generation EDR with limited SaaS/cloud log correlation	1. Compliance-as-a-Service: achieve compliance for PCI, GDPR, HIPAA, HITRUST, ISO, CCPA, SOC 1/2, NIST, ITIL 2. Managed Security Services: includes MDR with Remediation 3. NGFW Services: includes SOC/SIEM services 4. vCISO: end-to-end security strategy, implementation, and management 5. IAM: includes SSO and MFA	1. SASE / SSE: multi-platform SD-WAN and SSE (Check Point, Cisco, Palo Alto, VMware) 2. MDR / EDR 3. Consulting: penetration testing, vulnerability assessments, and/or social engineering 4. Security-as-a-Service: SOC, MDR, Public Cloud Security (AWS, Azure, & GCP) 5. Virtual CISO: consulting, governance, and best practices	1. SECaaS: perimeter security and threat event management 2. NGFaaS: hosted NGFW 3. Audit & Recommendation: penetration testing & gap analysis 4. Endpoint Protection	1. CleanIP NGFW: managed next-gen firewall (Fortinet) 2. CleanIP AntiVirus 3. Managed MFA (Duo based) 4. Mimecast Email Security 5. CleanIP XDR (Fortra Alert Logic, Fortinet): cyber monitoring and response solution including threat detection, rapid remediation, and risk reduction
Security Operations Center (SOC)	attributes of provider SOC(s)	In-House (3 locations; 100 employees)  can operate 24/7/365 physically in U.S. and limit access to U.S. persons	In-House (2 locations; 14 employees)  can operate 24/7/365 physically in U.S. and limit access to U.S. persons	In-House (3 locations; 35 employees)  can operate 24/7/365 physically in U.S. and limit access to U.S. persons	In-House (3 locations; 100 employees)	In-House/Outsourced (1 location; 6 employees)	In-House/Outsourced (1 location; 8 employees)  can operate 24/7/365 physically in U.S. and limit access to U.S. persons
Minimum MRC for Ongoing Security	what is the minimum deal size you will consider for an ongoing security opportunity (i.e. MRC, managed services)?	\$500	\$3,000	\$500	\$2,000	n/a	n/a
Minimum NRC for One-Time Security	what is the minimum deal size you will consider for a one-time security opportunity (i.e. NRC, professional services)?	\$5,000	\$10,000	\$1,800	\$10,000	n/a	varies by service
Cloud Access Security Broker (CASB)	CASB is a software that monitors all activity to cloud applications and enforces security policies on traffic destined for the cloud.	Product: Forcepoint	Offered as add-on only Product: Azure AD/Entra	Product: Palo Alto	Offered Standalone	Offered Standalone	Offered as add-on only
	scan hundreds of thousands of websites each day to look for		Included with all managed cybersecurity plans				

Dark Web Monitoring	personal/proprietary information that criminals can use to steal private data	Product: BreachSecure, Digital Shadows	Delivered via third party Product: PII Protect	n/a	n/a	n/a	n/a
Data Loss Prevention (DLP)	how vendor solves the data loss problem, not necessarily a product! protect/prevent data breaches, exfiltration, or unwanted destruction of sensitive data and comply with regulations	Product: Check Point, Cloudflare, Digistal, Fortinet, Keeper, Microsoft 365, Microsoft Defender, Okta, Proofpoint  DLP Solutions: Email, Endpoint, Identity, Network, SaaS, Web App	Offered as add-on only  Product: Crowdstrike, Microsoft Defender  DLP Solutions: Email, Endpoint, Identity, Web App	Product: Cloudflare, Duo, Imperva, Microsoft 365, Microsoft Defender, Mimecast, Palo Alto, Ping, ThreatX  DLP Solutions: Email, Endpoint, Identity, Network, SaaS, Web App	Min. \$5K  Product: Check Point, Cloudflare, CrowdStrike, Microsoft 365, Microsoft Defender, Okta, Palo Alto, Proofpoint  DLP Solutions: Email, Endpoint, Identity, Network, SaaS, Web App	Product: Fortinet, Microsoft 365, Microsoft Defender, Zscaler  DLP Solutions: Email, Endpoint, Identity, Network, SaaS, Web App	Product: Fortinet, Imperva, Microsoft 365, Microsoft Defender, Mimecast  DLP Solutions: Email, Endpoint, Identity, Network, SaaS, Web App
DDoS Mitigation	Solution designed to block Distributed Denial of Service attacks from taking down a network or online application; especially relevant for companies who do business online	Delivered via third party  Product: Cloudflare	Included with all managed cybersecurity plans  Product: Cloudflare	Delivered via third party  Product: Cloudflare, Imperva, Palo Alto, ThreatX	Min. \$5K  Self-service  Product: Radware	Offered as add-on only  Delivered via third party  Product: Cloudflare	Product: Imperva
Email Security	Secure Email Gateway or other product meant to detect malicious or fraudulent email content	Product: Fortinet, Microsoft Defender, Mimecast	Included with all managed cybersecurity plans  Delivered via third party  Product: Microsoft Defender	Product: Mimecast	Product: Proofpoint	Product: Mimecast	Delivered via third party  Product: Microsoft Defender, Mimecast
Identity Provider (IdP)	service that stores and manages digital identities, letting users manage access, adding, or removing privileges	Product: Azure AD, Duo, Forcepoint, Okta	Offered as add-on only Product: Azure AD/Entra	Product: Azure AD, Duo, Palo Alto, Ping	Product: Azure AD, Duo, Okta	Offered as add-on only Product: Fortinet, Proprietary	Product: AWS Director Service, Azure AD, Duo
Incident Response (IR)	an organized, forensic approach to investigate and remediate a security breach; can be on-demand or via monthly retainer	On-Prem & Remote  On-Demand or On Retainer	Delivered via in-house/third party combination  On-Prem & Remote  On-Demand or On Retainer	Delivered via in-house/third party combination  Remote  On-Demand	n/a	Delivered via third party  On-Prem & Remote  On Retainer	n/a
Kubernetes Security	identify and prevent threats in Kubernetes container environments	Offered Standalone	n/a	Product: Palo Alto	n/a	n/a	n/a
Managed Detection & Response (MDR)	combination of security tools and SOC analysts used to identify threats and respond to incidents within a customer environment	Underling Product: Arctic Wolf, Cylance, Microsoft Defender, SentinelOne, Sophos, VMware Carbon Black	Product: Azure Lighthouse, Azure Sentinel, CrowdStrike, Microsoft Defender	Product: Microsoft Defender, Palo Alto	Min. \$5K MRC  Product: CrowdStrike, Fortra's Alert Logic, Microsoft Defender, Microsoft Sentinel	Product: Microsoft Defender	Delivered via third party (Fortra)  Product: Fortra's Alert Logic
Managed Patching	distribute/apply software (OS, applications, embedded systems) updates to remediate vulnerabilities; for a deeper dive, look at our "Managed Solutions" Dynamic Matrix	Product: InTune, Ivanti, Manage Engine	Product: Auvik, Kaseya, Microsoft	Product: BigFix	Min. \$5K  Product: BigFix	n/a	n/a
Multi-Factor Authentication (MFA)	an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence	Product: Duo, OneLogin, Ping, SecureAuth	Product: Azure AD/Entra, Duo	Product: Azure AD, Duo, Ping	Product: Duo	Product: Fortinet, Microsoft Defender	Offered as add-on only  Product: Duo
Next-Gen Firewall	A next-gen firewall includes features such as intrusion detection, intrusion prevention, URL filtering, deep packet inspection, and more.	Cloud / On-Prem  Product: Aruba, Cisco, Fortinet, Palo Alto	Offered as add-on only  Cloud / On-Prem  Product: Cisco, Cisco Meraki, Fortinet, Juniper, Palo Alto, SonicWall	Offered as add-on only  Cloud / On-Prem  Product: Palo Alto	Min. \$500 users  Cloud / On-Prem  Product: Check Point, Cisco, Palo Alto	n/a	pending
Password Manager	allows security leaders to gain control over (manage) company passwords in a secure manner	Includes Secrets Management for Development Pipeline  Product: CyberArk, Dashline, Keeper, LogMeOnce, ManageEngine, Zoho	n/a	n/a	n/a	Delivered via third party	n/a
Penetration Test	can be offered for infrastructure/network, apps (web/mobile), devices	CBI Secure, External, Internal, IoT, Network, Phishing, Web App	Delivered via third party (EDWPS): External, Internal, IoT, Network, Phishing, Social Engineering, Web App	External, Internal, IoT, Network, Phishing, Social Engineering, Web App	External, Internal, IoT, Network, Phishing, Social Engineering, Web App	Delivered via third party External, Internal, Web App	Delivered via third party External, Internal, IoT, Network, Phishing, Social Engineering, Web App
		Min. \$5K  One-Time Services:					

Physical Security	cloud-based monitoring of onsite infrastructure	assessments  Ongoing Services: access control, analytics, armed/private security, biometrics, drone management, perimeter radar, video surveillance, vulnerability assessments  Product: Avigilon, Axis, Brivo, Exacq, Hanwa, I-Pro, Lenel, Milestone, Qognify, S2, Samsung, Verkada	n/a	n/a	Min. \$5K  One-Time Services: professional services for Meraki camera design, placement, and strategy  Ongoing Services: management and monitoring of Meraki camera infrastructure	n/a	n/a
Privileged Access Management (PAM)	PAM allows organizations to secure infrastructure and applications by designating special access or abilities above that of a standard user.	Product: BeyondTrust, CyberArk, Manage Engine	Offered as add-on only Product: Azure AD/Entra	Product: Azure AD, CyberArk	Min. \$5K Product: CyberArk	Offered as add-on only Product: Fortinet	n/a
Ransomware / Threat Actor Negotiation	expert assistance to reduce total loss, stop further damage, and assist in recovery	Offered as add-on only	Delivered via third party	n/a	n/a	n/a	n/a
Reputation Management	increase brand/keyword driven search results; decrease negative content within search engines	Product: BitSight	n/a	n/a	n/a	n/a	n/a
Risk & Compliance Assessments	may include risk assessments and gap analyses to evaluate security posture, assessments to determine compliance	Supported Standards: CCPA, CMMC, GDPR, HIPAA, HITRUST, ISO 27001/2, ITAR, NIST CSF, NIST 800-53, NIST 800-171, PCI-DSS, SOC 2, SOX	Delivered via in-house/third party combination  Supported Standards: CCPA, CMMC, GDPR, HIPAA, NIST 800-71, SOC 2, SOX	Delivered via in-house/third party combination  CCPA, CMMC, GDPR, HIPAA, HITRUST, ISO 27001/2, NIST CSF, NIST 800-53, NIST 800-171, PCI, SOC 2	Supported Standards: CCPA, CMMC, GDPR, HIPAA, ISO 27001/2, NIST CSF, NIST 800-53, NIST 800-171, PCI	Delivered via third party  Supported Standards: HIPAA	Delivered via third party  Supported Standards: CCPA, CMMC, Federa ATO, FedRAMP, GDPR HIPAA, HITRUST, ISO 27001/2, ITAR, NIST CS, NIST 800-53, NIST 800-171, PCI-DSS, SOX
Secure Web Gateway (SWG)	SWG protects users from web-based threats and blocks access to inappropriate content.	Product: Cisco, Cloudflare, Palo Alto, Zscaler	n/a	Offered as add-on only Product: Palo Alto	Min. 500 users Product: Check Point, Cisco, Palo Alto, VMware	Product: Fortinet	pending
Security Awareness Training	one-time or ongoing cybersecurity awareness training offered directly to end users	Delivered via third party Product: Hook (min. 10 users), KnowBe4	Delivered via in-house/third party combination Product: KnowBe4, PII Protect	Offered as add-on only Product: KnowBe4	n/a	n/a	Product: Microsoft Defender
Security Workshop (NRC)	one-time engagement with IT/Security staff and primary stakeholders to discuss their cybersecurity strategy and means of improvement	Offered Free	Delivered via in-house/third party combination	Offered as add-on only	Min. \$5K	n/a	n/a
SIEM & Log Management	a managed solution that provides holistic view of customer's environment and correlates various data sources to identify threats in real time	Delivered via in-house/third party combination  On-Prem & Hosted  Can install, operate, and maintain a SIEM purchased by client.  Product: Arctic Wolf, Fortinet, Fortra's Alert Logic, Microsoft Sentinel, QRadar, Splunk	Offered as add-on only  Hosted Product: Microsoft Sentinel	Hosted  Can install, operate, and maintain a SIEM purchased by client (Microsoft Sentinel only) Product: LogRhythm, Microsoft Sentinel	Hosted  Can install, operate, and maintain a SIEM purchased by client. Product: Fortra's Alert Logic, Microsoft Sentinel	Offered as add-on only Product: Fortinet	Delivered via third party (Fortra, Stratozen) Hosted Product: Fortinet, Fortra's Alert Logic
Single Sign-On (SSO)	allows a user to log in with a single ID to any of several related, yet independent, software systems without re-entering authentication factors	Okta offered standalone; CyberArk/Duo offered as add-on only  Deploy & Manage: CyberArk, Duo, Okta	Offered as add-on only Deploy & Manage: Azure AD/Entra, Duo, Okta	Deploy & Manage: Azure AD, Ping	Deploy: Duo, Okta Manage: Duo	Deploy & Manage: Fortinet	n/a
Virtual CISO	an outsourced CISO to help a company build and maintain an information security program without an FTE; especially relevant to align with compliance standards	Min. \$5K retainer	Min. \$3K MRC	Min. 4 hours / week	Min. \$20,000 (60 hours)  Delivered via in-house/third party combination	n/a	n/a
Vulnerability Scanning	tool to assess computers, networks or applications for known weaknesses	Delivered via third party  One-Time or Ongoing Product: Rapid7	Offered as add-on only  One-Time or Ongoing Product: Crowdstrike, Microsoft Defender, Tenable.io	Delivered via third party  One-Time or Ongoing Product: Tenable.io	One-Time or Ongoing Product: BigFix, Tenable.io	Qualys	One-Time or Ongoing Product: Rapid7, Tenable.io
WAF	Web Application Firewall used to protect against attacks targeting Internet-facing applications	Product: Cato, Cloudflare, Zscaler	Offered as add-on only Product: Azure, Cloudflare	Product: Cloudflare, Imperva, Prisma Cloud, ThreatX	Product: Cloudflare	Delivered via in-house/third party combination Product: Fortinet	Delivered via third party Product: Imperva
			Delivered via in-				

Zero Trust Network Access (ZTNA)	ZTNA provides secure, remote access to applications based on defined access control policies.	Product: Aruba, Cisco, Palo Alto	house/third party combination Product: Cloudflare, Microsoft Entra	Product: Palo Alto	Delivered via third party Product: Check Point, Cisco, Palo Alto, VMware	Offered as add-on only Product: Fortinet	<i>pending</i>
----------------------------------	---	----------------------------------	---	--------------------	---	---	----------------