CALNET 3
Category 7 – Network Based Management Security

Table of Contents

7.2.1.4.a DDoS Detection and Mitigation Service Features

Contractor's Summary description of service: AT&T Distributed Denial of Service (DDoS) Defense is a service that is designed to detect and mitigate distributed denial of service attacks on your network using best practices and best of breed tools. DDoS Defense helps identify and block malicious packets in near real time to help you prevent possible negative affects regarding the flow of your business traffic.

DDoS Defense is the service based on the data from the AT&T IP backbone network and doesn't require you to purchase additional bandwidth or premises equipment.

Depending on your configuration, a shared or dedicated set of network mitigation devices scrub your traffic for denial of service attacks. A shared configuration allows you to share network detector devices and a farm of network mitigation devices with other AT&T customers. A dedicated configuration provides you with network mitigation devices dedicated to you. AT&T and non AT&T circuits can be supported.

Geographic Availability: Domestic United States

Service Limitations and Restrictions Tier will be determined by AT&T accessing the customer's requirements.

Change Charge Applicability: N/A (except as noted below in Feature Restrictions, Limitations and Additional Information)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
1	DDoS Detection and Mitigation, 1 – 2 GB	DDOS2	DDos Detection and Mitigation Service as described in Section 7.2.1.3 for 1-2 GB of traffic flow.		$0.00	$2,123.80	Per Network	N/A	Yes	Required
2	DDoS Detection and Mitigation, 3 – 4 GB	DDOS4	DDoS Detection and Mitigation Service as described in Section 7.2.1.3 for 3-4 GB of traffic flow		$0.00	$2,410.80	Per Network	N/A	Yes	Required
3	DDoS Detection and Mitigation, 5 – 6 GB	DDOS6	DDoS Detection and Mitigation Service as described in Section 7.2.1.3 for 5-6 GB of traffic flow		$0.00	$2,927.40	Per Network	N/A	Yes	Required

7.2.2.3 Email Monitoring and Scanning Service Features

Contractor's Summary description of service: AT&T Secure E-Mail Gateway (SEG) is a network-based Security as a Service (SecaaS) offering. SEG protects customers from internal and external email threats that can include: commercial spam, malicious attachments, direct email server connections from spammers and botnet-controlled endpoints, and email embedded URL-based attacks. SEG provides features and tools that enable customers to comply with data privacy and retention regulations, meet legal discovery requirements, and implement data loss prevention strategies. SEG customers retain responsibility and control over much of the configuration and settings for the service.

SEG Advanced

The Secure E-Mail Gateway (SEG) Advanced service helps protect customer networks from inbound messages containing spam, viruses, and malware.
The Service provides features that enable customer to manage and enforce its security policy on outbound email content.
The Service provides disaster recovery protection against lost email data in the event of a customer email server outage and provides end-user continuity functionality if the customer email server becomes unavailable.
SEG is administered by the customer through a self-service web console and provides a suite of reports.
SEG requires that the Customer own and manage their own Simple Mail Transfer Protocol (SMTP) email server or servers. The customer must also own and manage their own internet domain(s) in order to direct email to the Service for filtering.

Geographic Availability: Domestic United States

Service Limitations and Restrictions None

Change Charge Applicability: N/A (except as noted below in Feature Restrictions, Limitations and Additional Information)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
1	Email Monitoring and Scanning Service, 1-49	SEGA01	Email managed security services seat as described in Section 7.2.2.		$0.00	$2.85	Seat	N/A	Yes	Required
2	Email Monitoring and Scanning Service, 50-74	SEGA50	Email managed security services seat as described in Section 7.2.2.		$0.00	$1.62	Seat	N/A	Yes	Required
3	Email Monitoring and Scanning Service, 75-99	SEGA75	Email managed security services seat as described in Section 7.2.2.		$0.00	$1.30	Seat	N/A	Yes	Required
4	Email Monitoring and Scanning Service, 100-500	SEGA100	Email managed security services seat as described in Section 7.2.2.		$0.00	$0.96	Seat	N/A	Yes	Required
5	Email Monitoring and Scanning Service, 501-1000	SEGA501	Email managed security services seat as described in Section 7.2.2.		$0.00	$0.59	Seat	N/A	Yes	Required
6	Email Monitoring and Scanning Service, 1001 and above	SEG1001	Email managed security services seat as described in Section 7.2.2.		$0.00	$0.45	Seat	N/A	Yes	Required

7.2.3.2 Web Security and Filtering Service Features

Contractor's Summary description of service: AT&T Web Security service helps create a protected and productive Internet environment for your organization. The service is designed to keep malware off your organizations network and allow you to control the use of the Web by employing Web Filtering, Web Malware Scanning and Anywhere+ Control features. As a fully managed service, AT&T Web Security Service requires no additional hardware, upfront equipment costs or ongoing system maintenance.

Implementation is completed via conference calls with the customer. AT&T will direct the customer to perform certain software configurations onsite.
In addition to predefined reports, custom reports and analysis through the drill down tool is available to gather specific information regarding web usage.

Active Directory Integration:
AT&T Web Security integrates into your active directory service with a Connector Software, provided as part of the service.

Firewall Redirection:
The Proxy Settings are pushed to browsers via an Active Directory GPO, browsers connect through Firewall on port 8080 to the Connector which receives client information and queries the Active Directory Server for Group Information, it then proxies to AWS upstream.
The Firewall blocks all other GET requests this provides End User/Group granularity for applying rules and reporting.

Archiving:
Archiving of historical data is 90 days for allowed traffic and 1 year for blocked. Custom reports can be created to export CSV data dumps on a monthly basis for customer archiving of historical periods longer than provided.

Geographic Availability: Domestic United States

Service Limitations and Restrictions None

Change Charge Applicability: N/A (except as noted below in Feature Restrictions, Limitations and Additional Information)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
1	Web Security and Filtering Service	WSSBND	Web Security and Filtering service as described Section 7.2.3.		$0.00	$0.66	Per User	$0.00	Yes	Required
	GSG Select Business		The Service Component Global Security Gateway - Business ("GSG - Business") supports configuration and enforcement of security policies that are Web and Internet Security with Standard Cloud Firewall and scans web traffic (ports 80 and 443) as well as non-web Internet traffic in a sequential manner. When web traffic is received, the service's web module scans the traffic for policy enforcement, after which the traffic is sent to the firewall module for additional policy enforcement. The standard firewall included supports IP address-, port-, and protocol-							

			based allow/block policies. When the service encounters any HTTPS traffic, further inspection of the traffic is completed with SSL inspection. The Service inspects the traffic and sends it to the web module for policy enforcement. If SSL inspection is disabled, the Service will only perform policy checking and enforcement on unencrypted traffic. The Service supports several options for forwarding traffic including the ability to forward traffic from the enterprise via a tunnel termination endpoint using Generic Routing Encapsulation (GRE) or IPsec Tunnel (unencrypted only). Traffic can also be forwarded via PAC file, or mobile application. If using the mobile application, it is Customer's responsibility to deploy the application. The application is only available where allowed by local regulations. AT&T will configure traffic forwarding from AT&T-managed tunnel termination devices (managed routers or firewalls, for example) only until Service is activated. It is Customer's responsibility to configure traffic forwarding on any Customer-owned/managed or third-party managed tunnel termination devices.							
	GSG Business 1-99	Multiple (See Below)	GSG Business 1-99							
2	GSG - BUS 1-99	GSGB1	GSG - Business 1-99 Seats - Compatible with add on features below. Self installation included. For additional installation assistance, utilize Network Security Implementation Consultant		$0.00	$8.50	Seat	$0.00	Yes	Required

	GSG Add On Features 1-99	Multiple (See Below)	Add On Features that can be added to GSG-BUS 1-99 Only							
3	Advanced Cloud Sandbox 1-99	GSGB2	Needed if organization requires custom rule capabilities not offered in the standard sandbox		$0.00	$5.35	Seat	$0.00	Yes	Required
4	Advanced Cloud Firewall 1-99	GSGB3	Needed if organization requires full inline inspection of all SSL traffic with granular policy control		$0.00	$5.35	Seat	$0.00	Yes	Required
5	Data Loss Prevention 1-99	GSGB4	Needed if organization wants to perform inline scanning to prevent confidential data from leaving the organization		$0.00	$3.26	Seat	$0.00	Yes	Required
	GSG Business 100-499	Multiple (See Below)	GSG Business 100-499							
6	GSG - BUS 100-499	GSGB5	GSG - Business 100-499 Seats - Compatible with add on features below.		$3,910.00	$7.35	Seat	$0.00	Yes	Required
	GSG Add On Features 100-499	Multiple (See Below)	Add On Features that can be added to GSG-BUS 100-499 Only							
7	Advanced Cloud Sandbox 100-499	GSGB6	Needed if organization requires custom rule capabilities not offered in the standard sandbox		$0.00	$4.39	Seat	$0.00	Yes	Required
8	Advanced Cloud Firewall 100-499	GSGB7	Needed if organization requires full inline inspection of all SSL traffic with granular policy control		$0.00	$4.39	Seat	$0.00	Yes	Required
9	Data Loss Prevention 100-499	GSGB8	Needed if organization wants to perform inline scanning to prevent confidential data from leaving the organization		$0.00	$2.43	Seat	$0.00	Yes	Required
	GSG Business 500-999	Multiple (See Below)	GSG Business 500-999							
10	GSG - BUS 500-999	GSGB9	GSG - Business 500-999 Seats - Compatible with add on features below.		$3,910.00	$6.96	Seat	$0.00	Yes	Required
	GSG Add On Features 500-999	Multiple (See Below)	Add On Features that can be added to GSG-BUS 500-999 Only							
11	Advanced Cloud Sandbox 500-999	GSGB10	Needed if organization requires custom rule capabilities not offered in the standard sandbox		$0.00	$4.13	Seat	$0.00	Yes	Required
12	Advanced Cloud Firewall 500-999	GSGB11	Needed if organization requires full inline inspection of all SSL traffic with granular policy control		$0.00	$4.13	Seat	$0.00	Yes	Required

13	Data Loss Prevention 500-999	GSGB12	Needed if organization wants to perform inline scanning to prevent confidential data from leaving the organization		$0.00	$2.26	Seat	$0.00	Yes	Required
	GSG Business 1000-2499	Multiple (See Below)	GSG Business 1000-2499							
14	GSG - BUS 1000-2499	GSGB13	GSG - Business 1,000-2,499 Seats - Compatible with add on features below.		$3,910.00	$6.62	Seat	$0.00	Yes	Required
	GSG Add On Features 1000-2499	Multiple (See Below)	Add On Features that can be added to GSG-BUS 1000-2499 Only							
15	Advanced Cloud Sandbox 1,000-2,499	GSGB14	Needed if organization requires custom rule capabilities not offered in the standard sandbox		$0.00	$3.92	Seat	$0.00	Yes	Required
16	Advanced Cloud Firewall 1,000-2,499	GSGB15	Needed if organization requires full inline inspection of all SSL traffic with granular policy control		$0.00	$3.92	Seat	$0.00	Yes	Required
17	Data Loss Prevention 1,000-2,499	GSGB16	Needed if organization wants to perform inline scanning to prevent confidential data from leaving the organization		$0.00	$2.11	Seat	$0.00	Yes	Required
	GSG Business 2500-4999	Multiple (See Below)	GSG Business 2500-4999							
18	GSG - BUS 2500-4999	GSGB17	GSG - Business 2,500-4,999 Seats - Compatible with add on features below.		$3,910.00	$6.01	Seat	$0.00	Yes	Required
	GSG Add On Features 2500-4999	Multiple (See Below)	Add On Features that can be added to GSG-BUS 2500-4999 Only							
19	Advanced Cloud Sandbox 2500-4999	GSGB18	Needed if organization requires custom rule capabilities not offered in the standard sandbox		$0.00	$3.56	Seat	$0.00	Yes	Required
20	Advanced Cloud Firewall 2500-4999	GSGB19	Needed if organization requires full inline inspection of all SSL traffic with granular policy control		$0.00	$3.56	Seat	$0.00	Yes	Required
21	Data Loss Prevention 2500-4999	GSGB20	Needed if organization wants to perform inline scanning to prevent confidential data from leaving the organization		$0.00	$1.93	Seat	$0.00	Yes	Required
	GSG Business 5000-9999	Multiple (See Below)	GSG Business 5000-9999							
22	GSG - BUS 5000-9999	GSGB21	GSG - Business 5,000-9,999 Seats - Compatible with add on features below.		$3,910.00	$5.85	Seat	$0.00	Yes	Required

	GSG Add On Features 5000-9999	Multiple (See Below)	Add On Features that can be added to GSG-BUS 5000-9999 Only							
23	Advanced Cloud Sandbox 5000-9999	GSGB22	Needed if organization requires custom rule capabilities not offered in the standard sandbox		$0.00	$3.46	Seat	$0.00	Yes	Required
24	Advanced Cloud Firewall 5000-9999	GSGB23	Needed if organization requires full inline inspection of all SSL traffic with granular policy control		$0.00	$3.46	Seat	$0.00	Yes	Required
25	Data Loss Prevention 5000-9999	GSGB24	Needed if organization wants to perform inline scanning to prevent confidential data from leaving the organization		$0.00	$1.88	Seat	$0.00	Yes	Required
	GSG Business 10,000+	Multiple (See Below)	GSG Business 10,000+							
26	GSG - BUS 10000+	GSGB25	GSG - Business 10,000+ Seats - Compatible with add on features below.		$3,910.00	$5.26	Seat	$0.00	Yes	Required
	GSG Add On Features 10,000+	Multiple (See Below)	Add On Features that can be added to GSG-BUS 10,000+ Only							
27	Advanced Cloud Sandbox 10000+	GSGB26	Needed if organization requires custom rule capabilities not offered in the standard sandbox		$0.00	$3.13	Seat	$0.00	Yes	Required
28	Advanced Cloud Firewall 10000+	GSGB27	Needed if organization requires full inline inspection of all SSL traffic with granular policy control		$0.00	$3.13	Seat	$0.00	Yes	Required
29	Data Loss Prevention 10000+	GSGB28	Needed if organization wants to perform inline scanning to prevent confidential data from leaving the organization		$0.00	$1.70	Seat	$0.00	Yes	Required
	GSG Business Universal	Multiple (See Below)	GSG Business Universal Options (Available for all levels of GSG-BUS)							
30	NSS Log Recovery Web Mgmt Fee	GSGB29	Needed if organization needs 1-hour of log recovery		$0.00	$1952.80	Each	$0.00	Yes	Required
31	NSS Log Recovery Firewall Mgmt Fee	GSGB30	Needed if organization needs 1-hour of log recovery		$0.00	$1952.80	Each	$0.00	Yes	Required
32	ICAP For DLP	GSGB31	Needed if organization requires the use of Internet Content Adaption Protocol		$0.00	$2424.42	Each	$0.00	Yes	Required
33	Dedicated Proxy Port	GSGB32	Needed if organization needs to forward remote user traffic to dedicated ports for the		$0.00	$616.52	Each	$0.00	Yes	Required

			purpose of applying location policies							
34	SSL Interception Private Cert.	GSGB33	Allows the use of a organization-provided certificate for SSL inspection		$0.00	$1245.35	Each	$0.00	Yes	Required
35	Priority Categorization Service	GSGB34	Needed if organization needs the ability to generate daily categorization of their top 100 unknown domains		$0.00	$3603.47	Each	$0.00	Yes	Required
36	Network Security Implementation Consultant	GSGB35	May be required for implementation network security consultant performing advanced on-site installation and tests interoperability with other products. During normal business hours, Mon – Fri, 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in this category.		$251.25	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Contractor's Summary description of service:
Correlated Log Management Services (CLMS))/Advanced Threat and Log Analysis Service (ATLAS utilizes AT&T's expertise in security analysis and operations within the AT&T Security Operations Center (SOC) to correlate information from multiple devices and device types, both on premises and network based in the AT&T network.

- Provides AT&T an overview of your network by correlating alerts from multiple devices and device types across the entire enterprise.
- AT&T prioritizes security events based on threat and risk management methodologies generated from AT&T standards and customer defined standards.
- AT&T provides rapid notification to the customer when security events are detected and are identified as critical by AT&T SOC
- Includes customer access to weekly and monthly security summary analysis reports

The Correlated Log Management/Advanced Threat and Log Analysis service includes standard reports, threat analysis reports, log storage, Implementation assistance and initial device policy tuning. AT&T collects the security relevant log and event information from firewalls, intrusion prevention sensors and other network devices using agent-less Parser/Aggregator technology deployed in your network. Event collection is provided for a wide variety of security and network devices which may be located within the AT&T network or on your premises. A diverse set of "feeds" from security devices and services is recommended in order to get a better view of identified threats to your systems and take full advantage of the CLMS/ATLAS system's correlation capabilities. The intelligence produced is used by AT&T's security analysis team to make security recommendations to you. Security recommendations, in the form of an email or a phone call, may vary in detail depending on type of incident, granularity of visibility within the network and breadth of the view. The response will be both verbal (phone call) and written (e-mailed) for severe and high incidents, and written only (e-mailed) for others as appropriate.

Geographic Availability: Domestic United States

Service Limitations and Restrictions None

Change Charge Applicability: N/A (except as noted below in Feature Restrictions, Limitations and Additional Information)

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
1	SIEM, 1 – 15 Devices	CLMS1	SIEM service as described in Section 7.2.4.		$10,000.00	$1,260.75	Initial Deployment	N/A	Yes	Required
2	Each additional device	CLMS1A	Each additional device above 15.		$100.00	$101.48	Device	N/A	Yes	Required
3	SIEM, 16 - 40 Devices	CLMS2	SIEM service as described in Section 7.2.4.		$14,000.00	$3,034.00	Initial Deployment	N/A	Yes	Required
4	Each additional device	CLMS2A	Each additional device above 40.		$100.00	$91.23	Device	N/A	Yes	Required
5	SIEM, 41 - 100 Devices	CLMS3	SIEM service as described in Section 7.2.4.		$16,000.00	$4,704.75	Initial Deployment	N/A	Yes	Required
6	Each additional device	CLMS3A	Each additional device above 100.		$100.00	$57.40	Device	N/A	Yes	Required
7	SIEM, 101 – 250 Devices	CLMS4	SIEM service as described in Section 7.2.4.		$19,000.00	$10,793.25	Initial Deployment	N/A	Yes	Required
8	Each additional device	CLMS4A	Each additional device above 250.		$100.00	$52.28	Device	N/A	Yes	Required
9	SIEM, 251 - 1000 Devices	CLMS5	SIEM service as described in Section 7.2.4.		$25,000.00	$23,739.00	Initial Deployment	N/A	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
10	Each additional device	CLMS5A	Each additional device above 1000.		$100.00	$28.70	Device	N/A	Yes	Required
11	SIEM, 1001 - 2500 Devices	CLMS6	SIEM service as described in Section 7.2.4.		$29,000.00	$34,850.00	Initial Deployment	N/A	Yes	Required
12	Each additional device	CLMS6A	Each additional device above 2500.		$100.00	$17.43	Device	N/A	Yes	Required
13	SIEM, 2501-5000 Devices	CLMS7	SIEM service as described in Section 7.2.4.		$40,000.00	$48,790.00	Initial Deployment	$0.00	Yes	Required
14	Each additional	CLMS7A	Each additional device above 5,000.	Each additional device added after the initial enablement will incur a separate one-time charge. Each additional device above the Tier threshold will include an additional monthly recurring charge as well as the one-time charge. Tier 7 threshold is 5,000+ devices.	$100.00	$10.22	Device	$0.00	Yes	Required
15	CLMS/ATLAS Tier 1 Storage	CLMY1	Correlated Log Management Service (CLMS)/Advanced Threat and Log Analysis Service (ATLAS) – Tier 1 Per Incremental Year of Storage used with CLMS1.	If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.	$0.00	$239.85	Per Enablement	$0.00	Yes	Required
16	CLMS/ATLAS Tier 2 Storage	CLMY2	Correlated Log Management Service (CLMS)/Advanced Threat and Log Analysis Service (ATLAS) – Tier 2 Per Incremental Year of Storage used with CLMS2.	If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.	$0.00	$546.33	Per Enablement	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
17	CLMS/ATLAS Tier 3 Storage	CLMY3	Correlated Log Management Service (CLMS)/Advanced Threat and Log Analysis Service (ATLAS) – Tier 3 Per Incremental Year of Storage used with CLMS3.	If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.	$0.00	$799.50	Per Enablement	$0.00	Yes	Required
18	CLMS/ATLAS Tier 4 Storage	CLMY4	Correlated Log Management Service (CLMS)/Advanced Threat and Log Analysis Service (ATLAS) – Tier 4 Per Incremental Year of Storage used with CLMS4.	If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.	$0.00	$1,295.60	Per Enablement	$0.00	Yes	Required
19	CLMS/ATLAS Tier 5 Storage	CLMY5	Correlated Log Management Service (CLMS)/Advanced Threat and Log Analysis Service (ATLAS) – Tier 5 Per Incremental Year of Storage used with CLMS5.	If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.	$0.00	$2,373.90	Per Enablement	$0.00	Yes	Required
20	CLMS/ATLAS Tier 6 Storage	CLMY6	Correlated Log Management Service (CLMS)/Advanced Threat and Log Analysis Service (ATLAS) – Tier 6 Per Incremental Year of Storage used with CLMS6.	If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.	$0.00	$3,485.00	Per Enablement	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
21	CLMS/ATLAS Tier 7 Storage	CLMY7	Correlated Log Management Service (CLMS) Advanced Threat and Log Analysis Service (ATLAS) – Tier 7 Per Incremental Year of Storage used with CLMS7.	If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.	$0.00	$4,612.50	Per Enablement	$0.00	Yes	Required
22	CLMS/ATLAS Device Interface	CLMCDI	Correlated Log Management Service (CLMS)/Advanced Threat and Log Analysis Service (ATLAS) – Custom (Non-standard) Device Interface	Devices not included in the Supported Devices List incur a One-Time charge per each unique device (or group of devices). If a customer has multiple devices of the same type with the same operating environment, one fee will be levied. Development time may vary, and will be identified at time of request. Check with your AT&T Account Team to determine if your device is supported.	$250.00	$0.00	Per Device	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
23	CLMS/ATLAS Report	CLMRPT	Correlated Log Management Service (CLMS)/Advanced Threat and Log Analysis Service (ATLAS) – Custom (Non-standard) Report	Customers requiring special reports not listed in the SETA REPORTS List will incur a One-Time charge per each report. Development time may vary.	$250.00	$0.00	Per Report	$0.00	Yes	Required
24	Custom Log Sources – Level 1	CLMC1	Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Level 1 is a threshold of 15 devices.	Custom Level is based on the number of custom sources.	$250.00	$126.08	Per Custom Source	$0.00	Yes	Required
25	Custom Log Sources – Level 2	CLMC2	Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Level 2 is a threshold of 40 devices.	Custom Level is based on the number of custom sources.	$250.00	$113.78	Per Custom Source	$0.00	Yes	Required
26	Custom Log Sources – Level 3	CLMC3	Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Level 3 is a threshold of 100 devices.	Custom Level is based on the number of custom sources.	$250.00	$70.73	Per Custom Source	$0.00	Yes	Required
27	Custom Log Sources – Level 4	CLMC4	Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Level 4 is a threshold of 250 devices.	Custom Level is based on the number of custom sources.	$250.00	$64.58	Per Custom Source	$0.00	Yes	Required
28	Custom Log Sources – Level 5	CLMC5	Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Level 5 is a threshold of 1000 devices.	Custom Level is based on the number of custom sources.	$250.00	$35.88	Per Custom Source	$0.00	Yes	Required
29	Custom Log Sources – Level 6	CLMC6	Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Level 6 is a threshold of 2500 devices.	Custom Level is based on the number of custom sources.	$250.00	$20.50	Per Custom Source	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
30	Custom Log Sources – Level 7	CLMC7	Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Level 7 is a threshold of 5000+ devices.	Custom Level is based on the number of custom sources.	$250.00	$20.91	Per Custom Source	$0.00	Yes	Required
31	Advanced Correlation – Tier 1	CLMA1	Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 1 is a threshold of 15 devices.		$750.00	$239.85	Per Device	$0.00	Yes	Required
32	Advanced Correlation – Tier 2	CLMA2	Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 2 is a threshold of 40 devices.		$1,500.00	$546.33	Per Device	$0.00	Yes	Required
33	Advanced Correlation – Tier 3	CLMA3	Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 3 is a threshold of 100 devices.		$2,000.00	$799.50	Per Device	$0.00	Yes	Required
34	Advanced Correlation – Tier 4	CLMA4	Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 4 is a threshold of 250 devices.		$3,000.00	$1,295.60	Per Device	$0.00	Yes	Required
35	Advanced Correlation – Tier 5	CLMA5	Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 5 is a threshold of 1000 devices.		$4,000.00	$2,373.90	Per Device	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
36	Advanced Correlation – Tier 6	CLMA6	Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 6 is a threshold of 1000 devices.		$5,000.00	$3,485.00	Per Device	$0.00	Yes	Required
37	Advanced Correlation – Tier 7	CLMA7	Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 7 is a threshold of 5000 devices.		$6,000.00	$5,125.00	Per Device	$0.00	Yes	Required
	AT&T VSS-PRO (Vulnerability Scanning Service)		The VSS-Pro service is used to conduct host discovery and/or vulnerability scans on external and/or internal IP-based systems and networks. A variety of scanning techniques are employed to survey the security posture of the target IP-based systems and networks. These scans proactively test for known vulnerabilities and the existence of mainstream industry practice security configurations. External scanning addresses all Internet-facing assets such as routers, firewalls, web servers, and e-mail servers for potential security weaknesses, checking for the "open doors" that could allow a hacker to gain unauthorized access to the network and exploit critical assets. Internal scanning addresses all internal assets such as workstations, intranet servers, and printers for Trojans, improper configurations, peer-to-peer (PTP) file sharing programs such as Morpheus, Kazaa, etc., and more. The VSS-Pro service also provides workflow management, host-based risk assignments, and							

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			remediation progress reporting. In addition, VSS-Pro includes assistance in setting up and maintaining scan profiles and scheduling, project management of the customer's remediation efforts (regardless of whether they are handled by the customer's IT staff or 3rd party provider), and provides access to AT&T's staff of security analysts for additional information and guidance regarding more complex technical issues. In addition to the portal view, critical vulnerabilities that are identified are forwarded on a regular basis to the CLMS/ATLAS systems for correlation with other events within the network. Understand the vulnerabilities that exist, and the threats against these assets can be another critical element in the detection and prevention of a successful attack from either external or internal resources or devices.							
38	VSS –PRO Reconnaissance Network Appliance (RNA) Set UP - Desktop	VSSDRN	Desktop RNA Installation and Set Up		$1,800.00	$0.00	Per Enablement	$0.00	Yes	Required
39	VSS –PRO Reconnaissance Network Appliance (RNA) Set UP - Rackmount	VSSRRN	Rackmount RNA Installation and Set Up		$3,600.00	$0.00	Per Enablement	$0.00	Yes	Required
40	VSS-PRO – Quarterly Scanning 130	VSSQ130	Up to 130 devices		$0.00	$248.31	Per Enablement	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
41	VSS-PRO – Quarterly Scanning 250	VSSQ250	Up to 250 devices		$0.00	$335.94	Per Enablement	$0.00	Yes	Required
42	VSS-PRO – Quarterly Scanning 500	VSSQ500	Up to 500 devices		$0.00	$438.19	Per Enablement	$0.00	Yes	Required
43	VSS-PRO – Quarterly Scanning 1000	VSSQ1K	Up to 1000 devices		$0.00	$584.25	Per Enablement	$0.00	Yes	Required
44	VSS-PRO – Quarterly Scanning 2000	VSSQ2K	Up to 2000 devices		$0.00	$934.80	Per Enablement	$0.00	Yes	Required
45	VSS-PRO – Quarterly Scanning 3000	VSSQ3K	Up to 3000 devices		$0.00	$1,226.93	Per Enablement	$0.00	Yes	Required
46	VSS-PRO – Quarterly Scanning 3000+ per 1K incremental	VSSQ3KP	Each added 1K above 3K		$0.00	$262.91	Per Enablement	$0.00	Yes	Required
47	VSS-PRO – Monthly Scanning 130	VSSM130	Up to 130 devices		$0.00	$372.95	Per Enablement	$0.00	Yes	Required
48	VSS-PRO – Monthly Scanning 250	VSSM250	Up to 250 devices		$0.00	$504.40	Per Enablement	$0.00	Yes	Required
49	VSS-PRO – Monthly Scanning 500	VSSM500	Up to 500 devices		$0.00	$657.28	Per Enablement	$0.00	Yes	Required
50	VSS-PRO – Monthly Scanning 1000	VSSM1K	Up to 1000 devices		$0.00	$876.38	Per Enablement	$0.00	Yes	Required
51	VSS-PRO – Monthly Scanning 2000	VSSM2K	Up to 2000 devices		$0.00	$1,402.20	Per Enablement	$0.00	Yes	Required
52	VSS-PRO – Monthly Scanning 3000	VSSM3K	Up to 3000 devices		$0.00	$1,840.39	Per Enablement	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
53	VSS-PRO – Monthly Scanning 3000+ per 1K incremental	VSSM3KP	Each added 1K above 3K		$0.00	$394.37	Per Enablement	$0.00	Yes	Required
54	VSS-PRO – On Demand Scanning 130	VSSD130	Up to 130 devices		$0.00	$496.61	Per Enablement	$0.00	Yes	Required
55	VSS-PRO – On Demand Scanning 250	VSSD250	Up to 250 devices		$0.00	$671.89	Per Enablement	$0.00	Yes	Required
56	VSS-PRO – On Demand Scanning 500	VSSD500	Up to 500 devices		$0.00	$876.38	Per Enablement	$0.00	Yes	Required
57	VSS-PRO – On Demand Scanning 1000	VSSD1K	Up to 1000 devices		$0.00	$1,168.50	Per Enablement	$0.00	Yes	Required
58	VSS-PRO – On Demand Scanning 2000	VSSD2K	Up to 2000 devices		$0.00	$1,869.60	Per Enablement	$0.00	Yes	Required
59	VSS-PRO – On Demand Scanning 3000	VSSD3K	Up to 3000 devices		$0.00	$2,453.85	Per Enablement	$0.00	Yes	Required
60	VSS-PRO – On Demand Scanning 3000+	VSSD3KP	Each added 1K above 3K		$0.00	$525.83	Per Enablement	$0.00	Yes	Required
61	Network Security Consultant I	NSCLT1	Pre-implementation site survey and network security design. Provides basic consulting skills. Conducts assessments and design for non-complex installations. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Site Survey – Facility site survey required for successful design and implementation. Network Design – Design for Services supporting network security.	$0.00	$153.75	Per hour	$0.00	Yes	Required
62	Network Security Consultant II	NSCLT2	Pre-implementation site survey and network security design. Provides advanced consulting skills. Conducts assessments and design for complex installations. Only to be sold in conjunction with	Site Survey – Facility site survey required for successful design and implementation. Network Design – Design for Services	$0.00	$205.00	Per hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			the support of services specifically listed in Category 7.	supporting network security.						
63	Senior Network Security Consultant	SNSCLT	Pre-implementation site survey and network security design. Provides advanced consulting skills across multiple disciplines. Conducts assessments and design for complex installations involving multiple technologies. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Site Survey – Facility site survey required for successful design and implementation. Network Design – Design for services supporting network security.	$0.00	$256.25	Per hour	$0.00	Yes	Required
64	Principal Network Security Architect	PNSARHT	Pre-implementation site survey and network security design. Provides highly advanced consulting skills across multiple disciplines. Conducts assessments, design, and overall technical oversight for highly complex installations involving multiple technologies. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Site Survey – Facility site survey required for successful design and implementation. Network Design – Design for services supporting network security.	$0.00	$307.50	Per hour	$0.00	Yes	Required
65	Network Security Consultant I	NSCLT1N	Implementation network security consultant performs basic on-site installation and tests interoperability with other products. During normal business hours, Mon – Fri 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Implementation professional service combines a well-trained, well-equipped integration team with a highly skilled support organization to seamlessly install and integrate your new network. AT&T engineers perform installation and have extensive experience with numerous technologies, environments, and manufacturers' equipment. We test interoperability with other products.	$0.00	$153.75	Per hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
66	Network Security Consultant I	NSCLT1O	Implementation network security consultant performs basic on-site installation and tests interoperability with other products. During outside of normal business hours, Sat, Sun & Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Implementation professional service combines a well-trained, well-equipped integration team with a highly skilled support organization to seamlessly install and integrate your new network. AT&T engineers perform installation and have extensive experience with numerous technologies, environments, and manufacturers' equipment. We test interoperability with other products.	$0.00	$230.63	Per hour	$0.00	Yes	Required
67	Network Security Consultant II	NSCLT2N	Implementation network security consultant performs advanced on-site installation and tests interoperability with other products. During normal business hours, Mon – Fri, 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Implementation professional service combines a well-trained, well-equipped integration team with a highly skilled support organization to seamlessly install and integrate your new network. AT&T engineers perform installation and have extensive experience with numerous technologies, environments, and manufacturers' equipment. We test interoperability with other products.	$0.00	$205.00	Per hour	$0.00	Yes	Required
68	Network Security Consultant II	NSCLT2O	Implementation network security consultant performs advanced on-site installation and tests interoperability with other products. During outside of	Implementation professional service combines a well-trained, well-equipped integration team with a	$0.00	$307.50	Per hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			normal business hours, Sat, Sun & Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	highly skilled support organization to seamlessly install and integrate your new network. AT&T engineers perform installation and have extensive experience with numerous technologies, environments, and manufacturers' equipment. We test interoperability with other products.						
69	Network Security Project Manager	NSPMGRN	Network Security implementation project manager coordinates project resources including your staff and other internal AT&T resources. The project manager defines the project responsibility assignments for you. During normal business hours, Mon – Fri 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Project management for complex network security solutions. Project Management includes the statement of work, master schedule and site schedules, project acceptance criteria, and other key deliverables that support your overall plan. Project Management provides a project manager who coordinates project resources including your staff and other internal AT&T resources. Our project managers define the project responsibility assignments for you.	$0.00	$153.75	Per hour	$0.00	Yes	Required
70	Network Security Project Manager	NSPMGRO	Network Security implementation project manager coordinates project resources including your staff and other internal AT&T resources. The project manager defines the project responsibility assignments for you. During	Project management for complex network security solutions. Project Management includes the statement of work, master schedule and site	$0.00	$230.63	Per hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			outside of normal business hours, Sat, Sun and Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	schedules, project acceptance criteria, and other key deliverables that support your overall plan. Project Management provides a project manager who coordinates project resources including your staff and other internal AT&T resources. Our project managers define the project responsibility assignments for you.						
	Premises Based Firewall Service (PBFW) – (AT&T Owned and Managed Firewalls) Complete Service		The AT&T owned and managed Premises-Based Firewall Service – Complete Service provides a highly functional layer of security to your networks. The service is a fully managed bundled solution, which includes all hardware and software components, configuration, installation, day to day management and maintenance, as well as expert customer support and proactive network monitoring. The PBFW service can forward log information to the CLMS/ATLAS for advanced correlation within the network. With the ability to understand the communications as well as the ability to actively modify rules with customer approval based on attack information gathered from the CLMS/ATLAS system, AT&T can provide that additional level of protection and ability to not only report, but act on actionable events.						

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
	Cisco Configurations – Managed PBFW		Cisco Configurations - Managed PBFW							
71	Cisco Single Firewall for Large Office	PFSLC	Cisco Single Firewall for Large Office	AT&T Owned and Managed Cisco Single firewall for large office – 650 Mbps Firewall Throughput	$0.00	$1,420.65	Per Device	$0.00	Yes	Required
72	Cisco Single Firewall for Medium Office	PFSMC	Cisco Single Firewall for Medium Office	AT&T Owned and Managed Cisco Single firewall for Medium office – 450 Mbps Firewall Throughput	$0.00	$938.90	Per Device	$0.00	Yes	Required
73	Cisco Single Firewall for Small Office	PFSSC	Cisco Single Firewall for Small Office	AT&T Owned and Managed Cisco Single firewall for small office – 300 Mbps Firewall Throughput	$0.00	$435.63	Per Device	$0.00	Yes	Required
74	Cisco High Availability Firewall for Extra Large Office	PFELHAC	Cisco High Availability Firewall for Extra Large Office	AT&T Owned and Managed Cisco High Availability Firewall for Extra Large Office - 1.2 Gbps Firewall Throughput	$0.00	$4,891.30	Per Device	$0.00	Yes	Required
75	Cisco High Availability Firewall for Large Office	PFLHAC	Cisco High Availability Firewall for Large Office	AT&T Owned and Managed Cisco High Availability Firewall for Large Office – 650 Mbps Firewall Throughput	$0.00	$2,842.33	Per Device	$0.00	Yes	Required
76	Cisco High Availability Firewall for Medium Office	PFMHAC	Cisco High Availability Firewall for Medium Office	AT&T Owned and Managed Cisco High Availability Firewall for Medium Office – 450 Mbps Firewall Throughput	$0.00	$1,878.83	Per Device	$0.00	Yes	Required
	Fortigate Configurations – Managed PBFW		Fortigate Configurations - Managed PBFW							
77	Enterprise Office for Fortigate Single Firewall	PFEOS	Fortigate Single Firewall for Enterprise Office	Managed firewall service monthly recurring fee including single Fortigate CPE, all required licensing	$0.00	$6,840.44	Per Device	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				and full AT&T management – 10 Gbps Firewall Throughput.						
78	Fortigate Single Firewall for Extra Large Office	PFSELF	Fortigate Single Firewall for Extra Large Office	Managed firewall service monthly recurring fee including single Fortigate CPE, all required licensing and full AT&T management – 5 Gbps Firewall Throughput	$0.00	$3,060.65	Per Device	$0.00	Yes	Required
79	Fortigate Single Firewall for Large Office	PFSLF	Fortigate Single Firewall for Large Office	Managed firewall service monthly recurring fee including single Fortigate CPE, all required licensing and full AT&T management – 500 Mbps Firewall Throughput.	$0.00	$2,256.03	Per Device	$0.00	Yes	Required
80	Fortigate Single Firewall for Medium Office	PFSMF	Fortigate Single Firewall for Medium Office	Managed firewall service monthly recurring fee including single Fortigate CPE, all required licensing and full AT&T management – 100 Mbps Firewall Throughput.	$0.00	$1,329.43	Per Device	$0.00	Yes	Required
81	Fortigate Single Firewall Small Office	PFSSF	Fortigate Single Firewall for Small Office	Managed firewall service monthly recurring fee including single Fortigate CPE, all required licensing and full AT&T management – 10 Mbps Firewall Throughput.	$0.00	$681.63	Per Device	$0.00	Yes	Required
82	Fortigate Single Firewall for SOHO Office	PFSSHF	Fortigate Single Firewall for SOHO Office	Managed firewall service monthly recurring fee including single Fortigate CPE, all required licensing and full AT&T	$0.00	$548.38	Per Device	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				management – 5 Mbps Firewall Throughput.						
83	Enterprise Office for Fortigate High Availability Firewall	PFEOHAF	Fortigate High Availability Firewall for Enterprise Office	Managed firewall service monthly recurring fee including HA Fortigate CPE, all required licensing and full AT&T management – 10 Gbps Firewall Throughput.	$0.00	$9,435.43	Per Device	$0.00	Yes	Required
84	Fortigate High Availability Firewall for Extra Large Office	PFELHAF	Fortigate High Availability Firewall for Extra Large Office	Managed firewall service monthly recurring fee including HA Fortigate CPE, all required licensing and full AT&T management – 5 Gbps Firewall Throughput.	$0.00	$5,259.58	Per Device	$0.00	Yes	Required
85	Fortigate High Availability Firewall for Large Office	PFLHAF	Fortigate High Availability Firewall for Large Office	Managed firewall service monthly recurring fee including HA Fortigate CPE, all required licensing and full AT&T management – 500 Mbps Firewall Throughput.	$0.00	$3,847.75	Per Device	$0.00	Yes	Required
86	Fortigate High Availability Firewall for Medium Office	PFMOHAF	Fortigate High Availability Firewall for Medium Office	Managed firewall service monthly recurring fee including HA Fortigate CPE, all required licensing and full AT&T management – 100 Mbps Firewall Throughput.	$0.00	$2,455.80	Per Device	$0.00	Yes	Required
86a.	AT&T Remote Access 5 Tokens	FTM5	FortiTokenMobile access password tokens for iOS, - qty 5	Only to be provisioned in conjunction with AT&T Managed Fortinet Firewall solutions	$0.00	$256.25	Each	$0.00	Yes	Discretionary
86b.	AT&T Remote Access 20 Tokens	FTM20	FortiTokenMobile access password tokens for iOS, - qty 20	Only to be provisioned in conjunction with AT&T Managed Fortinet Firewall solutions	$0.00	$512.50	Each	$0.00	Yes	Discretionary

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
86c.	AT&T Remote Access 100 Tokens	FTM10	FortiTokenMobile access password tokens for iOS, - qty 100	Only to be provisioned in conjunction with AT&T Managed Fortinet Firewall solutions	$0.00	$820.00	Each	$0.00	Yes	Discretionary
86d.	AT&T Remote Access 1200 Tokens	FTM12	FortiTokenMobile access password tokens for iOS, - qty 1200	Only to be provisioned in conjunction with AT&T Managed Fortinet Firewall solutions	$0.00	$2870.00	Each	$0.00	Yes	Discretionary
86e.	AT&T Remote Clients	FTC25	FortiClient Security Fabric Agent for 25 Clients Security Fabric Agent with EPP subscription for 25 endpoints. Includes Fabric Agent, Anti- Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent (On-Prem), Central Management and 24x7 Support.	Only to be provisioned in conjunction with AT&T Managed Fortinet Firewall solutions	$0.00	$256.25	Each	$0.00	Yes	Discretionary
86f.	AT&T Remote Clients MRC Option	FTC12	FortiClient Security Fabric Agent for 1200 Clients Security Fabric Agent with EPP subscription for 1200 endpoints. Includes Fabric Agent, Anti- Malware, Remote Access, Web Filter, Vulnerability Scan, Software Inventory, Application Firewall, SSOMA, Threat Outbreak Detection, Sandbox Agent (On-Prem), Central Management and 24x7 Support.	Only to be provisioned in conjunction with AT&T Managed Fortinet Firewall solutions	$0.00	$1025.00	Each	$0.00	Yes	Discretionary
	Firewall Optional Add-On Features									
87	IPS Add-On – MIDS 3	OPTIPSF	IPS Add-On provides the customer with intrusion protection capability to the firewall. Includes the following: • 7x24 monitoring • CPE Managed Option (customized to equipment • Signature updates		$0.00	$666.25	Each	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			• Vendor updates (3-5 business days) • Emergency updates (24 hours) • Incident Notification (Email for medium alerts within; High includes a telephone call) • Sensor Configuration: o Custom Tuning o Continuous Sensor Tuning o Custom Signatures (20) • Sensor Location: o Alarm Analysis o Event Correlation & Analysis with additional real time analyst support o Root cause analysis for high level alerts o Investigation support o Customer notification based on SLO o Attack signature recognition o Problem ticketing/Reporting o Initial configuration support Configuration maintenance							
88	URL Filtering Add-On	OPTURLF	URL Filtering Add-On provides the customer with basic URL filtering capability. Enables enterprises to build their own Web access policies by selectively blocking access to sites. Enables the customer to allow domain name control within the firewall to block specific sites.		$0.00	$143.50	Each	$0.00	Yes	Required
89	Anti-virus Add-On	OPTAVF	Anti-virus Add-On additional feature which will look for known malicious software and protect against threats.		$0.00	$117.88	Each	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
90	IPSEC (VPN) Add-On	OPTVPN	IPSEC (VPN) Add-On allows remote VPN user access to applications behind the firewall.		$0.00	$107.63	Each	$0.00	Yes	Required
91	Additional Port Add-On (DMZ) (2+, First Port is included)	OPTPORT	Additional Port Add-On (DMZ) (2+, First Port is included) to allow additional DMZ to segment the local area network into additional segments.		$0.00	$430.50	Each	$0.00	Yes	Required
	Premises Based Firewall Service (PBFW) Customer Owned and AT&T Managed – Complete Service		The customer owned and AT&T managed Premises-Based Firewall Service – Complete Service provides a highly functional layer of security to your networks. The service is a fully managed solution, which includes day to day management and maintenance, as well as expert customer support and proactive network monitoring. The PBFW service can forward log information to the CLMS/ATLAS for advanced correlation within the network. With the ability to understand the communications as well as the ability to actively modify rules with customer approval based on attack information gathered from the CLMS/ATLAS system, AT&T can provide that additional level of protection and ability to not only report, but act on actionable events.							
92	Installation for Firewall Administration	PFCINST	Installation for Firewall Administration		$500.00	$0.00	Per Network	$0.00	Yes	Required
93	Firewall Administration 1 to 4 firewalls	PFCA4	Firewall Administration 1 to 4 firewalls	Management Kit required.	$0.00	$794.38	Per Device	$0.00	Yes	Required
94	Firewall Administration 5 to 9 firewalls	PFCA9	Firewall Administration 5 to 9 firewalls	Management Kit required.	$0.00	$754.24	Per Device	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
95	Firewall Administration 10 to 19 firewalls	PFCA19	Firewall Administration 10 to 19 firewalls	Management Kit required.	$0.00	$709.86	Per Device	$0.00	Yes	Required
96	Firewall Administration 20 to 29 firewalls	PFCA29	Firewall Administration 20 to 29 firewalls	Management Kit required.	$0.00	$665.50	Per Device	$0.00	Yes	Required
97	Firewall Administration 30 to 44 firewalls	PFCA44	Firewall Administration 30 to 44 firewalls	Management Kit required.	$0.00	$621.13	Per Device	$0.00	Yes	Required
98	Firewall Administration 45 or greater firewalls	PFCA45	Firewall Administration 45 or greater firewalls	Management Kit required.	$0.00	$612.26	Per Device	$0.00	Yes	Required
99	Management Kit	PFCMK	Management Kit supports 4 Port out of band management including power and console connections for previse based managed solutions. Requires customer provided Measured Business Line or equivalent.		$2,500.00	$0.00	Per Kit	$0.00	Yes	Required
	Managed Intrusion Detection Service - MIDS 3 (Customer owned and AT&T managed equipment)		AT&T Managed Intrusion Detection Service provides security monitoring capabilities to include security audit, monitoring, attack recognition, control over employee Internet access, virus scanning, and incident response for customer owned equipment. AT&T Certified IPS Sensors is provided based on the number of zones monitored. The qualifications for multi-sensor/zone discounts: • Counts are based on a per-department/organization order • Minimum of two monitored zones per location with Internet access point • Additional monitored IDS zones on same							

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			network count towards volume discount • Must include an AT&T management kit at the Internet access location. • Configuration may require separate security management demilitarized zone (DMZ) off the customer firewall. The AT&T MIDS solution integrates into the CLMS/ATLAS to provide enhanced visibility into network segments protected by IPS/IDS capabilities. Alarms/alerts and log information from these IPS/IDS devices are correlated into the advanced analytics within CLMS/ATLAS to allow these factors discovered by the MIDS systems to aid in the detection of hacker activity within a network.							
100	Setup for IPS	MICINST	Setup for IPS	Installation charge for IPS Service. MIDS Level 3 sensor placement must be behind a screening device (i.e., Firewall, screening router, etc.).	$1,000.00	$0.00	Per Network	$0.00	Yes	Required
101	IPS 1 to 59 zones	MIC59	IPS 1 to 59 zones	Management Kit required.	$0.00	$1,020.72	Each	$0.00	Yes	Required
102	IPS 60 to 89 zones	MIC89	IPS 60 to 89 zones	Management Kit required.	$0.00	$956.92	Each	$0.00	Yes	Required
103	IPS – 90 to 134 zones	MIC134	IPS – 90 to 134 zones	Management Kit required.	$0.00	$893.12	Each	$0.00	Yes	Required
104	IPS - 135 to 179 zones	MIC179	IPS - 135 to 179 zones	Management Kit required.	$0.00	$880.36	Each	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
105	IPS 180 or greater zones	MIC180	IPS 180 or greater zones	Management Kit required.	$0.00	$871.14	Each	$0.00	Yes	Required
	Managed Network Access Control Service (NAC)		Managed Network Access Control Service (NAC) utilizes AT&T's expertise in endpoint security to analyze information about how endpoints impact the security posture of the network. Base service includes Hardware Other capabilities include: •Rogue Device Detection – Detects and alerts when unknown devices attempt to connect to a network (wired or wireless) •Advanced Asset Visibility – Identifies & classifies all devices with an IP address connecting to the network, by device & location on the network. Supports wired, wireless and VPN networks •Endpoint Compliance Identification – Remote inspection of Windows, Mac and Linux operating systems for compliance. Identify missing patches, out of date AV, required services not running, etc. Infractions can be reported on •Unauthorized Application Notification – Remote inspection of the endpoint will inventory the applications installed and notify on unauthorized applications •Misconfigured Asset Detection – Assets that have been misconfigured can be identified. •IoT Device Detection – identify IoT devices on the network and ensure they are properly segmented to prevent the threat of botnets attacking the internal network or being used as a threat to other organizations	The Customer is required to provide the following: •Internet Connection •Network documentation & flow diagrams, including topology, data flow, network switches, IP device assignment categories •Inbound & Outbound remote access via SSH to at least one sensor at each location •3 network ports on the core network switch for NAC sensors •A compatible managed switch and available ports •Internal management IP address for each sensor •Internal IP address for each network segment (or VLAN) •Customer is responsible for the configuration of a FQDN on the network domain for name resolution of the IP address assigned to the sensor for captive portal redirection •Physical installation and cabling of the sensor and other equipment included in service						

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			•System Patching & Security Updates – Support, management, maintenance of management server and sensors •System Health monitoring for all NAC solution components •Technical Support – phone & remote-based support 24x7 •Real-time monitoring and alerting of NAC events 24x7 with response and notification to customer actionable events •Correlation NAC events in association with customer log event sources if provided by customer for analysis (Note: Requires ATLAS coverage for other supported log sources) •Customer Web Portal – for reports, support tickets, log analyzer, log charts, security dashboard & web portal with alert data, event drill downs, graphs, etc. NAC Reporting – On Rogue Device Detection and additional use cases the customer purchases.	•Active participation as requested for review of network devices. May include confirmation and/or guidance regarding device categories of both known and unknown devices •If available, an OOB (Out of Band) method such as a IP KVM or Serial connection be connected to any sensor installed •Compatible managed switch, including switch documentation •Customer Project Manager/Coordinator and a Technical Resource to provide coordination of schedules and resources required for installation and configuration.						
106	Managed Network Access Control Service (NAC) – Tier 1	NACSV1	Managed Network Access Control Service (NAC) – Tier 1 (Small) -Advanced Visibility of Assets -Identify Compliancy of Endpoints -Unauthorized/Authorized Applications Notification -Misconfigured Asset Detection -IoT Device Detection	NAC is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at any time per incremental costs. Tier 1 is an initial enablement of up to 500 devices and/or 150 users per site. If customer users and devices fall into two tier levels, the higher tier	$6,000.00	$2,240.35	Per Site	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				will apply. May require agent or WMI connectivity for some features.						
107	Managed Network Access Control Service (NAC) – Tier 2	NACSV2	Managed Network Access Control Service (NAC) – Tier 2 (Medium) -Advanced Visibility of Assets -Identify Compliancy of Endpoints -Unauthorized/Authorized Applications Notification -Misconfigured Asset Detection -IoT Device Detection	NAC is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at any time per incremental costs. Tier 2 is an initial enablement of 501 to 1,000 devices and/or 151-350 users per site. If customer users and devices fall into two tier levels, the higher tier will apply. May require agent or WMI connectivity for some features.	$7,333.33	$4,201.98	Per Site	$0.00	Yes	Required
108	Managed Network Access Control Service (NAC) – Tier 3	NACSV3	Managed Network Access Control Service (NAC) – Tier 3 (Large) -Advanced Visibility of Assets -Identify Compliancy of Endpoints -Unauthorized/Authorized Applications Notification -Misconfigured Asset Detection -IoT Device Detection	NAC is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at any time per incremental costs. Tier 3 is an initial enablement of 1,001 to 2,500 devices and/or 351-850 users per site. If customer users and devices fall into two tier levels, the higher tier will apply. May require	$9,066.67	$7,159.08	Per Site	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				agent or WMI connectivity for some features						
109	Managed Network Access Control Service (NAC) – Tier 4	NACSV4	Managed Network Access Control Service (NAC) – Tier 4 (Extra Large) -Advanced Visibility of Assets -Identify Compliancy of Endpoints -Unauthorized/Authorized Applications Notification -Misconfigured Asset Detection -IoT Device Detection	NAC is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at any time per incremental costs. Tier 4 is an initial enablement of 2,501 to 4,000 devices and/or 851-1,500 users per site. If customer users and devices fall into two tier levels, the higher tier will apply. May require agent or WMI connectivity for some features, May require agent or WMI connectivity for some features	$10,666.67	$10,520.24	Per Site	$0.00	Yes	Required
110	Managed Network Access Control Service (NAC) – Tier 5	NACSV5	Managed Network Access Control Service (NAC) – Tier 5 (Enterprise) -Advanced Visibility of Assets -Identify Compliancy of Endpoints -Unauthorized/Authorized Applications Notification -Misconfigured Asset Detection -IoT Device Detection	NAC is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at any time per incremental costs. Tier 5 is an initial enablement of 4,001-10,000 devices and/or 1,501-3,500 users per site. If customer users and devices fall into	$13,333.33	$20,298.64	Per Site	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				two tier levels, the higher tier will apply. May require agent or WMI connectivity for some features						
	Managed Network Access Control Service (NAC) – Additional Features		Managed Network Access Control Service (NAC) – Additional Features							
111	Managed Network Access Control Service (NAC) – Tier 1 Advanced NAC Use Case	NSV1AUC	Managed Network Access Control Service (NAC) – Tier 1 Advanced NAC Use Case - Flexible Access Control by User, Device or Policy - Remediation of Out of Compliance Endpoints - Unauthorized Application Prevention - Rogue Device Prevention	Tier 1 Advanced NAC Use Case – Customer-requested use cases are defined as specific functionality requirements defined for NAC Service. These use cases are ranked into one of two categories: Basic and Advanced. A list of advanced use cases can be provided. Some features may require: CLI access to layer 2 or 3 switch so ACL's can be applied. Enforcement to be enabled, AD integration, and WMI integration or agent. Agent or WMI connectivity	$4,184.00	$769.44	Per Site	$0.00	Yes	Required
112	Managed Network Access Control Service (NAC) – Tier 2 Advanced NAC Use Case	NSV2AUC	Managed Network Access Control Service (NAC) – Tier 2 Advanced NAC Use Case - Flexible Access Control by User, Device or Policy - Remediation of Out of Compliance Endpoints - Unauthorized Application Prevention - Rogue Device Prevention	Tier 2 Advanced NAC Use Case – Customer-requested use cases are defined as specific functionality requirements defined for NAC Service. These use cases are ranked into one of two categories: Basic and Advanced. A list of advanced use cases	$5,666.67	$1,025.00	Per Site	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				can be provided. Some features may require: CLI access to layer 2 or 3 switch so ACL's can be applied. Enforcement to be enabled, AD integration, and WMI integration or agent. Agent or WMI connectivity						
113	Managed Network Access Control Service (NAC) – Tier 3 Advanced NAC Use Case	NSV3AUC	Managed Network Access Control Service (NAC) – Tier 3 Advanced NAC Use Case - Flexible Access Control by User, Device or Policy - Remediation of Out of Compliance Endpoints - Unauthorized Application Prevention - Rogue Device Prevention	Tier 3 Advanced NAC Use Case – Customer-requested use cases are defined as specific functionality requirements defined for NAC Service. These use cases are ranked into one of two categories: Basic and Advanced. A list of advanced use cases can be provided. Some features may require: CLI access to layer 2 or 3 switch so ACL's can be applied. Enforcement to be enabled, AD integration, and WMI integration or agent. Agent or WMI connectivity	$7,226.67	$1,537.50	Per Site	$0.00	Yes	Required
114	Managed Network Access Control Service (NAC) – Tier 4 Advanced NAC Use Case	NSV4AUC	Managed Network Access Control Service (NAC) – Tier 4 Advanced NAC Use Case - Flexible Access Control by User, Device or Policy - Remediation of Out of Compliance Endpoints - Unauthorized Application Prevention - Rogue Device Prevention	Tier 4 Advanced NAC Use Case – Customer-requested use cases are defined as specific functionality requirements defined for NAC Service. These use cases are ranked into one of two categories: Basic and Advanced. A list of	$9,781.33	$2,391.66	Per Site	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				advanced use cases can be provided. Some features may require: CLI access to layer 2 or 3 switch so ACL's can be applied. Enforcement to be enabled, AD integration, and WMI integration or agent. Agent or WMI connectivity						
115	Managed Network Access Control Service (NAC) – Tier 5 Advanced NAC Use Case	NSV5AUC	Managed Network Access Control Service (NAC) – Tier 5 Advanced NAC Use Case - Flexible Access Control by User, Device or Policy - Remediation of Out of Compliance Endpoints - Unauthorized Application Prevention - Rogue Device Prevention	Tier 5 Advanced NAC Use Case – Customer-requested use cases are defined as specific functionality requirements defined for NAC Service. These use cases are ranked into one of two categories: Basic and Advanced. A list of advanced use cases can be provided. Some features may require: CLI access to layer 2 or 3 switch so ACL's can be applied. Enforcement to be enabled, AD integration, and WMI integration or agent. Agent or WMI connectivity	$13,166.67	$3,075.00	Per Site	$0.00	Yes	Required
116	Managed Network Access Control Service (NAC) – Tier 1 Dedicated Management Server	NSV1DMS	Managed Network Access Control Service (NAC) – Tier 1 Dedicated Management Server (DMS)	Allows for management of multiple NAC devices in a Customer's environment. Required for configurations with more than 2 sensors. Pricing includes service, and hardware. A Tier 1 DMS can	$0.00	$1,494.64	Per Site	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				support up to 5 appliances/sensors.						
117	Managed Network Access Control Service (NAC) – Tier 2 Dedicated Management Server	NSV2DMS	Managed Network Access Control Service (NAC) – Tier 2 Dedicated Management Server (DMS)	Allows for management of multiple NAC devices in a Customer's environment. Required for configurations with more than 5 sensors. Pricing includes service, and hardware. A Tier 2 DMS can support 6-10 appliances/sensors.	$0.00	$1,869.26	Per Site	$0.00	Yes	Required
118	Managed Network Access Control Service (NAC) – Tier 3 Dedicated Management Server	NSV3DMS	Managed Network Access Control Service (NAC) – Tier 3 Dedicated Management Server (DMS)	Allows for management of multiple NAC devices in a Customer's environment. Required for configurations with more than 10 sensors. Pricing includes service, and hardware. A Tier 3 DMS can support 11-25 appliances/sensors.	$0.00	$2,243.88	Per Site	$0.00	Yes	Required
119	Managed Network Access Control Service (NAC) – Tier 4 Dedicated Management Server	NSV4DMS	Managed Network Access Control Service (NAC) – Tier 4 Dedicated Management Server (DMS)	Allows for management of multiple NAC devices in a Customer's environment. Required for configurations with more than 25 sensors. Pricing includes service, and hardware. A Tier 4 DMS can support 26-50 appliances/sensors.	$0.00	$2,494.98	Per Site	$0.00	Yes	Required
120	Managed Network Access Control Service (NAC) – Tier 5 Dedicated Management Server	NSV5DMS	Managed Network Access Control Service (NAC) – Tier 5 Dedicated Management Server (DMS)	Allows for management of multiple NAC devices in a Customer's environment. Required for configurations with	$0.00	$4,432.17	Per Site	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				more than 50 sensors. Pricing includes service, and hardware. A Tier 5 DMS can support 51-100 appliances/sensors.						
121	Managed Network Access Control Service (NAC) – Tier 1 Co-Management	NSV1CM	Managed Network Access Control Service (NAC) – Tier 1 Co-Management	End-user NAC console access for end point MAC/IP management by designated IT staff (Note: requires training & dedicated management server). Required.	$0.00	$546.66	Per Site	$0.00	Yes	Required
122	Managed Network Access Control Service (NAC) – Tier 2 Co-Management	NSV2CM	Managed Network Access Control Service (NAC) – Tier 2 Co-Management	End-user NAC console access for end point MAC/IP management by designated IT staff (Note: requires training & dedicated management server). Required.	$0.00	$546.66	Per Site	$0.00	Yes	Required
123	Managed Network Access Control Service (NAC) – Tier 3 Co-Management	NSV3CM	Managed Network Access Control Service (NAC) – Tier 3 Co-Management	End-user NAC console access for end point MAC/IP management by designated IT staff (Note: requires training & dedicated management server). Required.	$0.00	$546.66	Per Site	$0.00	Yes	Required
124	Managed Network Access Control Service (NAC) – Tier 4 Co-Management	NSV4CM	Managed Network Access Control Service (NAC) – Tier 4 Co-Management	End-user NAC console access for end point MAC/IP management by designated IT staff (Note: requires training & dedicated management server). Required.	$0.00	$546.66	Per Site	$0.00	Yes	Required
125	Managed Network Access Control Service (NAC) – Tier 5 Co-Management	NSV5CM	Managed Network Access Control Service (NAC) – Tier 5 Co-Management	End-user NAC console access for end point MAC/IP management by designated IT staff (Note: requires training & dedicated	$0.00	$546.66	Per Site	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
				management server). Required.						
126	Managed Network Access Control Service (NAC) – Collector	NACSVC	Managed Network Access Control Service (NAC) – Collector	Log Collector placed at the Customer Site which collects and aggregates the log data from the Customer's device logs generated by its network and systems.	$0.00	$273.34	Per Site	$0.00	Yes	Required
	AT&T Security Network Device Management – Riverbed		AT&T managed security for devices is provided effectively across multiple product categories and create a process/methodology to include valuable flow and security analytics in the CLMS platform for enhanced correlation and analysis. Customers receive application performance analysis, capacity audits, issue root-cause determinations, and receive recommendations for increasing network and application performance. This is for customer owned devices. This service includes: Initial basic set-up and policy development 24x7x365 Monitoring of applications Monthly analysis of mission-critical application performance Quarterly tuning of policy and performance settings Hardware support for both custom and off-the-shelf applications Forwarding of critical alerts to CLMS platform for security correlation and analysis Post Implementation Network Management - Network monitoring service with carrier and	The Customer is required to provide the following: -Internet Connection -MIB-II compliant hardware required -Inbound & Outbound remote access via SSH to at least one device at each location -Internal management IP address for each device						

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			vendor coordination for CPE supporting WAN access AT&T Network Management is a set of support solutions that provides you a single-point-of-contact to outsource or back-up some or all of the State's network support functions. You can use AT&T Network Management Services as a supplementary and disaster-recovery organization. We can assist the State to manage, monitor, and assume responsibility for your network on an as-needed basis. This will ensure that your network is reliable, available, efficient, and successfully performs your critical operations. AT&T provides a one-stop shop. We are able to manage most pieces of your network, including SNMP-MIB II-compliant devices. This means we can manage routers, CSU/DSUs, LAN switches, LAN hubs, etc. You do not have to work only with equipment we supply. If you have equipment supplied by other vendors, we can coordinate with them to make sure that your AT&T Network Management solution supports their CPE. AT&T Network Management is also flexible. We can mold your solution to fit the State environment from very hands-on, requiring detailed reporting to hands-off where the State only engages AT&T on an as-needed basis. We can monitor your CPE (e.g., routers, hubs, switches, CSU/DSUs, call managers) remotely from our AT&T Data Services Customer Care. You can								

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
			choose from three levels of service to ensure the right fit with your staff and budget needs: Basic, Essential, and Complete. We will monitor supported devices over a customer-provided permanent virtual circuit ("PVC") or virtual private network ("VPN"). A customer premise router (e.g., Cisco 1800 with VPN) may also be required for AT&T to deliver this service.							
127	Basic level Category A	DMRBBA	Basic level Category A With our Basic level service, you receive network monitoring, event detection, and subsequent notification and correlation with the CLMS/ATLAS team. You may use your internal staff for event and fault management and remediation support. AT&T's Network Management support team will alert you about the detected faults and it is your responsibility to contact your vendor directly for maintenance.	Basic Service is suited for you if your need is to supplement your existing network monitoring capabilities or off-hours support (or both). Basic service is available on any AT&T Approved SNMP MIB II-compliant device. Category A Devices Router Switch Centralized WLAN - Management/Sec. Switch Firewall (BASIC only)	$105.00	$71.75	Per Device	$0.00	Yes	Required
128	Basic level Category B	DMRBBB	Basic level Category B With our Basic level service, you receive network monitoring, event detection, and subsequent notification and correlation with the CLMS/ATLAS team. You may use your internal staff for event and fault management and remediation support. AT&T's Network Management support team will alert you about the detected faults and it is your responsibility to contact your vendor directly for maintenance.	Basic Service is suited for you if your need is to supplement your existing network monitoring capabilities or off-hours support (or both). Basic service is available on any AT&T Approved SNMP MIB II-compliant device. Category B Devices Centralized WLAN: "Thin" Access Points	$40.00	$27.34	Per Device	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
129	Essential Level Category A	DMRBEA	Essential Level Category A Our Essential Service provides you with comprehensive, end-to-end fault management. In addition to fault management, the service includes network monitoring, technical assistance (with carrier and vendor coordination), configuration support, software support, and the ability to open or view web-based trouble tickets as well as correlation with the CLMS/ATLAS team on events.	If you elect Essential Service, AT&T becomes your single-point-of-contact for network problems. When we diagnose a problem with your equipment, our Network Management Service support team manages the vendor to coordinate your dispatch. Work with the vendor may include opening trouble tickets and escalating to resolve the problem quickly. Throughout this process, our engineer takes total responsibility for ensuring that the problem is resolved. The AT&T NOC will update you as appropriate and will not close the trouble ticket until the problem is resolved to your satisfaction. Carrier and Vendor coordination requires that a valid Letter of Agency (LOA) be on file with AT&T Network Device Management support team. Available on any AT&T Approved SNMP MIB II-compliant device. Category A Devices Router Switch Centralized WLAN: management/security switch	$150.00	$102.50	Per Device	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
130	Essential Level Category B	DMRBEB	Essential Level Category B Our Essential Service provides you with comprehensive, end-to-end fault management. In addition to fault management, the service includes network monitoring, technical assistance (with carrier and vendor coordination), configuration support, software support, and the ability to open or view web-based trouble tickets as well as correlation with the CLMS/ATLAS team on events.	If you elect Essential Service, AT&T becomes your single-point-of-contact for network problems. When we diagnose a problem with your equipment, our Network Management Service support team manages the vendor to coordinate your dispatch. Work with the vendor may include opening trouble tickets and escalating to resolve the problem quickly. Throughout this process, our engineer takes total responsibility for ensuring that the problem is resolved. The AT&T NOC will update you as appropriate and will not close the trouble ticket until the problem is resolved to your satisfaction. Carrier and Vendor coordination requires that a valid Letter of Agency (LOA) be on file with AT&T Network Device Management support team. Available on any AT&T Approved SNMP MIB II-compliant device. Category B Devices Centralized WLAN: "Thin" Access Points CSU/DSU (w/ Router)	$60.00	$41.00	Per Device	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of Measure	Charge per change per item	Delegation Needed (Yes/No)	Required/ Discretionary
131	Complete Level Category A	DMRBCA	Complete Level Category A The Complete option provides performance management support in addition to all the services you receive with our Essential service offering.	Through performance management, we can measure and report on your network performance to keep internetworking performance at an optimal level. Our Complete Network Management offering includes web-based performance reporting on network elements and supported CPE and monthly performance reviews through an assigned engineer. Available on any AT&T Approved SNMP MIB II-compliant device. Category A Devices Router Switch Centralized WLAN: management/security switch	$200.00	$136.66	Per Device	$0.00	Yes	Required