Table of Contents

LevelBlue Secure Workforce with Check Point

This Service Guide consists of the following parts:

- Service Description (SD)
- Service Level Objectives (SLO)
- Pricing (P)
- Country Specific Provisions (CSP)

In addition, the LevelBlue Acceptable Use Policy and the General Provisions are incorporated and apply as specified therein.

Service Description (SD)

SD-1. Overview

Section Effective Date: 18-May-2023

LevelBlue Secure Workforce with Check Point (the "Service") is a suite of fully managed cloud-delivered security solution providing protection for a Customer's Internet, web traffic, email, browser, and office solutions.

SD-2. Features of LevelBlue Secure Workforce with Check Point

The Service is made up of four different security features including:

- Secure Web Gateway (SWG)
- Secure Remote Access (SRA)
- Email
- Browse

SD-2.1. Secure Web Gateway (SWG)

This technology includes secure internet access, Next-Generation Firewall, application control, DLP, IPS, anti-virus, anti-bot, and threat emulation via zero day and ransomware protection.

SD-2.2. Secure Remote Access (SRA)

This technology provides users with a remote access platform based on Zero Trust Access principles that enable application and network level access to most enterprise resources. The SRA functionality authenticates a user's identity and authorizes access using defined permissions and contextual data such as device, location, and MFA, prior to granting user access to any asset.

SD-2.3. Email

This technology detects and blocks phishing attacks across inbound, outbound, and internal communications. Only O365 or Gmail supported at this time.

SD-2.4. Browse

This technology delivers web security from a Nano Agent® within a browser, inspecting all SSL traffic on the endpoint and preventing malicious behaviors.

SD-3. Secure Workforce with Check Point Packages

LevelBlue Secure Workforce with Check Point offers packages that combine features, or the features may be purchased on a stand-alone basis. These packages are sold at seat levels ranging from 5-25,000+

LevelBlue Secure Workforce with Check Point		
Package	**Included Features**	**Deployment Tier***
Stand-Alone		
LevelBlue Secure Web Gateway with Check Point	SWG	Tier 2 Tier 3 (seat levels above 5000)
LevelBlue Email Security with Check Point	Email Security (with Office and collaboration tools)	Tier 2 Tier 3 (seat levels above 5000)
LevelBlue Secure Remote Access	SRA	Tier 2 Tier 3 (seat levels above 5000)
Small Market		
LevelBlue Secure Workforce with Check Point – Browse and Email	Browser + Email Security (with Office and collaboration tools)	Tier 1
LevelBlue Secure Workforce with Check Point – Web and Email	SWG + Email Security (with Office and collaboration tools)	Tier 2
LevelBlue Secure Workforce with Check Point – Browse, Web, and Email	Browser + SWG + Email Security (with Office and collaboration tools)	Tier 2
Enterprise Bundles		
LevelBlue Secure Workforce with Check Point – Web and Email	SWG + Email Security (with Office and collaboration tools)	Tier 3
LevelBlue Secure Workforce with Check Point – Remote Access and Web	SRA + SWG	Tier 3
LevelBlue Secure Workforce with Check Point – Remote Access, Web, and Email	SRA + SWG + Email Security (with Office and collaboration tools)	Tier 3

LevelBlue Secure Workforce with Check Point		
Package	**Included Features**	**Deployment Tier***
LevelBlue Secure Workforce with Check Point – Browser, Remote Access, Web, and Email	Browser + SRA + SWG + Email Security (with Office and email collaboration tools)	Tier 3

*A non-recurring fee will be charged for deployment of the Service. Tiers are assigned to each package to indicate the level of engineering support needed to deploy the service. Higher seat levels require additional engineering support.

SD-4. Implementation

AT&T's structured process for implementation includes developing and gathering documentation and credentials, establishing a baseline of deliverables, timelines, and responsibilities, and verifying performance prior to LevelBlue assuming management of steady-state operations.

SD-4.1. Implementation Resources

SD-4.1.1. Security Implementation Management (SIM)

LevelBlue will assign a Cybersecurity Security Implementation Manager (SIM) to facilitate the LevelBlue Secure Workforce with Check Point deployment. This resource is designated to the Customer order and will set up a kickoff call to discuss the Customer's LevelBlue Secure Workforce with Check Point. The SIM is responsible to deliver the overall solution to see to it that the Customer is supported end-to-end, from post sales through service activation.

SD-4.1.2. Service Activation

LevelBlue will activate the Service for the Customer ("Service Activation"). Service Activation is complete when:

- The license has been provisioned with the ordered service
- The Service is successfully tested by the SIM

Billing will begin upon Service Activation of the license.

SD-4.1.3. Technical Implementation

SD-4.1.3.1. Customer Policy Implementation

LevelBlue will apply the Customer's security policies to the LevelBlue Secure Workforce with Check Point Service based on the Customer completed online technical provisioning document.

The SIM will validate the online technical provisioning document with the Customer to provide that all information is sufficient and accurate based on Customer's requests.

SD-5. Support and Management

The following describes the support and management capabilities included in LevelBlue Secure Workforce with Check Point.

SD-5.1. Help Desk Support

All issues, questions or requests for assistance related to LevelBlue Secure Workforce with Check Point can be made to the Managed Security Services (MSS). A trouble ticket will be opened for each incident. The trouble ticket begins when LevelBlue has acknowledged and validated a problem that is a result of the Customer's Service, and when an LevelBlue generated ticket is opened. A trouble ticket is deemed "Resolved" when the Incident has been addressed and the Service is restored, at which time the trouble ticket is closed.

SD-5.2. Infrastructure Management

LevelBlue will provide management of the LevelBlue Secure Workforce with Check Point environment, including maintaining availability of all tenants in the LevelBlue Secure Workforce with Check Point Service.

SD-5.3. LevelBlue Managed Policy

LevelBlue will provide policy management for the Service. Customer will log into to LevelBlue Business Center to request policy changes.

SD-5.3.1. Content Security Policy and Configuration Changes

- Following activation of the Service, Customer will be sent references on how to use the LevelBlue Change Management Portal to submit security policy changes.
- When using the Service, Customer designs and sets all filtering and interception policies (Security Policies). LevelBlue undertakes only to implement the Security Policies as directed by Customer and accepts no responsibility for the design or appropriateness of such design or settings.
- All changes to the Security Policies must be provided by the Security Liaison identified by Customer to be the point of contact to work with LevelBlue to notify and assist with problem resolution regarding the Customer environment.
- Customer will follow the LevelBlue change management process outlined in the Customer Expectation Document (CED) sent via email at the beginning of the Service. This includes the use of the LevelBlue MSS Change Management System to request policy changes.
- If changes to Customer’s Security Policy(s) are necessary, Customer will provide LevelBlue with minimum data set for policy change.

SD-5.4. Special Projects

Special Projects are professional services requests not specified in this Service Guide or Customer's Service Agreement. Special Projects will require further assessment, and additional charges will be applied to projects and will be negotiated between LevelBlue and Customer.

SD-6. Customer Responsibilities

SD-6.1. Customer Responsibilities for Service Delivery and Use

Prior to Service Activation, Customer shall:

- Participate in predelivery configuration and architectural reviews.
- Supply LevelBlue with all technical data and any additional information required for LevelBlue to activate the Service.
- Backup configuration information prior to Service Activation.
- Manage installation of the Service and related software on all end user laptops and mobile devices, and configure Customer applications, if needed.
- Provide equipment and application logs and network traces, if required, for troubleshooting and testing of installations.
- Review and provide relevant comments (in the form of additional data requirements, preliminary conclusions, or recommended technical architecture) or subject matter expert resources from applicable information technology departments or business units to assist in completing LevelBlue deliverables in a timely manner.

During use of the Service, Customer shall:

Undertake all necessary steps to keep confidential and not reveal or disclose to any third party, without prior permission from AT&T, any username or password information provided to Customer by AT&T. Customer is solely responsible for monitoring and controlling access to the Service, maintaining the confidentiality of the passwords and for any use of the Service that occurs during the use of the passwords. If for any reason LevelBlue believes that there has been a security related breach, LevelBlue may take whatever action LevelBlue deems appropriate to remedy the situation.

Direct User support remains the responsibility of Customer. This includes but is not limited to:

- Issues on machines of Users
- End-to-end network connectivity (e.g., Customer’s network, Internet Service Provider)
- Identity source management

SD-6.2. Customer Compliance Responsibilities

SD-6.2.1. Data Privacy Disclosure

LevelBlue Secure Workforce requires Customers to share with AT&T’s Supplier, certain User information such as email addresses, names, IP addresses, location data, MAC address, and other data elements necessary to provide this Service. Additional information regarding the data elements that are utilized by AT&T’s Supplier in conjunction with LevelBlue Secure Workforce, and the applicable Supplier policies, may be found here.

https://www.checkpoint.com/downloads/company/esg-privacy-policy.pdf

Customer consents to the collection of this data and agrees to obtain any necessary consents from its Users.

Customer represents and warrants that its use of LevelBlue Secure Workforce will be consistent with applicable privacy laws. Customer must conduct a privacy impact assessment/data protection impact assessment for Users where required by law.

Customer is solely responsible for its relationship with Users and their traffic. Customer has the authority to permit access to communications by its employees, guests, representatives, and other Users and is legally responsible for all consents. Customer represents and warrants that it has the appropriate rights to provide any User data to LevelBlue in connection with the LevelBlue Secure Workforce Service.

SD-6.2.2. Requests to Delete Data

Customer may submit a request under the California Consumer Privacy Act to delete all personal information associated with an individual or household. LevelBlue will seek to honor requests for deletion unless required or permitted by law to retain information that is subject to a data deletion request or LevelBlue determines it must retain information to provide the Services specified in this Agreement.

Requests for deletion of data must be provided to Customer’s LevelBlue account team in writing and must identify all individual(s) or household(s) whose information must be deleted.

SD-6.2.4. Cooperation with Requests

Customer agrees to, and will secure User agreement to, cooperate with and assist LevelBlue in connection with responses to requests or requirements of a regulator, authority or governmental body concerning the Service.

SD-6.2.5. Importation of Technology

When using the Service, Customer is responsible for compliance with all applicable laws in the jurisdictions in which the Service is used. In certain countries, Customer may be deemed to be the importer of technology. This technology includes encryption software that may be subject to restrictions with respect to its importation and/or use in certain countries. Customer agrees that it and/or its Users will not attempt to import such technology into any countries where LevelBlue does not offer the Service. Any violations of this provision shall entitle LevelBlue to immediately terminate Customer's Service Agreement.

SD-7. Use of Service

SD-7.1. Excessive Seats

During the Service Term, if the number of Customer’s Seats increases to more than the purchased number of Seats, LevelBlue will notify Customer to agree on a reduction plan, or to work in good faith to renegotiate pricing for remaining balance of the Service Term. If the Parties are unable to reach a mutually agreeable solution, then LevelBlue may terminate the remaining Service Term of the Customer and early termination fees may apply.

SD-7.2. System Access

LevelBlue will provide Customer with read only access to the Check Point management system.

SD-7.2.1. Restrictions on Use of Service

Customer shall use the Service solely for internal business purposes and Customer shall only permit access to the Service by its Users as stated herein. Customer is prohibited from: (i) modifying, copying, or making derivative works based on the technology of the Service; (ii) disassembling, reverse engineering, or decompiling any of the technology of the Service; or (iii) creating Internet "links" to or from the Service, or "frame" or "mirror" any of the Service's content which forms part of the Service (other than on Customers' own internal intranets).

- Customer shall not (and will not allow any third party to): (i) access the Service in order to build a competitive product or service, or copy any ideas, features, functions or graphics of the Service; (ii) use the Service to send spam or otherwise duplicative or unsolicited messages in violation of any applicable laws and/or regulations; (iii) use the Service to send infringing, obscene, threatening, libelous, or otherwise unlawful material; (iv) use the Service to access blocked services in violation of any applicable laws and/or regulations; (v) upload to the Service or use the Service to send or store viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs; (vi) interfere with or disrupt the integrity or performance of the Service or the data contained therein; (vii) attempt to gain unauthorized access to the Service or its related systems or networks; (viii) remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels in the Service; (ix) perform penetration or load testing on the Service without the prior written consent of LevelBlue and agreeing to certain conditions and requirements for such penetration or load testing; or (x) without the express prior written consent of AT&T, conduct any benchmarking or comparative study or analysis involving the Service for any reason or purpose except, to the limited extent absolutely necessary, to determine the suitability of Service to interoperate with Customer’s internal systems.
- Customer shall: (i) comply with any User instructions, and training materials for the Service ("Documentation") provided to it by AT&T; (ii) be solely responsible for its activities in using the Service, including without limitation the activities of its Users, or any third parties that Customer allows to utilize the Service; and (iii) supply all technical data reasonably requested from time to time in order for the Services to be provided to Customer.
- The Service must not be used for running automated queries to web services (e.g., a Customer running a script for searching on an internet search engine that would flag the internet search engine to blacklist AT&T's internet protocol) and in case of misuse offending source IP addresses may be blocked.

SD-7.2.2. Change Requests

To make a change or to update to their Service, Customers should submit a ticket through Business Center. Most change requests can be accommodated at no additional charge.
However, before the work is started, an LevelBlue Cybersecurity support specialist will review the request and communicate to the Customer if a fee will be charged for the work. If additional charges are needed to engineer the change, then the Customer will have to sign an addendum to their service contract before the work can proceed.

Service Level Objectives (SLO)

SLO-1. Service Level Objective

Service Level Objectives		
Change Requests	**Threshold**	**Monthly Average**
Acceptance of Change Requests	Within 24 hours.	99%
Execution of Change Requests	Within 48 hours of receipt of complete information or mutually agreed upon deployment window.	99%
Hold Times	**Threshold**	**Monthly Average**
Inbound hold times	Not to exceed 5 minutes average per week.	98%

Pricing (P)

P-1. LevelBlue Secure Workforce with Check Point Pricing

Applicable rates, prices, discounts, and other terms for the Service are set forth in Customer’s Service Agreement.

P-2. Billing

Billing commences upon Service Activation of the license. LevelBlue invoices will be presented monthly and will cover charges for Services performed during the previous calendar month. Invoices will be offered in electronic format only unless a paper invoice is explicitly requested by the customer.

Country Specific Provisions (CSP)

P-3. Country Availability

LevelBlue Secure Workforce with Check Point is available inside and outside the United States. Upon request, LevelBlue will provide Customer with a list of the currently supported countries.