DIEBOLD NIXDORF

COMPREHENSIVE SERVICES

ATM END-POINT PROTECTION MONITORING

GENERAL PROVISION

Service Activation. To activate the ATM End-Point Protection Monitoring Service it may be necessary to install hardware and/or software components. Diebold Nixdorf shall have the right to install hardware and/or software on the Client's ATM units. Diebold Nixdorf shall retain ownership of all hardware installed on the Client's ATMs as required to implement the ATM End-Point Protection Monitoring Service.

Network Certification. If the Client deems it necessary, for any reason, to have the ATM End-Point Monitoring Service certified with any authorization network or to certify compliance with any government or industry standard, it is the sole and exclusive responsibility of Client to do so.

Software. Notwithstanding any other provision, any software provided in connection with this ATM End-Point Protection Monitoring Service is provided AS-IS and WITHOUT WARRANTY.

Liability Limitation. ATM End-Point Protection Monitoring Service is offered under the terms and conditions set forth in the Agreement, and all software provided in connection therewith is provided pursuant to the terms set forth above, including, without limitation, the provisions thereof which limit Diebold Nixdorf's and its supplier's liability. **WITHOUT LIMITING THE FOREGOING, IN NO EVENT SHALL DIEBOLD NIXDORF OR ITS SUPPLIERS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, EXEMPLARY, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES THAT MAY BE SUFFERED OR INCURRED BY CLIENT OR ANY PERSON OR ENTITY AFFILIATED OR ASSOCIATED WITH CLIENT, EVEN IF DIEBOLD NIXDORF HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE OR SUCH DAMAGE RESULTS FROM PERFORMANCE, ATTEMPTED PERFORMANCE, OR NON-PERFORMANCE, INCLUDING WITHOUT LIMITATION RESULTING FROM ANY USE OF ANY WORK PRODUCT, IMPLEMENTATION OF ANY RECOMMENDATIONS, INACCURACY OR INABILITY TO USE RESULTS FROM THE SERVICES, DELAY OF DELIVERY OR COMPLETION OF THE SERVICES, INACCURACY OR MISREPRESENTATION OF DATA, OR LOSS OF PROFITS, DATA, BUSINESS OR GOODWILL. IN ADDITION, THE LIABILITY OF DIEBOLD NIXDORF AND ITS SUPPLIERS, FOR LOSSES, DAMAGES, LIABILITIES, SUITS AND CLAIMS, REGARDLESS OF THE FORM OF ACTION AND THE PERSON OR ENTITY BRINGING SUCH ACTION, SHALL NOT UNDER ANY CIRCUMSTANCES EXCEED THE AMOUNT SPECIFIED IN PART 9.2 OF THE AGREEMENT.**

MINIMUM REQUIREMENTS

a. Opteva terminal
b. Windows XP Pro Operating System, SP2 minimum
c. 2GB of RAM for any ATM running Deposit Automation and/or Text to Speech otherwise 1G of RAM to support an Endpoint Protection Agent .
d. TCP/IP capable with Ethernet capability. For wireless connectivity: sufficient signal strength is required using EVDO routers with a minimum 5 GIG plan. (dial-up connections not supported)

DIEBOLD NIXDORF

COMPREHENSIVE SERVICES

HOW IT WORKS

Diebold Nixdorf installs/configures the Symantec Endpoint Protection (SEP) software on the ATM to communicate with the End-Point Security system at Diebold Nixdorf's Operation Center. When the SEP software detects an event at an ATM, an alert is sent from the ATM to the system via this connection. Diebold Nixdorf monitors the SEP security log files for events related to security and react to security-related events as described below.

In addition to monitoring for security alerts/event, Diebold Nixdorf also manages the firewall, and Antivirus components of SEP. SEP software updates are automatically performed by the system, as they are made available by Symantec. The End-Point Security system checks the Symantec web site daily for any software updates. Each ATM checks-in to the End-Point Security system periodically to see if updates are available and if so, they are sent to the ATM to remain current with the latest levels of protection.

CORE SERVICE DESCRIPTION

Services include on-boarding, maintaining, reviewing, and reporting for "in-scope" ATMs configured with the standard SEP agent software build.

On-boarding

- Diebold Nixdorf licenses to the Client the Sygate/Symantec SEP software agent.
- Diebold Nixdorf configures the Symantec End Point Protection Server (SEP) console for Client's deployment at Diebold Nixdorf's Green facility.
- Diebold Nixdorf's ArcSight SEIM, which is located onsite at Diebold Nixdorf's facility, takes feeds from the SEP console.
- Diebold Nixdorf verifies the standard build prior to implementation on an initial ATM to ensure log feed information is available for monitoring.
- Diebold Nixdorf monitors and analyzes traffic detected by the SEP agent build to create a policy of expected or normal activity levels for the "in-scope" ATMs.

SEP Console Maintenance

- Diebold Nixdorf performs Rule Changes as described for each component in the below section title "ATM SEP Management Components" of this SOW.
- Diebold Nixdorf installs Diebold Nixdorf-approved (e.g., applicable, tested, and qualified) Symantec Updates for the "in-scope" SEP console.

Engineer Reviews

Prior to implementing changes and Symantec software updates, Diebold Nixdorf conducts an Engineer Review to endeavor to ensure:

- Hardware/software meets all prerequisites
- Backup of previous configuration information exists
- Change is consistent with security best practices
- Change is relevant to Diebold Nixdorf's environment
- Change can be implemented within allotted timeframe

Reporting

- Reports containing information on the number and types of events received the previous month will be included in the monthly reporting received from Diebold Nixdorf.

ATM SEP Managed Components

Diebold Nixdorf will manage the firewall, HIDS/HIPS, and Antivirus SEP components via a centralized SEP management console, as described below.

- Diebold Nixdorf maintains a configuration profile of the SEP console in case of SEP console failure.
- Diebold Nixdorf will not implement changes to the Client's configuration without prior approval from Client.

Firewall Component

- Diebold Nixdorf will modify Rules via Access Control Lists (ACLs) for inbound and outbound connections.
- Diebold Nixdorf will implement one set of Firewall Rule changes per calendar month at Client's request.

Antivirus Component

- Diebold Nixdorf configures the Antivirus component to automatically pull updates from Symantec.

Monitored Service Components

Diebold Nixdorf monitors SEP console logs utilizing a Log Transport Agent (LTA). Diebold Nixdorf utilizes a multi-phased approach to implement and "tune" monitoring services:

- Phase 1 – Configuration
- Phase 2 – Normalization
- Phase 3 – Ongoing Tuning and Support

Diebold Nixdorf works with Client's main Point of Contact (POC) to create a schedule with dates for all deliverables, customize and tune appropriate components for Diebold Nixdorf's environment, and ensure completion of the Client Profile for environmental information.

Phase 1 – Configuration: Diebold Nixdorf pre-configures the SEP console for Client. Configuration is dependent upon Client providing all the required information as requested by Diebold Nixdorf.

Phase 2 – Normalization: Diebold Nixdorf reviews data generated, performs statistical analysis in accordance with the project plan. Diebold Nixdorf performs the following major functions during the Normalization process:

- Map software errors
- Establish a baseline by monitored service component
- Establish a set of rules for blocking, reporting, and logging
- Work with Client to establish minimum and maximum log quantity thresholds in appropriate time intervals, specific to each log source.

Phase 3 – Ongoing Tuning and Support: Phase 3 lasts for the duration of the SOW and consists of Diebold Nixdorf performing the following functions:

- Generate Events based on settings established during Normalization.
- Review all Events and escalate appropriately to Client based on Client's pre-defined escalation procedures laid out in the Client Profile document.
- Report on all Events in the monthly reports provided by Diebold Nixdorf.

- Provide Client notifications and perform appropriate remediation tasks as defined in the “Response Plan” below
- Conduct Normalization and report card reviews when material shifts occur in Event patterns, for major network environment changes, or on an annual basis.
- Implement Rule Changes within a 24-hour implementation period within the standard business week, or within the first available Client-defined maintenance window.
- Contact Client of critical security events within fifteen minutes of detection by the system.

Response Plan

- Report Only - Event data is reported monthly as part of the monthly reports provided by Diebold Nixdorf.
- Low Severity incident - Email to Client
- High Severity incident - The following response will be executed.
- Help Desk notifies Client of the incident. This notification will consist of both an e-mail and an attempt to contact the primary or back-up contacts for security events via phone.
- If requested, the Help Desk will consult with the Client on responding to the security event.
- If the Client requests that a Diebold Nixdorf Service technician be dispatched to replace the hard drive or reinstall the software, charges will apply.

Response Categories

Client could receive notification for the events that include, but not limited to, the following categories of Events. The Client is responsible in determining what, if any, response will take place if an Event is received. Examples of the possible type of Events that could be received are as follows:

Category Options	Description	Severity
Chat/Instant Messaging Activity	A chat tool is being utilized like "gtalk" or AIM to communicate to/from the ATM. - Typically against company policies	High
SEP Configuration Change / Modification	Activity that indicates a change in the configuration of a device (i.e. Firewall config changes, etc.)	Low
Connectivity / Network Problem	These events indicate possible problems with network health or connectivity.	Low
Desktop Application Exploit	Any buffer overflow attempts to exploit vulnerabilities associated with user applications running on an ATM.	High
ATM Reconnaissance	Activity that attempts to find out what's on a ATM (e.g. Vulnerability scanning: Nessus, Whisker, OS Flaws, etc…)	Low
Informational Messages	These events are informational in nature and have little to no security or system impact (example: AV updates were updated successfully)	Report
Network Exploit	Network traffic, which represents anomalies or RFC violations for such protocols as TCP or ICMP. (Unexpected Data in an ICMP packet or Flags not set appropriately in a TCP packet, TCP-IP Protocol Anomalies, RFC Violation)	Low
Network Reconnaissance	Activity that attempts to find out what's on the network - Information/Discovery Scan: Nmap, SYS Scan, Port sweep	Low
OS Exploit	Any attempts to exploit vulnerabilities associated with an Operating System via buffer overflow. (example: Vulnerabilities with the windows kernel).	High

Unauthorized Remote Access	This activity is caused by use of unauthorized remote administration tools (e.g. RDP / Term Server, VNC, etc..).	Report
Spyware / Malware	Hostile or intrusive software which may monitor and report system activities to third parties or cause damage to the operating system without user consent.	High
Virus / Trojan / Worm	Malicious code/software that compromises system integrity and security. This may lead to network disruptions, data loss and system instability.	High

Changes in Service
If regulatory changes (e.g., changes by a regulatory agency, legislative body, or court of competent jurisdiction) require Diebold Nixdorf to modify the Services described herein, Client agrees in good faith to work with Diebold Nixdorf to amend this SOW accordingly.

Connectivity
Connectivity is required between the ATMs and Diebold Nixdorf's Network Operations Center (NOC). The following connectivity options may be implemented:

- **MPLS** – Circuits and routers are ordered and provisioned by Diebold Nixdorf; Client is billed by Diebold Nixdorf
  - to Client's wide-area network or directly to each ATM
- **Wireless using EVDO routers** (5 GB min. plan) of sufficient signal strength – Wireless plans are ordered and provisioned by Diebold Nixdorf; Client is billed by Diebold Nixdorf
  - directly from each ATM (Requires one circuit and router per ATM)
- **VPN – Managed** – VPN HW/SW is provided by Diebold Nixdorf; Client is billed by Diebold Nixdorf
  - to Client's wide-area network or directly to each ATM
- **VPN – Co-managed** – VPN HW/SW is provided by Client (Client location) and by Diebold Nixdorf (Diebold Nixdorf location); Client is billed by Diebold Nixdorf
  - to Client's wide-area network or directly to each ATM

IMPLEMENTATION PROJECT – DIEBOLD NIXDORF RESPONSIBILITIES

a. Review and reach agreement on the incident response plan.
b. Configuring the Symantec Endpoint Protection server for the standard ATM End-Point Protection Monitoring Service.

IMPLEMENTATION PROJECT – CLIENT RESPONSIBILITIES

a. Client must have a valid Master Licensing Agreement (MLA), Managed Equipment and Services Agreement (MESA), or Diebold Nixdorf Comprehensive Agreement (DCA) with Diebold Nixdorf representing the copies of Windows XP Pro, or later version, they have licensed for their ATMs. The number of copies purchased must equal the number of ATMs to be managed by this service.
b. Client must provide Diebold Nixdorf Technician with administrative rights to access the ATM during the Security Agent Client Installation process.
c. Client must have sufficient bandwidth available on their internal network to support large file transmissions; Diebold Nixdorf highly recommends that the internal network be a minimum of 128K.
d. Client must accept the addition of pre-defined rules to the ATMs firewall application to allow it to communicate with the Symantec Endpoint Protection Server operated by Diebold Nixdorf.

e. Schedule all service-related activities and communicate with the POC as needed for installation and ongoing tuning and support.
f. Provide Diebold Nixdorf with contact information updates.
g. Ensure access and connectivity to the “in-scope” SEP console.
h. Provide knowledgeable staff, and/or third party resources, to assist Diebold Nixdorf with on-boarding.
i. Configuring end-to-end connectivity.
j. Providing IP addresses.
k. Providing data on applications which must communicate to/from the ATM.
l. Provide Diebold Nixdorf with access to an initial ATM for configuration and piloting the support Services.
m. Provide a unique identifier (naming convention) for all “in-scope” ATMs to enable appropriate Event escalation.
n. Provide connectivity between the managed ATMs and Client’s network (except for wireless communications).
o. IT Security Agreement (for VPN based connectivity)
p. Provide any other information as requested.
q. Complete Diebold Nixdorf Change Request (AMC form) to authorize any required changes in scope.
r. The Change Request must be submitted by Client’s appropriately authorized individual, verifiable in Diebold Nixdorf’s client contact database.
s. Once the Service is installed and active, it is highly recommended that the Client perform a security scan of the installed system to validate the proper security configuration of the ATM.

Client acknowledges and agrees to the following:

a. Client will work reasonably with Diebold Nixdorf to establish an acceptable implementation period.
b. Rule Changes involving auto-blocking (shunning) require approval from an authorized Client individual (verifiable in Diebold Nixdorf’s database) prior to implementing an auto-blocking rule.
c. Diebold Nixdorf is not responsible for any loss of business incurred by Client (or third parties associated with Client) due to outages caused by a Client requested Rule Change involving auto-blocking.
d. Client’s failure to meet any of the Service Requirements on a timely basis can result in delays in the on-boarding process.
e. Diebold Nixdorf will not manage, update, or support altered, damaged, or modified software, or software, which is not the most-current or Symantec supported version.
f. Client is fully aware of Diebold Nixdorf’s recommendation to perform full back-ups prior to the performance of Services.
g. The “in-scope” SEP console may not have visibility into encrypted packets and therefore, may not detect viruses contained within those packets.