



WATERFALL SECURITY SOLUTIONS

התמודדות עם התקפות סייבר בארגון

הגנה מוחלטת על רשתות רגישות והגנה מפני דליפת נתונים

איתי ברק

פריסייל דירקטור

מייל: itayb@waterfall-security.com

טלפון: +972 50 444 1716

רקע על חברת Waterfall Security Solutions



הקמה
ב-2007
(Gita Technology)



בחירתם של
האנליסטים
הבינל' המובילים



אלפי התקנות מוצלחות
בארץ וברחבי העולם
בגופי תשתית קריטית



מטה החברה
ומח' פיתוח
בישראל



חברה ישראלית
מפוקחת מלמ"ב
בעלות סיווג רלוונטי



חבר בדירטוריון החברה
האלוף במיל' עמי שפרן
ראש אגף תקשוב



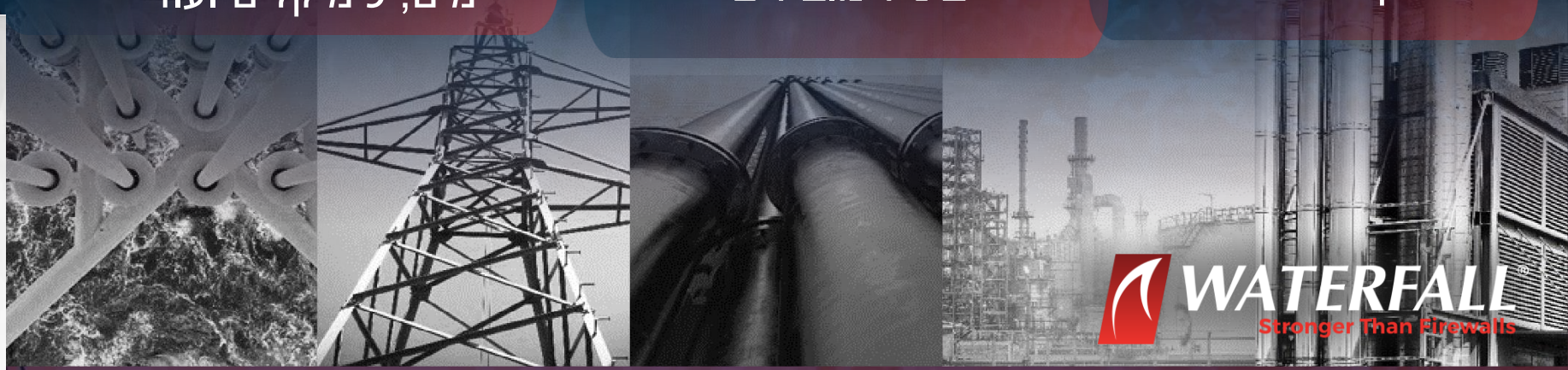
מגוון סגמנטים: ממשלה,
ביטחון, תחבורה, חשמל,
מים, כימיקלים ועוד



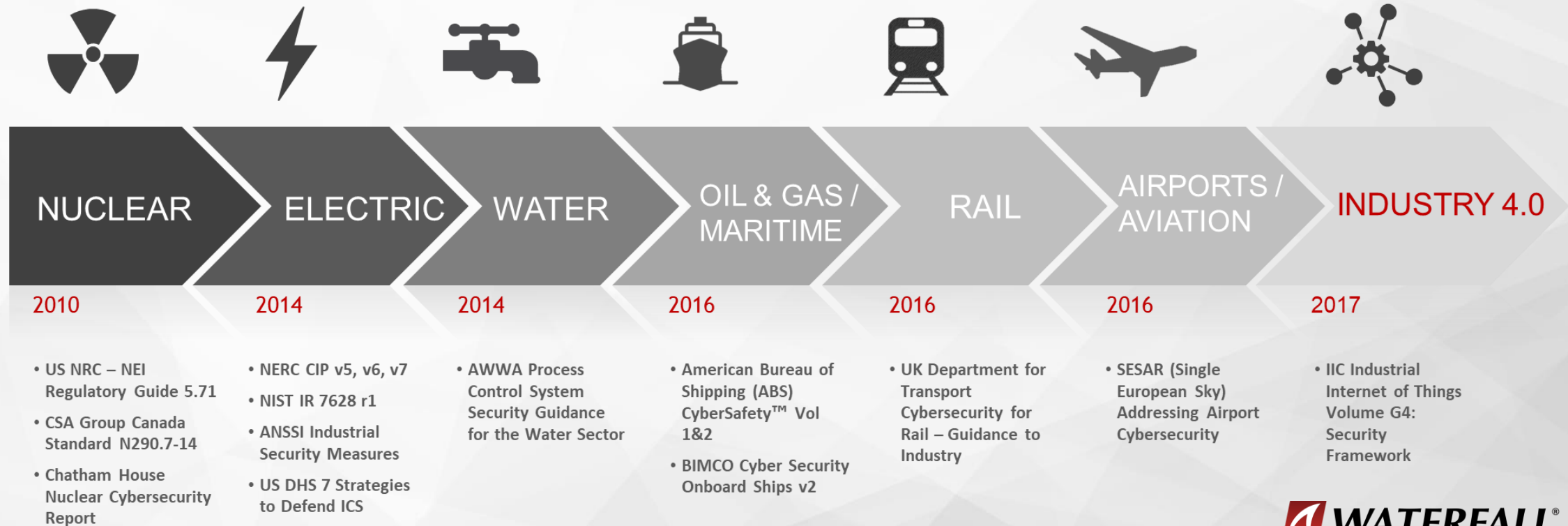
שת"פ עם יצרנים
ישראלים
בינל' מובילים



ספק מורשה של
משרד הביטחון:
מס' ספק: 11001986



התפתחות התקינה בנושא אבטחת סייבר מתשתיות קריטיות לתעשייה



הצורך

- זמינות מידע: בכל זמן, בכל מקום ועל גבי ממשקים שונים
- חשיפת המידע התפעולי של הארגון:
 - מערכות ענן
 - מעקב ובקרה פנימית של הארגון
 - ספקים חיצוניים

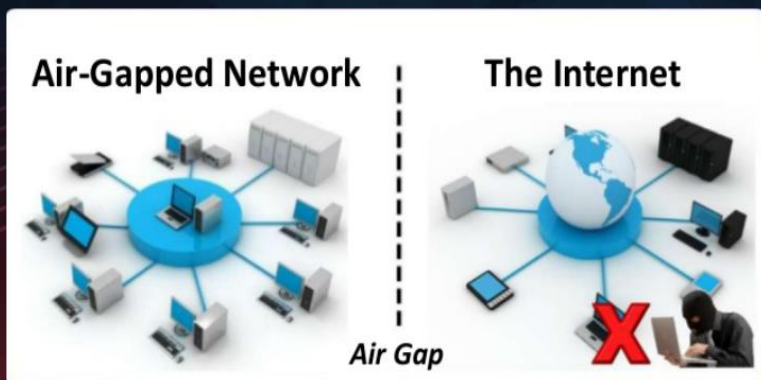


הסכנות

- חשיפת הרשתות למתקפות מסוגים שונים:
 - סוסים טרויאניים
 - כופר
 - מניעת שירות
 - ועוד

האתגר : חיבור רשתות בעלות סיווג שונה

- עם התפתחות הטכנולוגיה, סיכוני סייבר הפכו נרחבים
- מדי יום מתבצעות מתקפות רבות ומגוונות כנגד גופים פרטיים וממשלתיים, תשתיות לאומיות, רשתות תקשורת ציבוריות ופרטיות ועוד
- הגנה על רשתות רגישות מפני דליפת נתונים ומתקפות לגניבת נתונים
- המידע הנאסף ברשתות מסוג זה הוא רגיש מאוד
- יש צורך לקבל מידע מסביבות בעלות סיווג שונה
- זליגת נתונים רגישים עלולה ליצור נזק חמור, שאינו קביל ושלא ניתן לתקנו
- פתרון Air Gap אינו מאפשר העברת מידע מהירה בזמן אמת והמידע מועבר באופן ידני



התבססות על פתרונות מבוססי תוכנה אינם הפתרון האידאלי



FIREWALLS

Any number of firewall layers are porous and easily breached.



IDS

Intrusion Detection Systems detect attacks AFTER they happen.



UPDATES & PATCHES

are continuous, time consuming & might introduce new vulnerabilities.

A **different** security posture is required for protecting the safety & reliability of the **Critical network perimeter**

הפתרון של Waterfall - שער אבטחה חד כיוונית



רשת פנימית

רשת חיצונית

שער אבטחה המבוסס על רכיב **חומרה** להעברת סוגי **תוכנה** שונים באופן חד כיווני

- רכיב החומרה מכיל 2 מודולים : TX – לייצר הנמצא בצד השולח וRX הצד החיצוני המקבל הכולל תא פוטו אלקטרי .
- שניהם מחוברים בסיב אופטי בודד .
- הפתרון מהווה מעצור פיזיקלי חד סטרי המונע זליגת מידע בכיוון ההפוך .
- רכיבי התוכנה מאפשר שיכפול של סרברים מהרשת החיצונית לרשת הפנימית במגוון אפשרויות (דטה בייסים, MQ , ועוד)

תו תקן לדרישות המחמירות בתחום



US DHS SCADA
Security Test Bed



Certified Common
Criteria EAL4+
High Attack
Potential



Certified ANSSI
CSPN – Security
Certification
First Level



Japanese CSSC
Test Bed



NOM Mexico
Certification



South Korea
KC Certification



Israel Testing
Laboratories
Certification



National IT Evaluation
Scheme (NITES)
Singapore Govt

עמידה בדרישות רגולציה: מקומית / בינלאומית



רכיבי תוכנה להעברה חד כיוונית (רשימה חלקית)

HISTORIANS & DATABASES

- OSIsoft: PI System, PI Asset Framework, PI Backfill
- GE: iHistorian, iHistorian Backfill, OSM, Bently-Nevada System1,
- Schneider-Electric: Wonderware eDNA, Wonderware Historian, Wonderware Historian Backfill, SCADA Expert ClearSCADA
- AspenTech IP.21, Rockwell FactoryTalk Historian, Honeywell Alarm Manager, Scientech R*Time,
- Microsoft SQL Server, Oracle MySQL, PostgreSQL



OTHER CONNECTORS

- TimeSync, Netflow
- Video & audio streaming
- Kaspersky, Norton, FortiGate, Check Point, McAfee and OPSWAT Anti-virus updaters
- OPSWAT Metasploit
- WSUS and Linux Repository updaters
- Tenable Nessus Network Monitor, Nessus Security Center Updates
- Remote printing



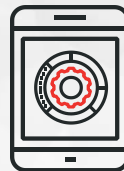
FILE TRANSFER

- Folder mirroring, Local Folders
- FTP/S, SFTP, TFTP, SMB, CIFS, NFS, HTTPFS
- Log Mirroring



INDUSTRIAL APPLICATIONS AND PROTOCOLS

- Siemens S7 & PCS7 Historian
- OPC DA, A&E, HDA, HDA Backfill and OPC UA
- Emerson: EDS,
- Yokogawa OPC, GE iFix
- Modbus, DNP3, ICCP, IEC 60870-5-104, Omni Flow



ENTERPRISE MONITORING

- FireEye: Helix & Managed Defense
- Email/SMTP, SNMP, Syslog
- HP ArcSight, Splunk, Splunk Universal Forwarder, IBM QRadar, McAfee ESM, CyberX, Radiflow iSID, ForeScout Silent Defence, Dragos, Indegy,
- MSMQ, IBM MQ, Active Message Queue, AMQP, TIBCO,
- SolarWinds Orion, Thales Aramis, IOSight, Panorama



REMOTE ACCESS

- Remote Screen View
- Secure Bypass



WF-500 Series Hardware רכיב חומרה

Modular, Powerful, Flexible

- Ours or your host modules
- Supports all-in-one rack-mount form factor, or each module in a separate cabinet, or any combination
- Optional DIN-Rail Hardware for sites with no rack space - contains both TX and RX Modules
- Windows or Linux
- User serviceable, user expandable
- Standard: 2x dual power supplies
- Standard: 1 Gbps
- **Certified Common Criteria EAL4+**



WATERFALL INNOVATION

Waterfall for IDS:

Unidirectional solutions for Intrusion Detection Systems

Waterfall FLIP:

Reversible unidirectional technology and remote access

Remote Screen View:

Safe remote support for unidirectionally protected networks

Secure Bypass:

Scheduled and emergency support by on-site personnel

Unidirectional CloudConnect:

Security for Cloud enabled devices

Waterfall BlackBox:

Secure logs repository





WATERFALL®

Stronger Than Firewalls