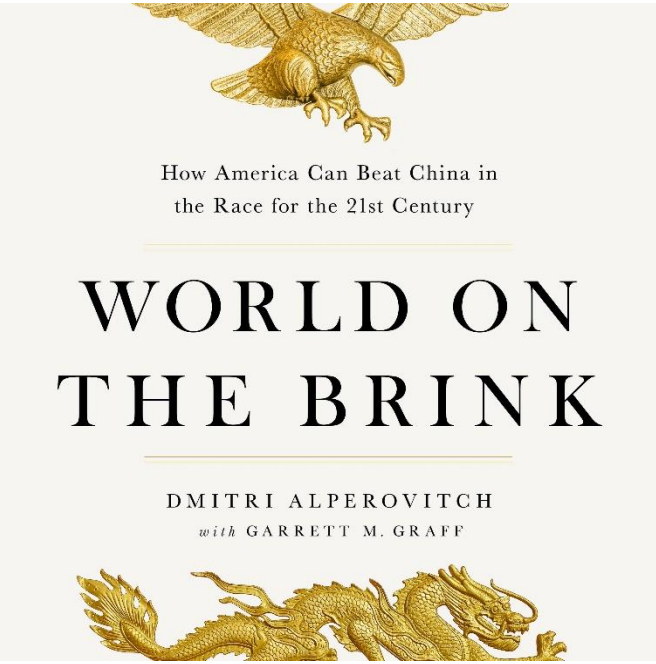
PDF/SOLUTIONS™

secureWISE & Cybersecurity in Semi

Presented by: Grant Swanson – Director, secureWISE Taiwan

Cybersecurity in Semi - Landscape



"We're not just protecting data anymore. We're protecting trust, sovereignty, and the continuity of our global semiconductor ecosystem."

- Cybersecurity no longer means lone hackers in basements. It is structured, well-resourced and occasionally state sponsored attacks meant to disrupt, extract data and undermine trust
- secureWISE exists not just to enable remote access, but to control it

In the new era of nation-state cyber operations
"good enough" security simply isn't good enough.

secureWISE

Market-standard provider of secure connectivity to the semiconductor industry

Secure, configurable end-to-end remote connectivity across private networks to equipment:

- Allows equipment manufacturers and equipment owners to collaborate **over private networks** that protect intellectual property (IP) for all involved parties
- Maximizes lifetime of machinery, improves tool performance, reduces downtime, and enhances the remote capabilities of its users
- Provides Fabs with full audit capabilities
- Not reachable via the Internet, protects the user from unwanted internet-facing attacks

>190
300mm Fabs connected

>100
Unique OEMs Connected

Tens of Thousands
Connected tools world-wide[1]

8
Global data hubs

Petabytes
Data transmitted

Role-Based Access Control

RBAC Authorization

Team or User Level Access

Fully configurable access per service type

Remote View

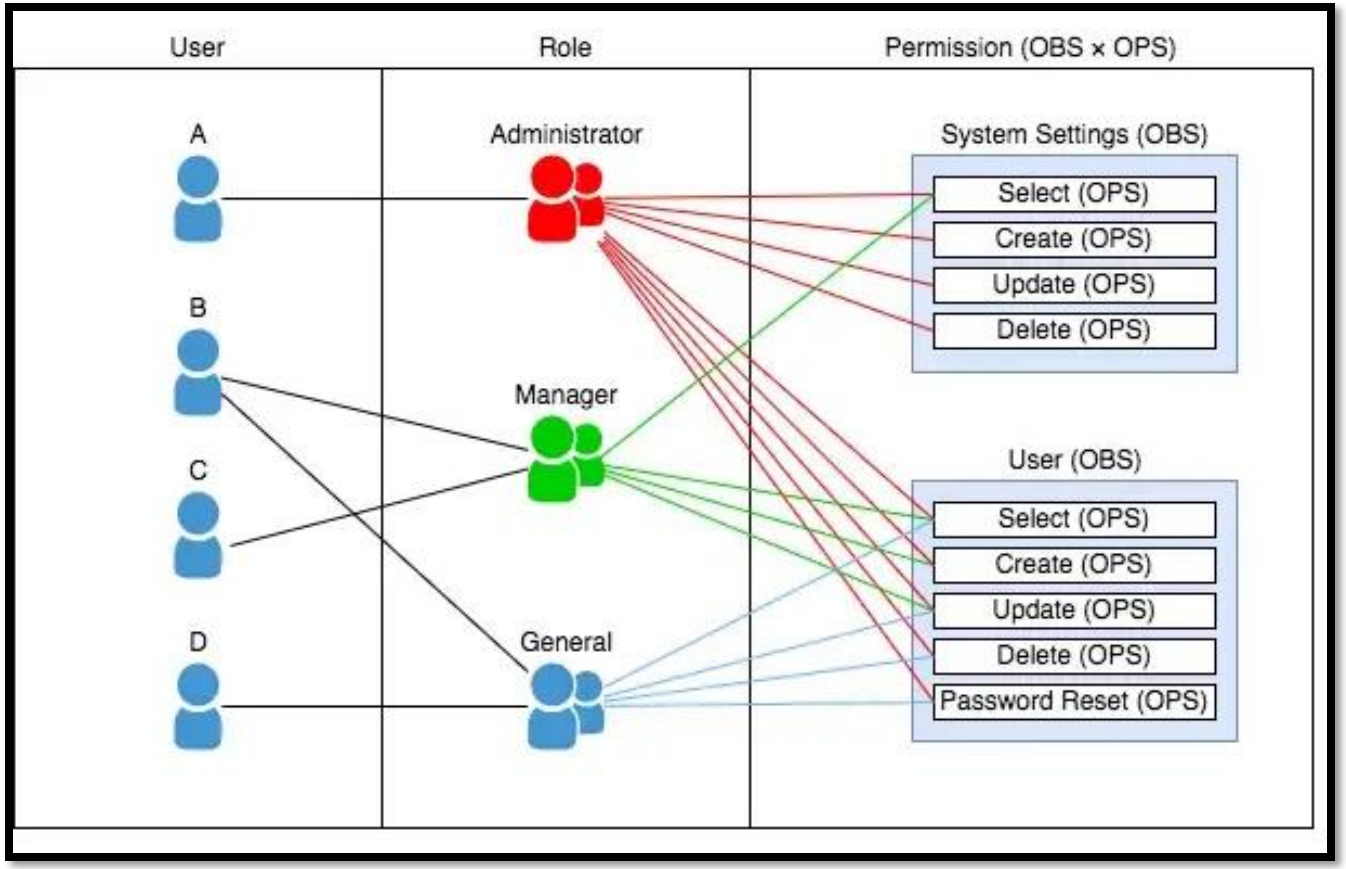
- Allow
- Deny
- On-tool approval required (optional)

Remote Control

- Allow
- Deny
- On-tool approval required (optional)

File Transfer

- Specific directory or file limitations
- Allowed listing
- Denied Listing



PDF/SOLUTIONS™

Multiple Services Supported

Secure File Transfers

- Allows files transferred to and from the secureWISE staging area
- Secure pushing or pulling files from tools
- Uses File Transfer Protocol (FTP)
- Access permissions set on secureWISE server
- Staging area scans for viruses
- Audited record of user activity

Remote Tool Operation (RTO)

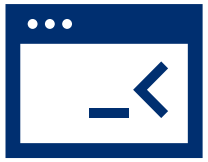
- Remote view of a tool's active display monitor or control of a tool's computer(s)
- Access the tool computer's desktop via Virtual Network Computing technology
- Remote tool operation and viewing at factory facility
- Select from all tools on network
- Verifies users' permissions
- TCS runs to communicate, act as client
- Audited record of user activity

HTTP/HTTPs

- Provides remote access to the tool's web server
- User logs into serviceNET server
- Server grants access
- View predefined 'bookmarked' web pages
- Audited record of user activity
- Web pages and attachments are scanned for viruses

Port Forwarding

- Allows remote access to a variety of TCP-based server applications running on the tool
- Access Collaborative Client
- serviceNET verification
- Audited record of user activity
- RDP would be one potential protocol for server connections (where permitted by customer)



Remote Application Access (RAA)

- RAA is a whitelisted command that returns a response to a remotely connected user
- Predefined Windows/UNIX commands for common diagnostic and status checks
- Generally passive in design
- RAA based on Secure Shell (SSH) protocol
- Supports secure file transfer with virus scanning

Chat

- Seamlessly collaborate as users operate on the tool

Multiple Services Supported

Scheduler Server Enterprise Edition

- Allows scheduled and event-based file transfer to/from multiple secureWISE servers
- Automates collection of files on tools
- Establishes SSEE script on server running SSEE
- Determines run time, what actions to run
- Activity report, FTP files collection, etc.

OEM Connector

- Enables on-site technicians to securely access their corporate network, assets (ex: documentation, CRM, etc.)
- Reverses the connection: Fab to OEM Network
- Can support OEM web server that is either Internet facing or only available from within the OEM's corporate network

securePASS/SSO

- Eliminates the need for separate logins per secureWISE server
- Allows the authentication to any securePASS enabled server - authentication is automatically propagated and honored at any other securePASS enabled server

High-Availability (HA) Options

- secureWISE server option for redundant network and server operation
- Maintain high availability in the hardware of the server

Business Management Portal (BMP)

- secureWISE usage dashboard
- Manage how secureWISE is being utilized by support staff
- Manage resources effectively

SAML 2 Support

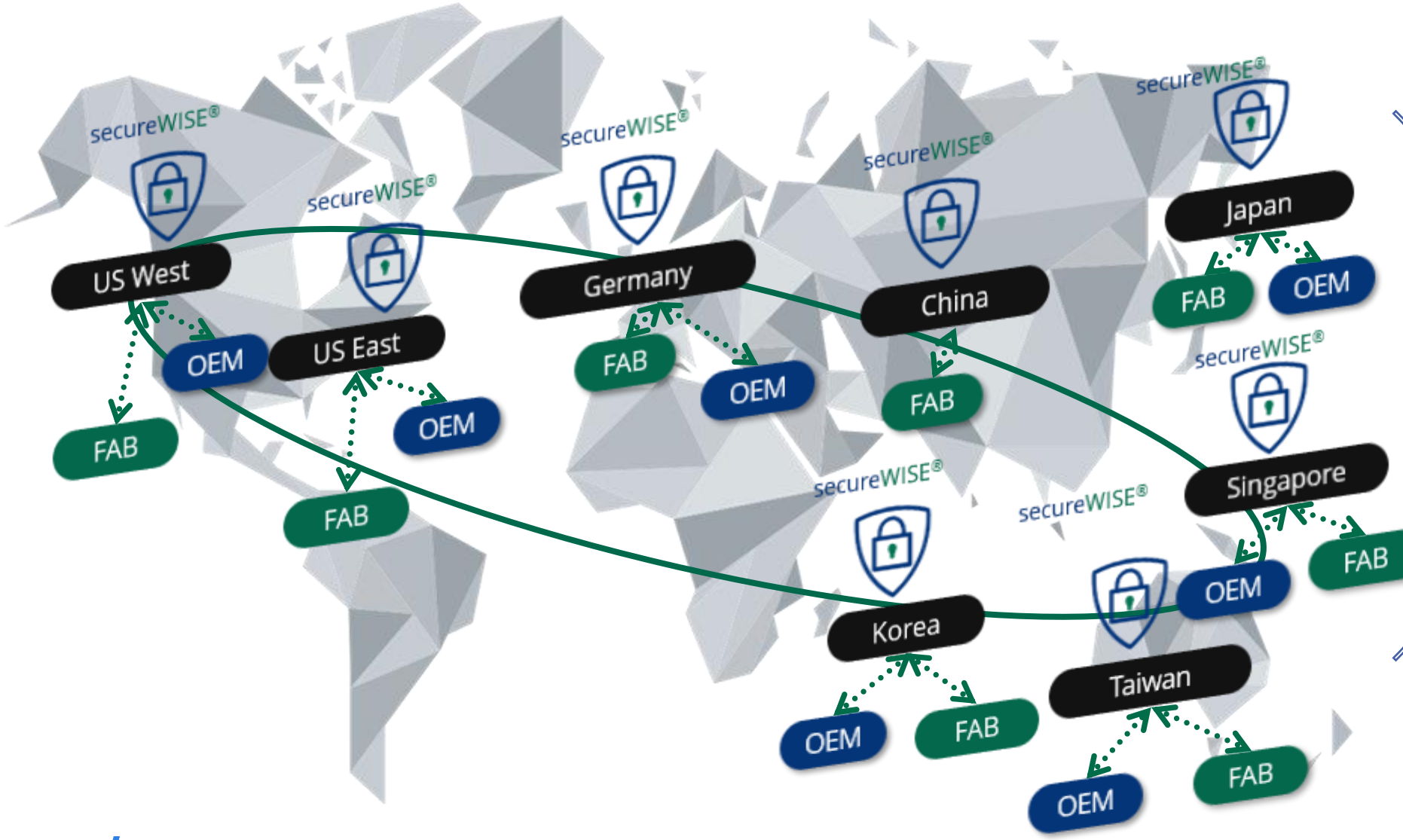
- Common interface for single sign on systems
- Extends corporate network authentication to secureWISE server

Activity Reporting/Audit Access – Report Sample

DATE	USER	DETAIL	COMMAND NAME
2022-08-11 02:25:12 UTC	ils_ils technology (ils_tech)	ils_tech is creating a transfer from staging to Tool: ILS.Server.eCentre	XFER_STG_TO_TOOL
2022-08-11 02:25:12 UTC	ils_ils technology (ils_tech)	ils_tech gets tool file list	LIST_FTP
2022-08-11 02:25:12 UTC	ils_ils technology (ils_tech)	ils_tech starting a ftp list service for Tool: ILS.Server.eCentre	USER_LOGON_FILEXFER
2022-08-11 02:25:12 UTC	ils_ils technology (ils_tech)	User ils_tech successfully authenticated from 35.171.53.9 using File Transfer	USER_AUTHENTICATE
2022-08-11 02:25:12 UTC	ils_ils technology (ils_tech)	ils_tech created a transfer from client to staging	UL_TO_STAGE
2022-08-11 02:25:12 UTC	ils_ils technology (ils_tech)	User 'ils_tech' from 35.171.53.9 failed to authenticate using his/her certificate to access /ecftp	USER_AUTHENTICATE_FAILED
2022-08-11 02:25:13 UTC	ils_ils technology (ils_tech)	transferring file: adhoc/symcdefs-unix-20220810.tar.gz from client to staging	UL_TO_STAGE
2022-08-11 02:25:44 UTC	ils_ils technology (ils_tech)	transferring file: adhoc/symcdefs-unix-20220810.tar.gz from staging to tool	XFER_STG_TO_TOOL
2022-08-11 05:16:42 UTC	ils_ils technology (ils_tech)	User ils_tech requested to get a list of sessions from Admin Client 36.234.151.175	LIST_SESSION
2022-08-11 05:16:42 UTC	ils_ils technology (ils_tech)	User ils_tech successfully logged on from 36.234.151.175 using Administrative Client.	USER_LOGON
2022-08-11 05:18:46 UTC	ils_ils technology (ils_tech)	User ils_tech successfully logged on from 36.234.151.175 using Customer Sites.	USER_LOGON
2022-08-11 05:18:53 UTC	ils_ils technology (ils_tech)	User ils_tech logged off from 36.234.151.175.	USER_LOGOFF
2022-08-11 05:19:22 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai failed to logon from 36.234.151.175 using Unknown. Details: The credenti	USER_LOGON_FAILED
2022-08-11 05:19:27 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai successfully logged on from 36.234.151.175 using Unknown.	USER_LOGON
2022-08-11 05:19:28 UTC	ils_Duncan Tsai (ils_duncan.tsai)	Secured message created for user id = ils_duncan.tsai, server name = ecdemo-us-east-01.secu	SM_AUTHENTICATION_CREATE_MESSAGE
2022-08-11 05:20:03 UTC	ils_Duncan Tsai (ils_duncan.tsai)	Secured message authentication was successful using Collaborative Client.	SM_AUTHENTICATION_VALIDATED_MESSAGE
2022-08-11 05:20:03 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai successfully logged on from 36.234.151.175 using Collaborative Client.	USER_LOGON
2022-08-11 05:20:07 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai got a list of sessions from 36.234.151.175	LIST_SESSION
2022-08-11 05:27:50 UTC	ils_ils technology (ils_tech)	User ils_tech requested to get a list of sessions from Admin Client 36.234.151.175	LIST_SESSION
2022-08-11 05:37:26 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai successfully logged on from 36.234.151.175 using Customer Sites.	USER_LOGON
2022-08-11 05:38:39 UTC	ils_ils technology (ils_tech)	User ils_tech requested to get a list of users.	USER_SEARCH
2022-08-11 05:38:48 UTC	ils_ils technology (ils_tech)	User ils_tech requested to get a list of users.	USER_SEARCH
2022-08-11 05:38:50 UTC	ils_ils technology (ils_tech)	User ils_tech requested to get a list of teams.	TEAM_SEARCH
2022-08-11 05:38:53 UTC	ils_ils technology (ils_tech)	User ils_tech requested to get a list of organizations.	ORGANIZATION_SEARCH
2022-08-11 05:46:33 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai logged off from 36.234.151.175.	USER_LOGOFF
2022-08-11 05:46:53 UTC	ils_ils technology (ils_tech)	User ils_tech failed to logon from 36.234.151.175 using Administrative Client. Details: The cre	USER_LOGON_FAILED
2022-08-11 05:47:26 UTC	ils_ils technology (ils_tech)	User ils_tech successfully logged on from 36.234.151.175 using Administrative Client.	USER_LOGON
2022-08-11 05:47:26 UTC	ils_ils technology (ils_tech)	User ils_tech requested to get a list of sessions from Admin Client 36.234.151.175	LIST_SESSION
2022-08-11 05:48:34 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai successfully authenticated from 36.234.151.175 using Collaborative Client	USER_AUTHENTICATE
2022-08-11 05:48:35 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai joined session 'ACME_Test_Demo' from collaborative client at 36.234.151.	JOIN_SESSION
2022-08-11 05:48:40 UTC	ils_Duncan Tsai (ils_duncan.tsai)	User ils_duncan.tsai successfully authenticated from 36.234.151.175 using File Transfer	USER_AUTHENTICATE
2022-08-11 05:48:41 UTC	ils_Duncan Tsai (ils_duncan.tsai)	ils_duncan.tsai starting a ftp staging service for Tool: ACME.Test.Demo	USER_LOGON_FILEXFER
2022-08-11 05:48:41 UTC	ils_Duncan Tsai (ils_duncan.tsai)	ils_duncan.tsai starting a ftp list service for Tool: ACME.Test.Demo	USER_LOGON_FILEXFER
2022-08-11 05:48:42 UTC	ils_Duncan Tsai (ils_duncan.tsai)	ils_duncan.tsai gets tool file list	LIST_FTP
2022-08-11 05:48:49 UTC	ils_Duncan Tsai (ils_duncan.tsai)	ils_duncan.tsai Initiated an RTA Service.	RAA_SERVICE_INIT

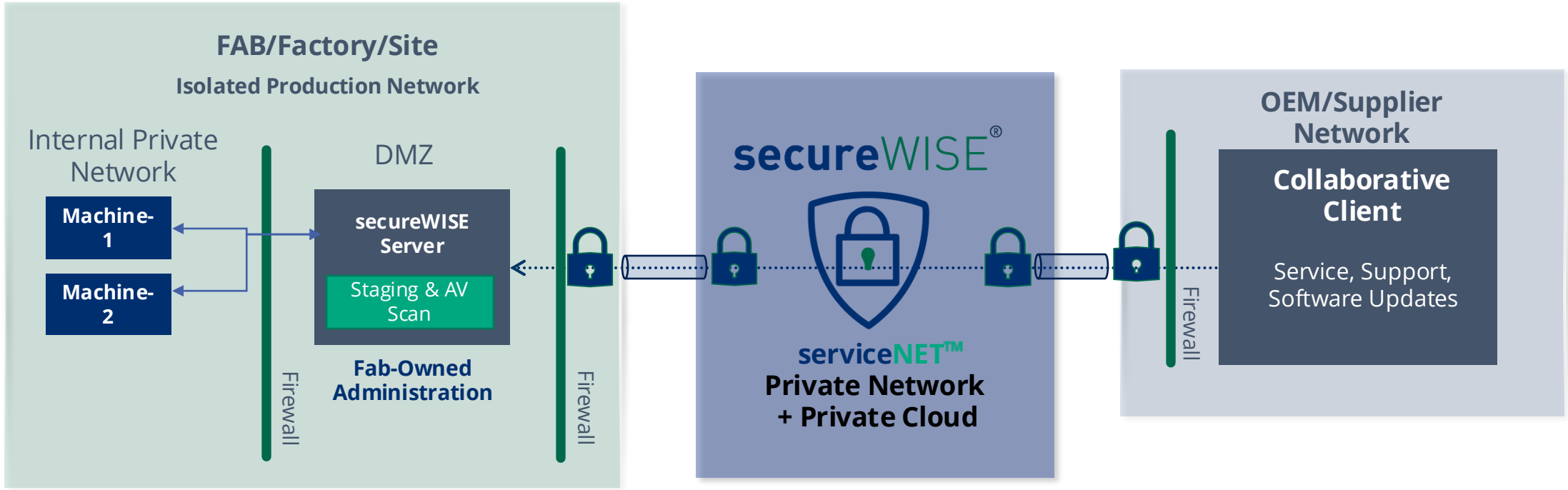
serviceNET

Global, secure, private network for machines



- Global, private worldwide network
- Runs on IPSec Layer
- Closed / unpublished
- Asia, Europe & North America Hubs
- OEM on / off-ramp
- Multi-tenant architecture
- Redundant

secureWISE Architecture



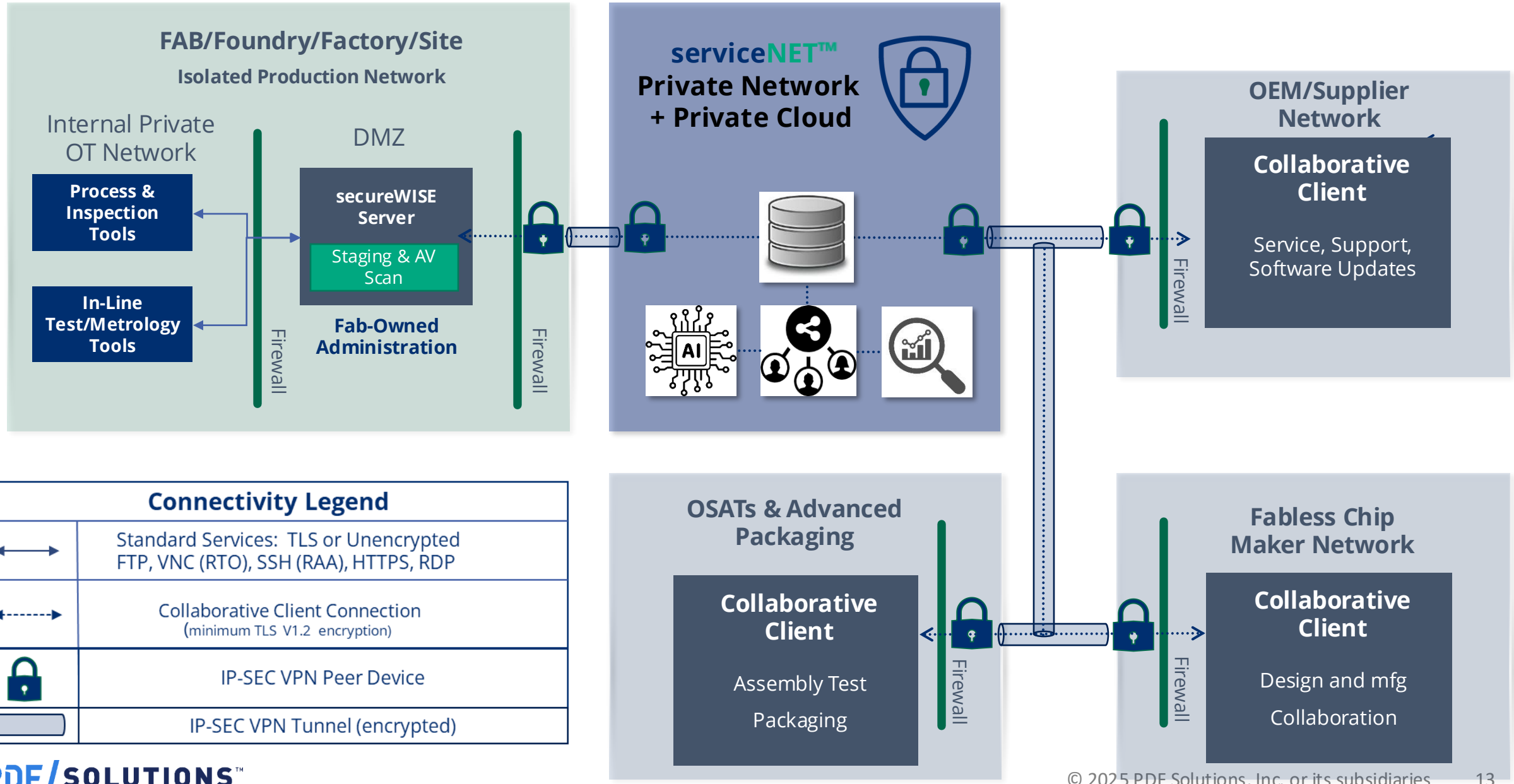
Connectivity Legend	
⟷	Standard Services: TLS or Unencrypted FTP, VNC (RTO), SSH (RAA), HTTPS, RDP
⟷ (dashed)	Collaborative Client Connection (minimum TLS V1.2 encryption)
🔒	IP-SEC VPN Peer Device
▭	IP-SEC VPN Tunnel (encrypted)

Secure Remote Access to Equipment

- Secure, end-to-end remote tool
- Multiple security barriers
- Not reachable via the internet
- Single pane-of-glass access management
- OEMs save money, offer value-added services
- Balanced security and access as defined by the fab

PDF SOLUTIONS™

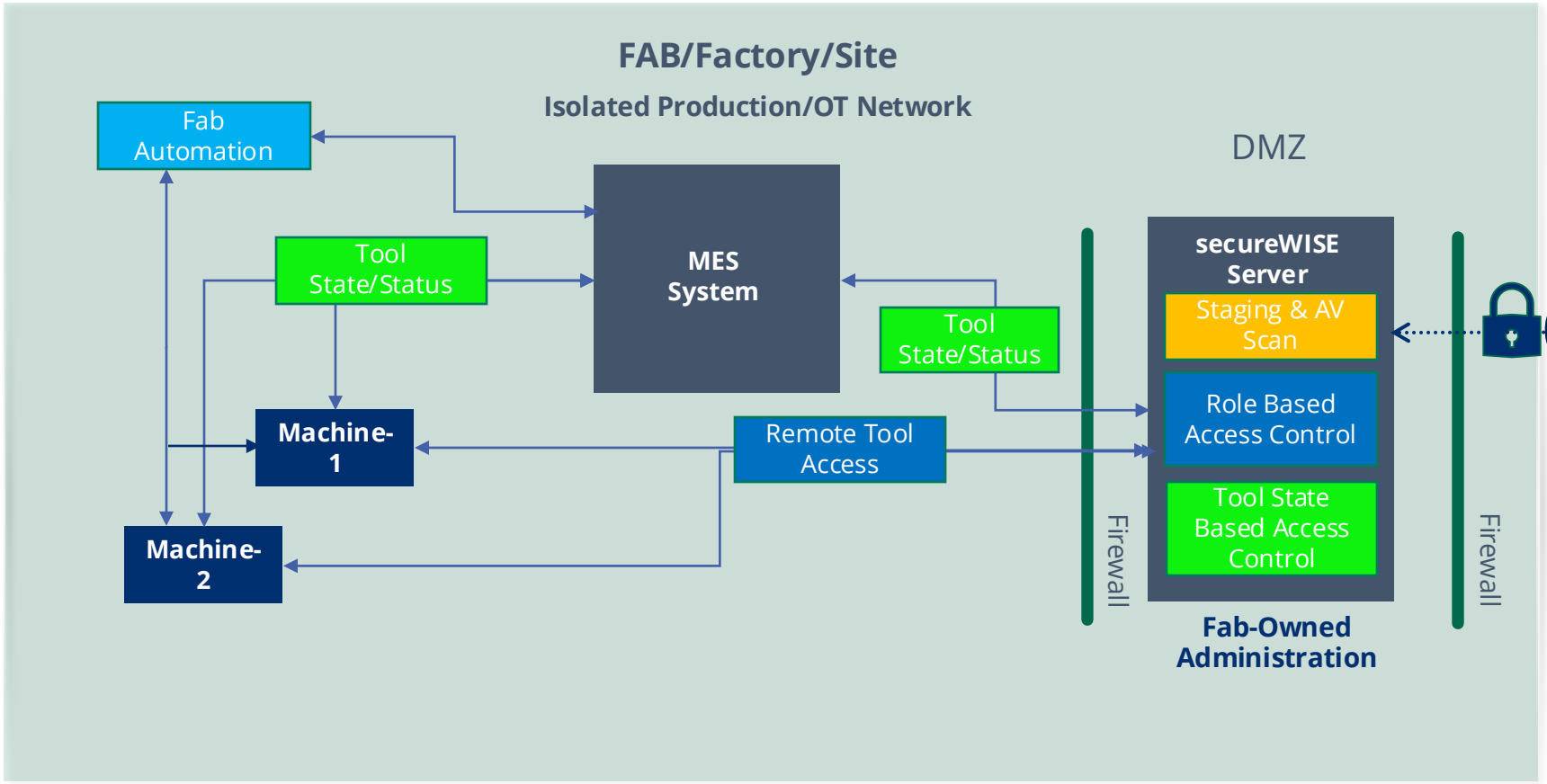
Secure Private Cloud - Design for Yield Applications



Connectivity Legend	
⟷	Standard Services: TLS or Unencrypted FTP, VNC (RTO), SSH (RAA), HTTPS, RDP
⟷	Collaborative Client Connection (minimum TLS V1.2 encryption)
🔒	IP-SEC VPN Peer Device
▭	IP-SEC VPN Tunnel (encrypted)

PDF SOLUTIONS™

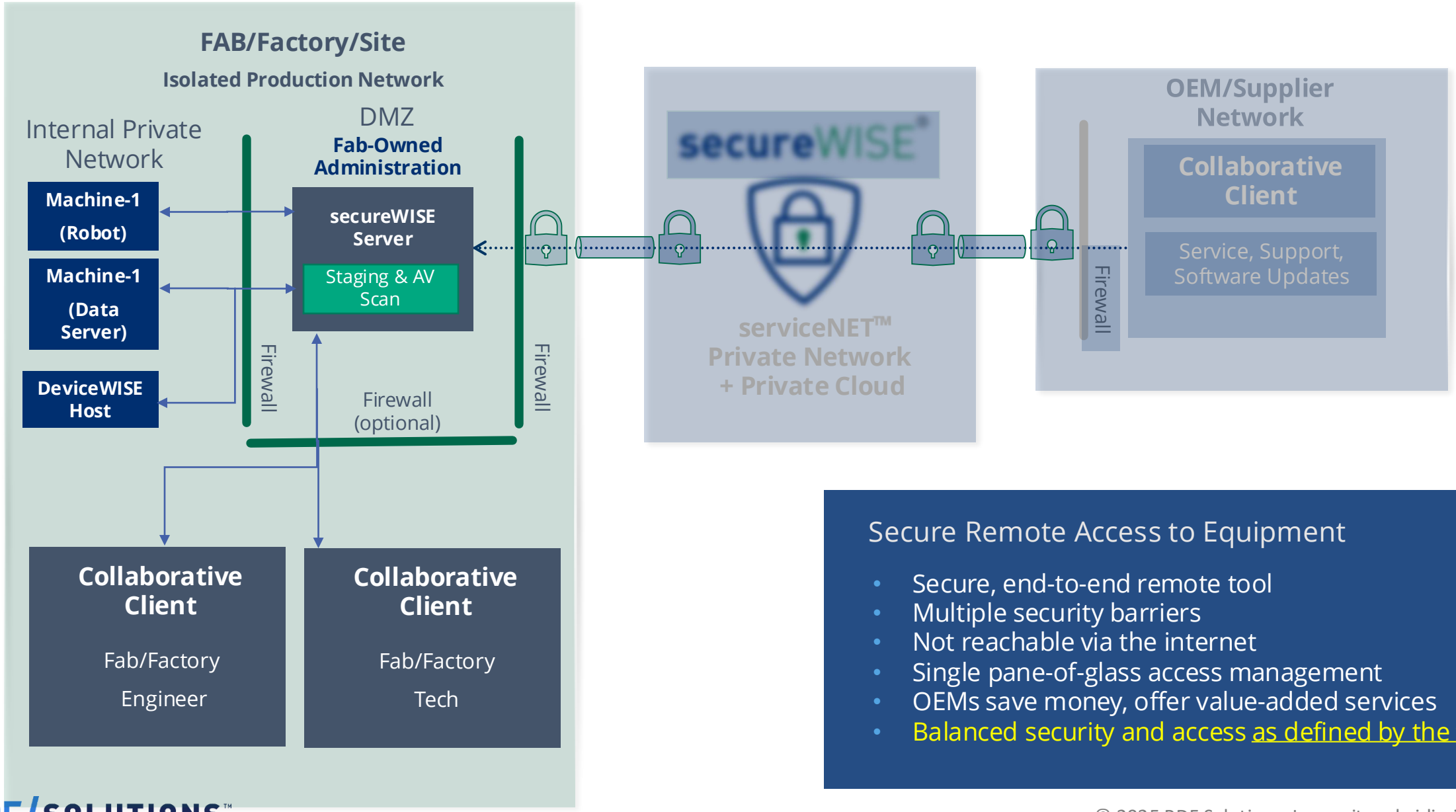
secureWISE MES Integration



Value Propositions

- All Parties: Enhanced Safety
- Fab: Intelligent control over remote tool access
- OEM: Access to tool availability data: Service/Fleet/Contract Management
- MES Supplier: Technology differentiator

secureWISE On-Prem Model



Secure Remote Access to Equipment

- Secure, end-to-end remote tool
- Multiple security barriers
- Not reachable via the internet
- Single pane-of-glass access management
- OEMs save money, offer value-added services
- Balanced security and access as defined by the fab

Case Study – secureWISE for OEMs

- A major semiconductor OEM leverages secureWISE as the backbone for global remote operations
- Real-time, secure access to tools across fabs worldwide reduces downtime and enhances efficiency
- Centralized infrastructure transforms maintenance, troubleshooting, and support while reducing costs

Centralized Control & Efficiency

- Unified access enables centralized monitoring & diagnostics
- Machine Data enables automated mediation reduces on-site interventions & accelerates resolution

Reduced Downtime & Cost Savings

- Remote troubleshooting minimizes unplanned downtime
- Reduces travel & on-site support needs for faster issue resolution

Robust Security & Compliance

- End-to-end encryption & multi-factor authentication
- Meets stringent industry security & compliance standards

PDF SOLUTIONS™

Case Study – secureWISE for FABs

A Fab can use secureWISE to connect its worldwide network of sites.
This enables real-time monitoring and control of tools and equipment, enforces virus inspections, and minimizes reliance on onsite support, reducing engineer travel, and fosters robust training programs—all while ensuring security and compliance.

This solution is implemented with an American full-service semiconductor foundry that manufactures integrated circuits in high volume. Owner of multiple 200mm and 300mm fabs with over 550 connected tools across 6 fabs around the World

Centralized Tool Monitoring & Control

- Remote access enables real-time monitoring and diagnostics across all sites.

Enhanced Cybersecurity & Compliance

- Integrated virus scans ensure equipment integrity.

Reduced Onsite Support & Travel

- Secure remote troubleshooting optimizes workforce efficiency.

Scalable, Global Collaboration

- Virtual training and centralized engineering support across regions.

Multi-Zone Engineering & Global Reach

- This fab operator manages fabs across three time zones with two centralized engineering centers.

Potential Benefits to Fabs

- Reduce reliance on onsite support through secure remote access.
- Lower travel costs while improving engineer training & knowledge transfer.
- Enable secure remote monitoring of OSAT partners for CoWoS QA.
- Optimize engineering support across global fabs while maintaining centralized expertise.

secureWISE enables multi-zone fab operations by centralizing equipment engineering and streamlining global support.

PDF Solutions Acquisition of secureWISE

Industry Context

- The semiconductor industry becomes more globally distributed
- Advanced devices rely on the integration of multiple chiplets into a single package
- As a result, more collaboration and integration are required across the semiconductor industry
- Data infrastructure and analytics are critical enabling technologies for improved integration and collaboration

PDF Solutions Leadership

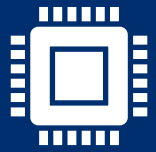
- For over 30 years, PDF Solutions has provided advanced analytics, unique data and secured data infrastructure to the semiconductor ecosystem
- Its data platform empowers companies in the semiconductor ecosystem to break down data silos within their supply chains, enabling them to leverage all their manufacturing and test data, resulting in key performance indicator (KPI) improvements
- With its DEXnetwork PDF Solutions provides the execution backbone for the outsourced semiconductor supply chain

With the acquisition of secureWISE, PDF Solutions expects to dramatically expand manufacturing equipment providers' and fab operators' remote access to securely exchange data with, optimize and control their equipment and processes.

secureWISE adds to PDF Solutions' Analytics Platform

Acceleration of equipment makers' ability to derive value from their equipment data

Expansion of PDF Solutions' secure DEX OSAT network



Expansion of a data collection, remote access, and AI/ML model execution platform

Positions PDF Solutions to address increasing semiconductor ecosystem complexity

With secureWISE, the PDF Solutions platform will help members of the semiconductor ecosystem collaborate through a secure, direct connection and control manufacturing process down to the production equipment.

Certifications and IP

Certifications

- SySS Penetration Test White-hat hacking test
- Fab penetration tests
- ISO 27001:2022 Certification

NSF ISR Certificate of Registration

This certifies that the Information Security Management System of

secureWISE LLC
750 Park of Commerce Blvd., Suite 100
Boca Raton, Florida, 33487, United States

has been assessed by NSF-ISR and found to be in conformance to the following standard(s):

ISO 27001:2022

Scope of Certification:
The Scope of registration encompasses key processes and activities critical to ensuring the Confidentiality, Availability, and Integrity of the data transported in the secureWISE platform, including Research and Development activities that support innovation and continuous improvement. These processes form part of the operations of secureWISE, LLC, in accordance with the statement of applicability.

Statement of Applicability (SOA): 11/15/2024 Version 2.0

Sameer Vachani
Senior Director, NSF-ISR

Certificate Number:	C0286766-IM4
Certificate Decision Date:	20-JAN-2025
Certificate Issue Date:	20-JAN-2025
Cycle Effective Date:	28-DEC-2022
Certificate Expiration Date*:	27-DEC-2025

Issued by:
NSF International Strategic Registrations (NSF-ISR)
789 N. Dixboro Road, Ann Arbor, MI 48105 USA

Authorized Certification and/or Accreditation Marks. This certificate is property of NSF-ISR and must be returned upon request.

*Company is audited for conformance at regular intervals. To verify certification call (888) NSF-9000 or visit our web site at www.nsf-isr.org

ANAB ANSI National Accreditation Board ACCREDITED ISO/IEC 17021-1 MANAGEMENT SYSTEMS CERTIFICATION BODY

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

Certification Roadmap

- FIPS 140-3 (US/Canada Gov Cert)
- NAIP (NSA Cybersecurity Cert)
- HIPAA Seal of Compliance (Healthcare)

SySS THE PENTEST EXPERTS.

CERTIFICATE

SySS GmbH
72072 Tübingen

herewith confirms to have performed a penetration test at the company

Telit IoT Platforms, LLC
33487 Boca Raton

Test Object:

A test instance of the service "secureWISE" was analyzed for security vulnerabilities. The tested software version was 4.0.1.0. In the course of the test, security scanners and manual attacking techniques in accordance with the "OWASP Top Ten" were put to use.

Summary of Test Results:

The SySS GmbH attests that the service "secureWISE" has a very high security level. Above all, during the tests it was not possible to access any confidential company data.

Certificate Number	DS-290916-001
Date of Test (Last Day of Test)	September 29th, 2016
Valid until / Next Test Required	September 2017

Tübingen, 29.09.2016

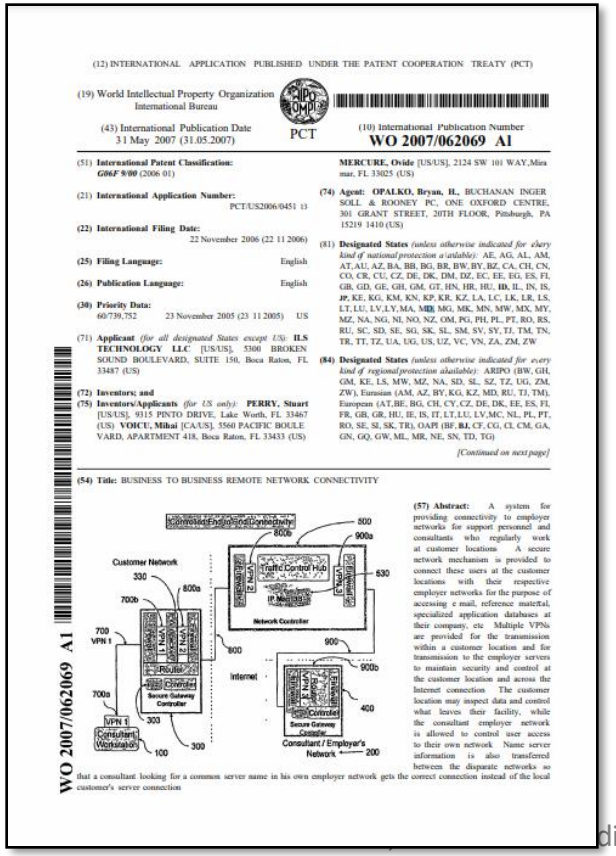
Sebastian Schreiber
(CEO)

Klaus Eisentraut
(IT-Security Consultant)

Patent

Business to Business Remote Network Connectivity patent

- Intl' publication number: WO 2007/062069 Al
- International filing date: 22 Nov 2006



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 May 2007 (31.05.2007)

PCT

(10) International Publication Number
WO 2007/062069 A1

(51) **International Patent Classification:**
G06F 9/00 (2006.01)

(21) **International Application Number:**
PCT/US2006/045113

(22) **International Filing Date:**
22 November 2006 (22.11.2006)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
60/739,752 23 November 2005 (23.11.2005) US

(71) **Applicant** *(for all designated States except US)*: **ILS TECHNOLOGY LLC** [US/US]; 5300 BROKEN SOUND BOULEVARD, SUITE 150, Boca Raton, FL 33487 (US)

(72) **Inventors; and**

(75) **Inventors/Applicants** *(for US only)*: **PERRY, Stuart** [US/US]; 9315 PINTO DRIVE, Lake Worth, FL 33467 (US). **VOICU, Mihai** [CA/US]; 5560 PACIFIC BOULEVARD, APARTMENT 418, Boca Raton, FL 33433 (US)

MERCURE, Ovide [US/US], 2124 SW 101 WAY, Miramar, FL 33025 (US)

(74) **Agent: OPALKO, Bryan, H.**, BUCHANAN INGERSOLL & ROONEY PC, ONE OXFORD CENTRE, 301 GRANT STREET, 20TH FLOOR, Pittsburgh, PA 15219 1410 (US)

(81) **Designated States** *(unless otherwise indicated for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW

(84) **Designated States** *(unless otherwise indicated for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

[Continued on next page]

(54) **Title:** BUSINESS TO BUSINESS REMOTE NETWORK CONNECTIVITY

(57) **Abstract:** A system for providing connectivity to employer networks for support personnel and consultants who regularly work at customer locations. A secure network mechanism is provided to connect these users at the customer locations with their respective employer networks for the purpose of accessing e mail, reference material, specialized application databases at their company, etc. Multiple VPNs are provided for the transmission within a customer location and for transmission to the employer servers to maintain security and control at the customer location and across the Internet connection. The customer location may inspect data and control what leaves their facility, while the consultant employer network is allowed to control user access to their own network. Name server information is also transferred between the disparate networks so that a consultant looking for a common server name in his own employer network gets the correct connection instead of the local customer's server connection

WO 2007/062069 A1

PDF/SOLUTIONS™

+

secureWISE®

Thank You

PDF/SOLUTIONS™


pdf-solutions


pdfsolutionsinc


pdfs.inc


pdf_solutions


pdfs_cn