Prodapt powering global telecom

Achieve security objectives at speed with automated vulnerability assignment

Reduce time taken to fix security vulnerabilities by 50% with vulnerability analysis best practices

Credits

Reza Nanoha

Sathya Narayanan

Rise in security vulnerabilities

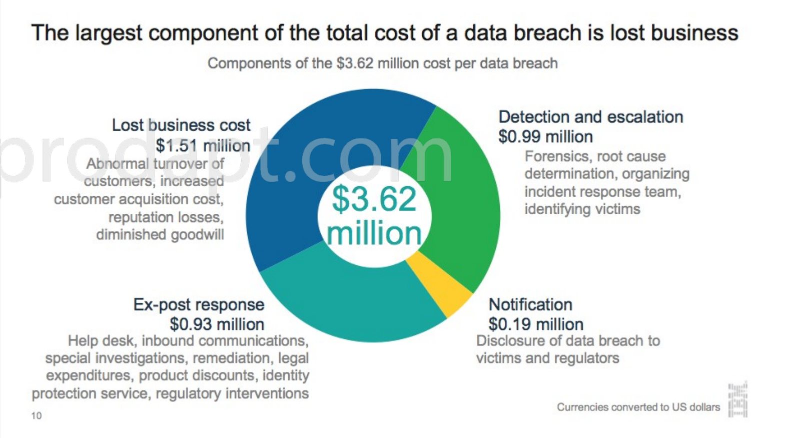
Cyber attacks against Digital Service Providers' (DSPs') critical infrastructure are soaring

In 2019,
massive telecommunication data breach
was linked to Chinese hackers who attacked 10 DSPs, exploiting their network's vulnerabilities

GSMA's Mobile Telecommunications Security Threat Landscape report 2019
says that there was a 55% increase in breaches caused by software vulnerabilities.

Addressing security vulnerabilities is a top priority for DSPs, because a successful cyber attack could essentially cause

- Disruption in service for millions of customers
- Loss of customers' trust
- Deterioration of DSP's brand & reputation
- Regulatory non-compliances
- Shut-down of DSP's operations



The largest component of the total cost of a data breach is lost business

Components of the $3.62 million cost per data breach

Currencies converted to US dollars

Source: 'Cost of a data breach study by Ponemon'

OCCRP report says "telecom fraud is a fast growing field of criminal activity and costing today's world some US $32.7 billion annually."

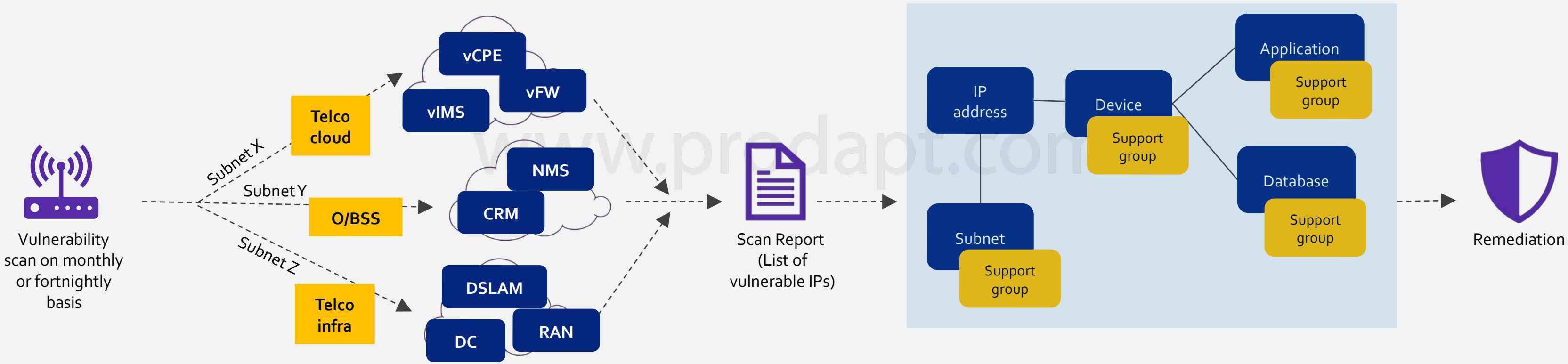
Addressing these threats will require DSPs to establish a systematic process for vulnerability management with high levels of automation. This includes discovering new vulnerabilities, performing risk assessment and **assigning the vulnerabilities to the appropriate support group** to facilitate quicker remediation.

Vulnerability management involves vulnerability scanning & assigning the identified vulnerabilities to the appropriate support groups for remediation

DSPs on an average have 100,000+ ports, nodes and thousands of software applications in different versions in their infrastructure. Getting such a complex ecosystem secure and establishing a systematic vulnerability management process is a mounting concern.

Vulnerability scanning

Vulnerability analysis, assignment & remediation



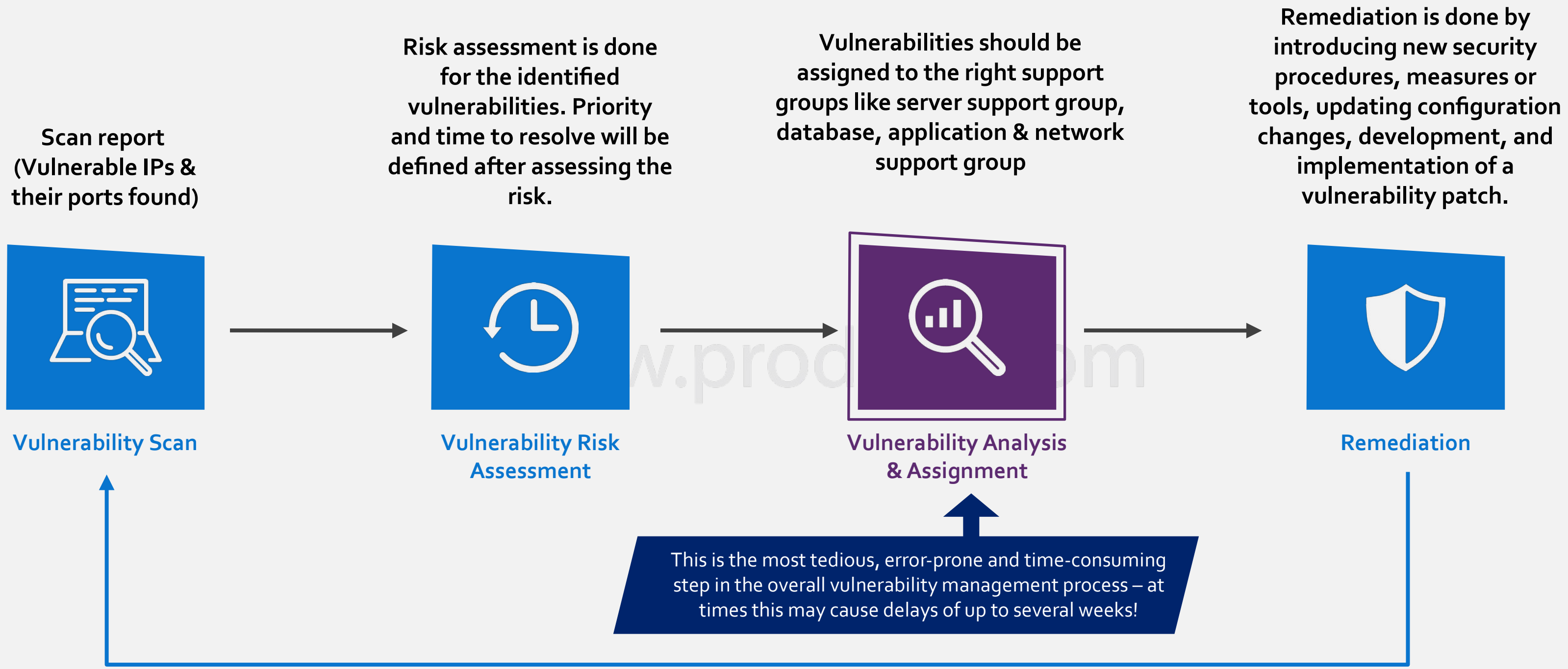
Vulnerability scanning in DSP's ecosystem involves scanning various subnets – telecom cloud, OSS/BSS, telecom infra. Once the scanning is complete, report will be sent for risk analysis & vulnerability assignment

Vulnerability assignment involves assigning the vulnerabilities to the appropriate support group, so that they can work on remediation. There might be different support group such as device, application, database and server support group .

vFW	Virtual Firewall	vIMS	Virtual IMS	CRM	Customer Relationship Management
vCPE	Virtual CPE	NMS	Network Management System	RAN	Radio Access Network

The most cumbersome task in vulnerability management is analysis & assignment

With manual administration, more than 70% of the vulnerabilities get assigned to the wrong support group



Scan report (Vulnerable IPs & their ports found)

Risk assessment is done for the identified vulnerabilities. Priority and time to resolve will be defined after assessing the risk.

Vulnerabilities should be assigned to the right support groups like server support group, database, application & network support group

Remediation is done by introducing new security procedures, measures or tools, updating configuration changes, development, and implementation of a vulnerability patch.

Vulnerability Scan
Vulnerability Risk Assessment
Vulnerability Analysis & Assignment
Remediation

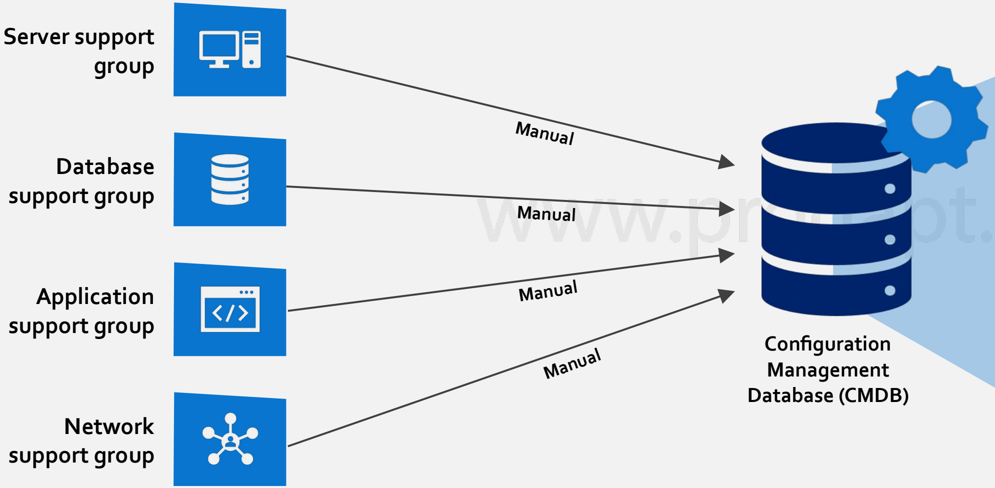
This is the most tedious, error-prone and time-consuming step in the overall vulnerability management process – at times this may cause delays of up to several weeks!

DSPs on an average have 400,000+ configuration items (CI's) in their infrastructure and 80,000+ vulnerabilities getting identified in the scan. All these vulnerabilities need to be assigned to the appropriate support group to work on remediation. By manual analysis & assignment, close to 70% of vulnerabilities are assigned to wrong support group. Hence, the lead time significantly increases due to this bottleneck.

Why is vulnerability assignment process so complex?

Large number of attributes & relationships administered manually in configuration management database (CMDB)

The support groups manually administer all the attributes and the required relationship between them for all the CIs. This leads to incompleteness in attributes data, inaccuracies in the mapping of relationship between attributes or sometimes the data is simply not updated



Server support group

Database support group

Application support group

Network support group

Manual

Manual

Manual

Manual

Configuration Management Database (CMDB)

Required Attributes
The support groups will enter all the attributes required in CMDB such as IP Subnets (CIDR), Space ID, network domain, interface port, etc.

Required Relations
The support groups will also provide relationships such as

- Device – Hypervisor relation
- Hypervisor – Support group relation
- IT application(s) – OS platform relation(s), etc.

The inaccuracies in the mapping of the relationship between attributes exponentially increases the complexity, as one wrong mapping can lead to hundreds of vulnerabilities assigned to wrong support groups.

Solution approach to ensure all the attributes & relationships are appropriately mapped in CMDB, thereby ensuring a seamless and automated vulnerability management process flow

1 2 3

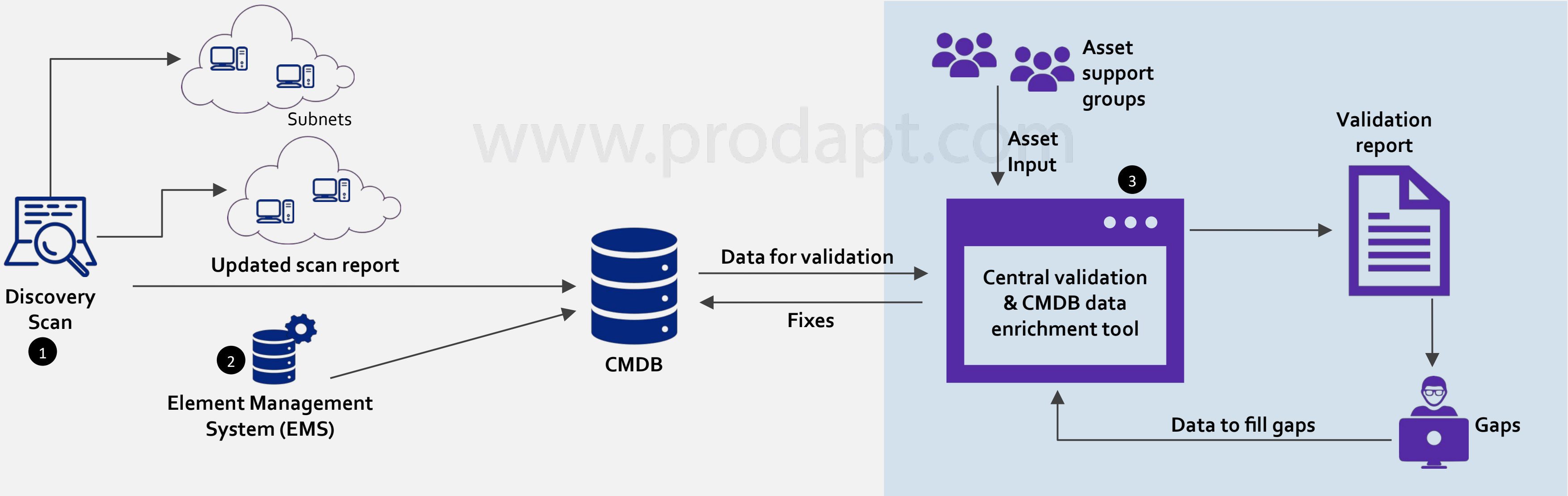
Automated asset & configuration management

Tool-based asset & configuration management validation

Automated scanning and collection of attributes & relationships and updating them in CMDB

Multi-vendor EMS system integration with CMDB- auto updating of provisioning information

Central validation & CMDB data enrichment tool - aids in automated validation of attributes & relationships in CMDB

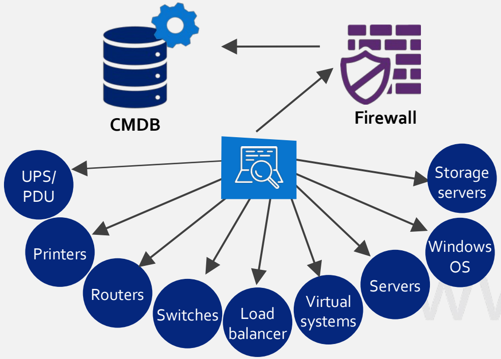


Enables automation of vulnerability assignment process

Reduction in wrong assignments in vulnerability assignment process

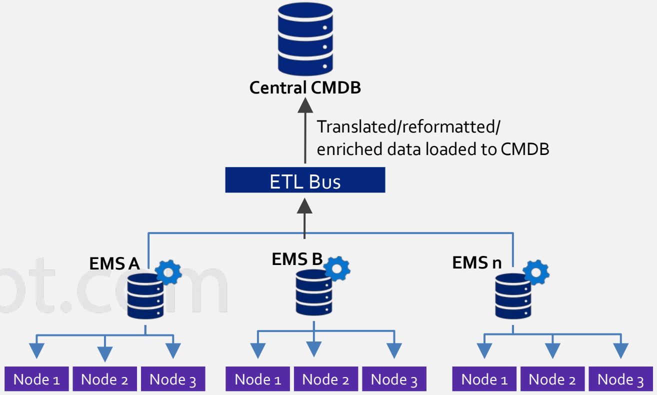
Discovery scan process & element management system integration with CMDB is crucial but not sufficient

Discovery Scan



- Discovery tooling needs to be deployed in the subnets and scanned on a fortnightly basis, to fill the gaps or correct any incorrect information in CMDB
- Agent-based (such as Pressler PRTG) or agent-less (using SNMP, WMI, CIM protocols) discovery tooling can aid in keeping the CMDB up-to-date without requiring user interaction
- Quick discovery of attributes and their relationships (less than 15 minutes)
- Discovery tool keeps track of attributes which are relevant for the vulnerability management process such as IP addresses, subnets, OS, installed software, and the relationship between assets

Element Management System (EMS)

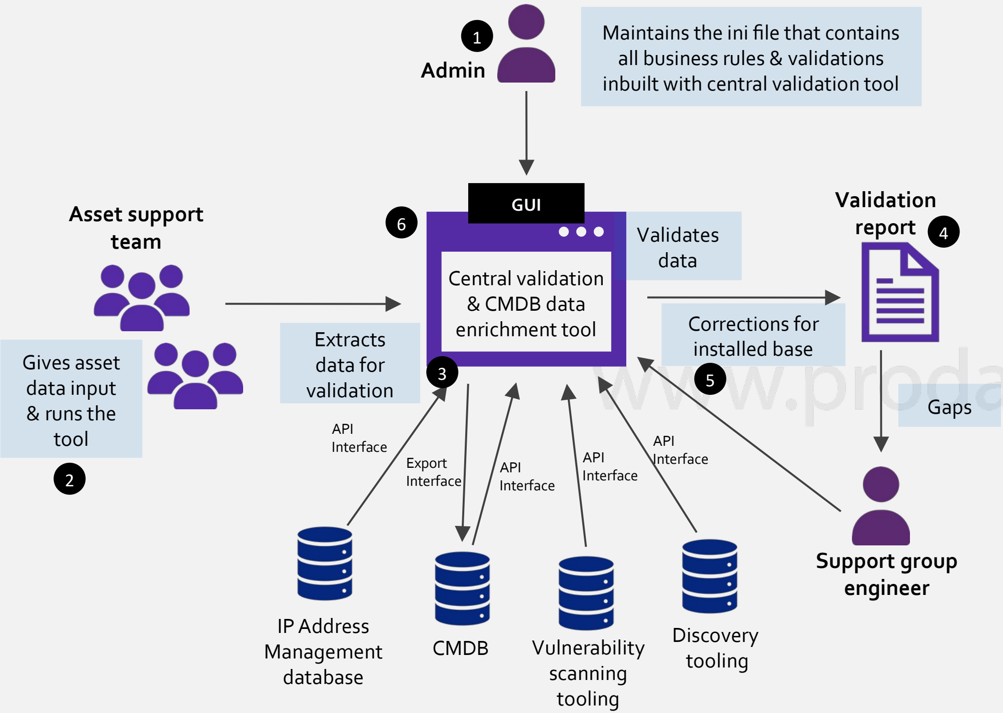


- Multi-vendor element management systems need to be integrated with central CMDB & integration is established through ETL bus, which translates/reformats/enriches the data from EMS systems
- Re-usable & customizable adaptors are deployed to enable faster integration
- With this integration, any change (provisioning or decommissioning) of nodes will be automatically updated in the central CMDB

The discovery tool and EMS integration to automate CMDB requirements are neither simple nor comprehensive. It uses external probes and scanners which could lead to incomplete asset data and creates a never-ending battle with aging data. This incomplete data creates issues in vulnerability assignment. Therefore, a data validation & enrichment tool is needed to ensure all the required attributes & relationships are present for seamless vulnerability assignment.

Central validation & data enrichment tool framework to find gaps in databases and fix them to ensure attributes & relationship data are correct

1 2 3


1
Admin
Maintains the ini file that contains all business rules & validations inbuilt with central validation tool
GUI
6
Central validation & CMDB data enrichment tool
Validates data
Validation report
4
Asset support team
Gives asset data input & runs the tool
2
Extracts data for validation
3
Corrections for installed base
5
Gaps
API Interface
Export Interface
API Interface
API Interface
API Interface
Support group engineer
IP Address Management database
CMDB
Vulnerability scanning tooling
Discovery tooling

1. **Admin creates/manages the customizable validation rule set**
2. **Asset support team runs the central validation & CMDB data enrichment tool**
3. **Central validation & CMDB data enrichment tool extracts the data from various databases and validates them on business rules**
4. **Gaps are identified in all the databases and validation report gets published with the asset support group that is responsible for fixing the gaps**
5. **Support group engineers from each asset support team work on fixing the gaps and send it to the respective databases through the central validation tool**
6. **The validation happens after fixing gaps to ensure there are no more gaps in databases**

The central validation tool incorporated with business rules and validation ensures that no data leakage or data mismatch happens in CMDB, ensuring a seamless vulnerability assignment once the vulnerable IPs and ports are identified through scans.

Key capabilities to be built on central validation & enrichment tool

Capability on validation rule set

Tool should provide prebuilt validation rule set.
Sample validation rule set

- Rule 1: Validate if servers are virtual or physical?
- Rule 2: Location information for physical servers added?
- Rule 3: Data center & relevant support group mapping done?
- Rule 4: Databases are not linked to a server?
- Rule n: Subnets related to the IP-addresses configured servers - are they registered in IPAM?

Flexibility to easily customize rules, add/delete rules

Other key capabilities

- Identifying gaps in vulnerability scanning and discovery scanning to improve coverage
- Identifying inaccuracies in the relationship between configuration items
- Identifying missing attributes such as IP addresses, network devices, servers, etc.
- Identifying inaccuracies in attributes relevant for vulnerability management (lifecycle status, DTAP pipeline, scanner zone, scan exclusions, etc.)
- Identifying inaccuracies in manual administration (e.g. support group data, missing IP subnets data, & incorrect interface port)

Key benefits of central validation & CMDB data enrichment tool

Increased vulnerability scan & discovery scan coverage by **40%**

Improved accuracy of first-time-right assignment of vulnerabilities by **23%**

Reduced average workload of security operations center (SOC) engineers by **30%**

Results achieved by a leading DSP in Latin America by leveraging the

The validation tool had 67 different business rules & validations to validate if the CMDB contains all the required attributes & relationships

Key Benefits

Implementing automated asset & configuration management framework discussed in this insight, resulted in the following benefits.

Vulnerability assignment time **improved by 80%**

Total lead time of vulnerability management process **improved by 50%**

Critical vulnerabilities that required immediate action could be **remediated within the SLA**

CMDB administration complexity reduced and attributes & relationship **data accuracy improved**

Vulnerability analysis & assignment process

	Before solution implementation	After solution implementation
% of correct assignment to the support group	25-30%	60-75%
Average lead time for assignment process	2-3 weeks	2-3 days
Total lead time of vulnerability management process	4-5 weeks	2-3 weeks

Get in touch

USA

Prodapt North America
Tualatin: 7565 SW Mohawk St.,
Phone: +1 503 636 3737

Dallas: 222 W. Las Colinas Blvd., Irving
Phone: +1 972 201 9009

New York: 1 Bridge Street, Irvington
Phone: +1 646 403 8158

CANADA

Prodapt Canada Inc.
Vancouver: 777, Hornby Street,
Suite 600, BC V6Z 1S4

UK

Prodapt (UK) Limited
Reading: Davidson House,
The Forbury, RG1 3EU
Phone: +44 (0) 11 8900 1068

EUROPE

Prodapt Solutions Europe
Amsterdam: Zekeringstraat 17A, 1014 BM
Phone: +31 (0) 20 4895711

Prodapt Consulting BV
Rijswijk: De Bruyn Kopsstraat 14
Phone: +31 (0) 70 4140722

Prodapt Germany GmbH
Aschheim: Sonnenstraße 31, 85609
Germany

SOUTH AFRICA

Prodapt SA (Pty) Ltd.
Johannesburg: No. 3,
3rd Avenue, Rivonia
Phone: +27 (0) 11 259 4000

INDIA

Prodapt Solutions Pvt. Ltd.
Chennai: Prince Infocity II, OMR
Phone: +91 44 4903 3000

“Chennai One” SEZ, Thoraipakkam
Phone: +91 44 4230 2300

Bangalore: “CareerNet Campus”
2nd floor, No. 53, Devarabisana Halli,
Phone: +91 44 4903 3000

THANK YOU!

insights@prodapt.com | www.prodapt.com

Prodapt powering global telecom