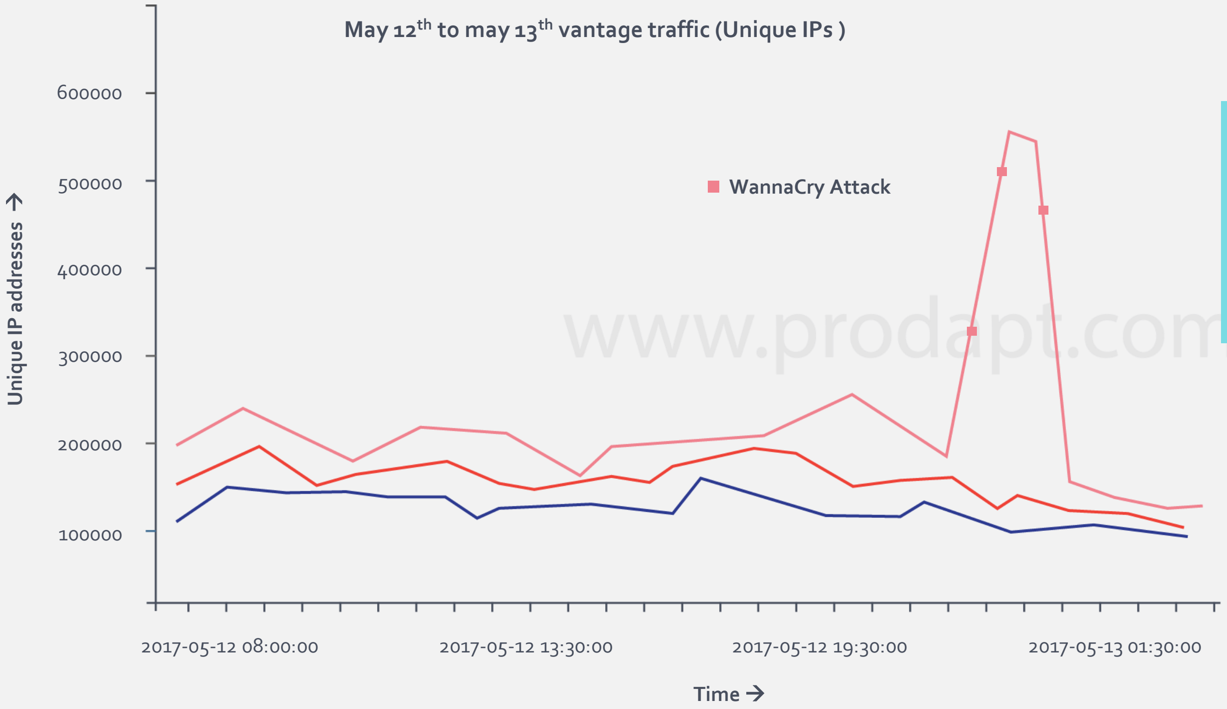
Prodapt powering global telecom

Staying ahead of Security Threats

Credits | Balaji T N | Rajeshkhanna J | Mogan AB

Major security issues tend to occur rarely, but the volume of impact disrupts normal business operations

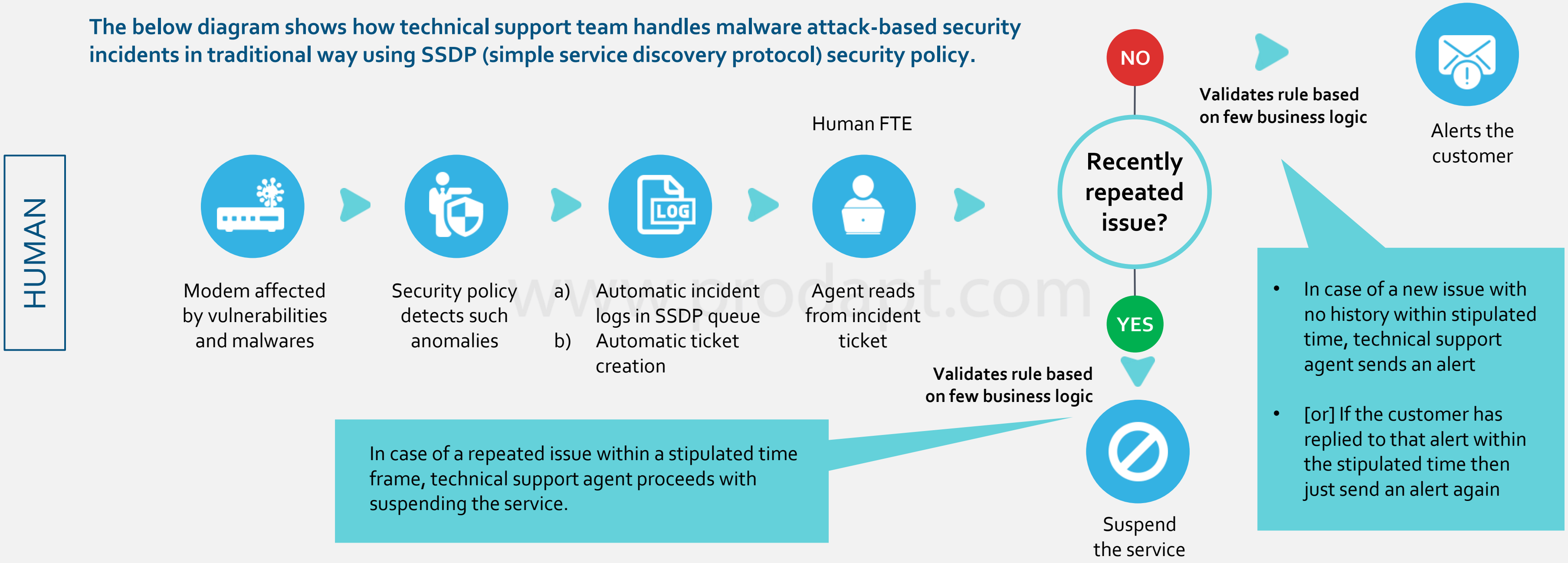


Security teams which typically tend to be smaller in size, are not equipped to handle the high volume of incidents when a major crash down occurs. The graph shows the sudden spike in the number of unique IPs affected during the 48 hrs of WannaCry virus attack.

Low frequency, high volume security threats are difficult to deal with due to bandwidth constraint

How DSPs’ business processes are handling the security threats using traditional methods

The below diagram shows how technical support team handles malware attack-based security incidents in traditional way using SSDP (simple service discovery protocol) security policy.



HUMAN
Modem affected by vulnerabilities and malwares
Security policy detects such anomalies
a) Automatic incident logs in SSDP queue
b) Automatic ticket creation
Human FTE
Agent reads from incident ticket
Recently repeated issue?
NO
Validates rule based on few business logic
Alerts the customer
YES
Validates rule based on few business logic
Suspend the service

In case of a repeated issue within a stipulated time frame, technical support agent proceeds with suspending the service.

- In case of a new issue with no history within stipulated time, technical support agent sends an alert
- [or] If the customer has replied to that alert within the stipulated time then just send an alert again

Usually, a small core team is assigned to deal with security incidents during regular operations. Once low frequency & high volume security threat occurs, business operations get disrupted. These sudden incidents require immediate action.

Common challenges with technical support agent in analyzing & fixing tickets

1 **Bandwidth issue**

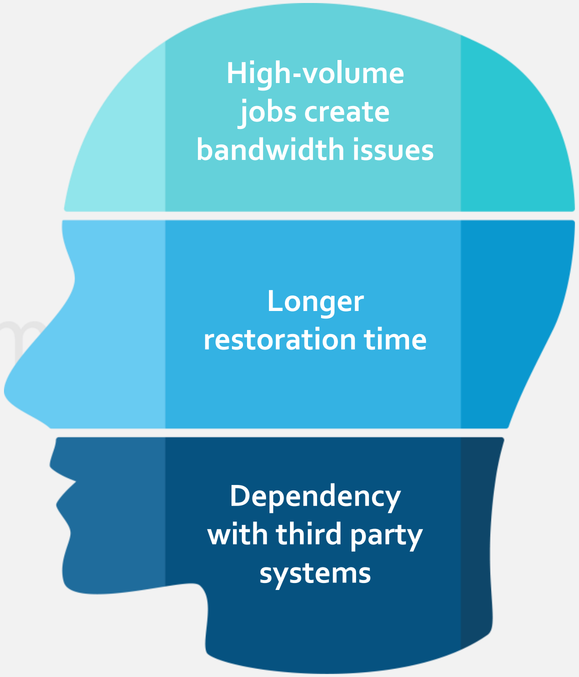
Unexpected volume of cyber-attacks make it almost impossible for the technical support agent to use manual threat analysis techniques to keep up with a rapidly changing threat landscape.

2 **Timing issue**

After the root-cause identification, the recovery process still takes time as it involves humans in different steps from ticket allocation phase to pre-diagnosis and restoration phase. Because of inefficient handling process in traditional method, it takes longer time for restoration.

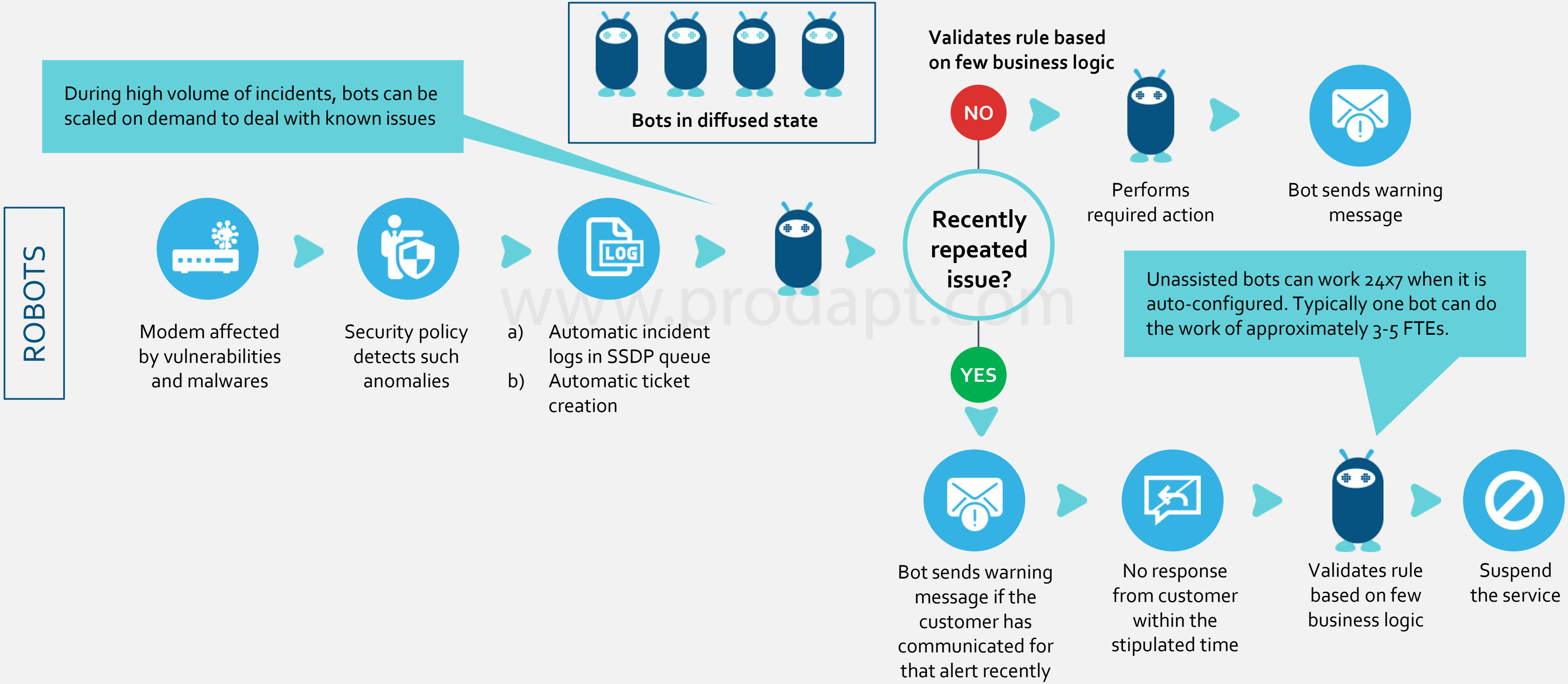
3 **Higher risk**

During the restoration phase, the agent performs multiple interactive tasks with many integrated third-party systems like planning and network system, provisioning and activation system. This increases the risk of impact on other systems.


High-volume jobs create bandwidth issues
Longer restoration time
Dependency with third party systems

By leveraging RPA capabilities, it’s possible to automate mundane, repeated, rule-based security operations to provide support agents with better access to information and enable smarter and faster decision making.

Security bots can be scaled as required during major security incidents



During high volume of incidents, bots can be scaled on demand to deal with known issues

Bots in diffused state

ROBOTS

Modem affected by vulnerabilities and malwares

Security policy detects such anomalies

a) Automatic incident logs in SSDP queue
b) Automatic ticket creation

Recently repeated issue?

Validates rule based on few business logic

NO

Performs required action

Bot sends warning message

Unassisted bots can work 24x7 when it is auto-configured. Typically one bot can do the work of approximately 3-5 FTEs.

YES

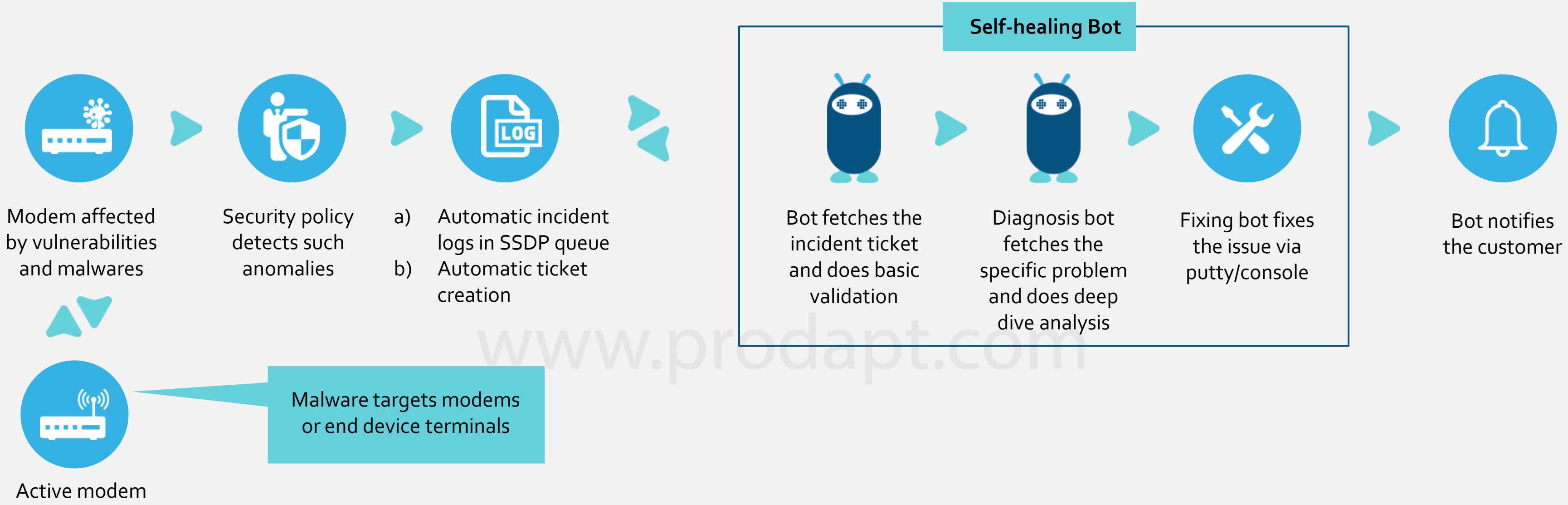
Bot sends warning message if the customer has communicated for that alert recently

No response from customer within the stipulated time

Validates rule based on few business logic

Suspend the service

Unassisted bots can be further augmented with advanced capabilities to help in self-healing process



Modem affected by vulnerabilities and malwares

Security policy detects such anomalies

a) Automatic incident logs in SSDP queue
b) Automatic ticket creation

Self-healing Bot

Bot fetches the incident ticket and does basic validation

Diagnosis bot fetches the specific problem and does deep dive analysis

Fixing bot fixes the issue via putty/console

Bot notifies the customer

Active modem

Malware targets modems or end device terminals

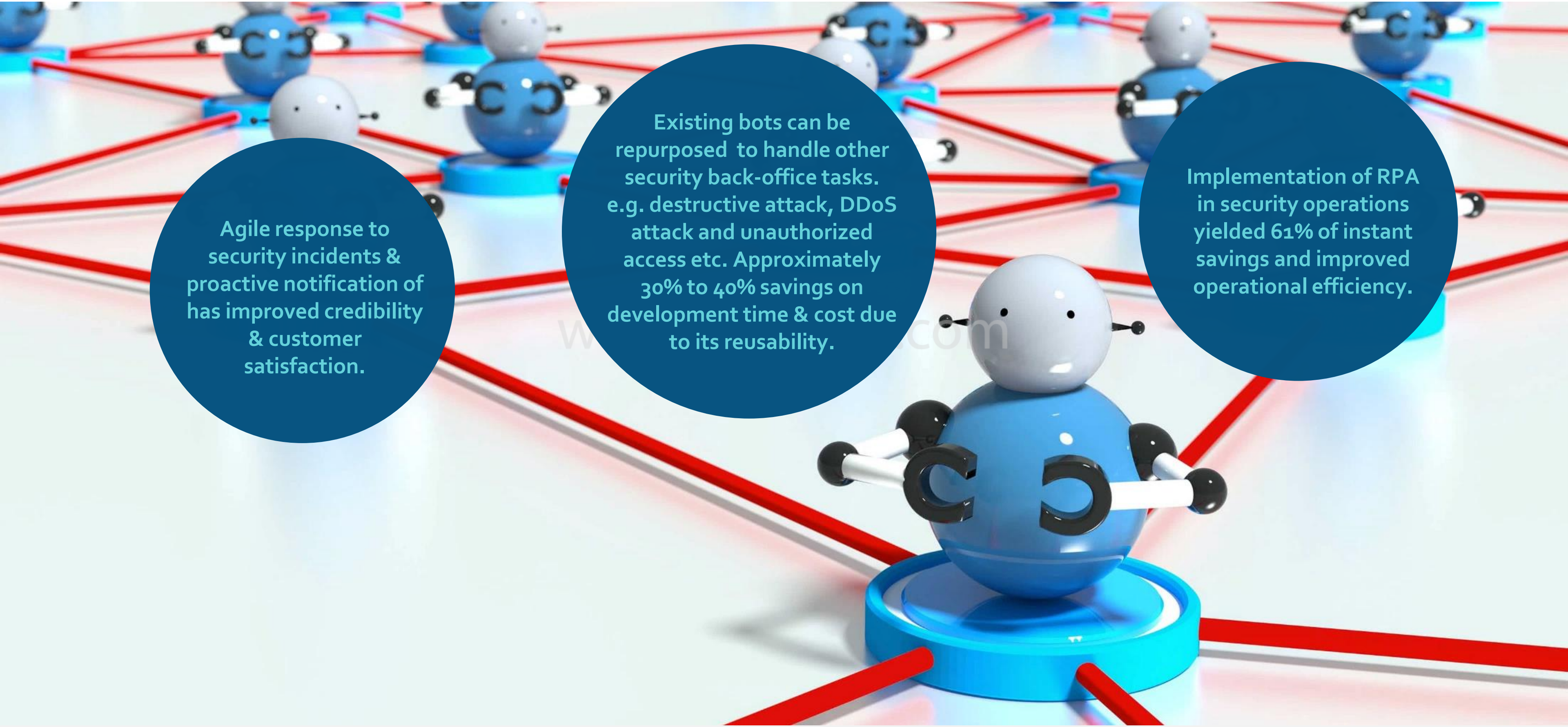
Activity 1: Deep dive analysis
After performing deep dive analysis for the specific problem, ***Diagnosis BOT*** runs audit process to understand the impact of infection using auto-regression functionality.

Activity 2: Recommended action
Based on the analysis, it gives recommended activities from preloaded repository. The repository has various templates with quick fix scripts. It will map the checklist with identical problem in known, repeated & common issue list.

Activity 3: Transfer the control
After generating a quick fix action scripts to fix a specific issue, it shares the execution commands with ***Fixing BOT***.

Activity 4: Fixing BOT
Fix the problem by executing specific action scripts via command windows or putty console

How RPA helped one of the leading operator in the US to achieve various benefits



Agile response to security incidents & proactive notification of has improved credibility & customer satisfaction.

Existing bots can be repurposed to handle other security back-office tasks. e.g. destructive attack, DDoS attack and unauthorized access etc. Approximately 30% to 40% savings on development time & cost due to its reusability.

Implementation of RPA in security operations yielded 61% of instant savings and improved operational efficiency.

insights@prodapt.com

THANK YOU!

Prodapt powering global telecom

USA

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

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

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

UK

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

THE NETHERLANDS

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

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

SOUTH AFRICA

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

INDIA

Prodapt Solutions Pvt. Ltd.

Chennai:
1. Prince Infocity II, OMR
Ph: +91 44 4903 3000

2. "Chennai One" SEZ, Thoraipakkam
Ph: +91 44 4230 2300

Bangalore: "CareerNet Campus"
No. 53, Devarabisana Halli,
Outer Ring Road