Securing Smart Cities Critical Infrastructure

Zero Trust Approach

Brijesh Miglani

SSE Security Strategist

EVOLUTION OF SMART CITIES

Smart City - ICCC

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY | INCIDENT MANAGEMENT | BEHAVIOUR ANALYTICS | WEB SECURITY | EMAIL SECURITY | SERVER SECURITY

HEALTH | EMERGENCY SERVICES | **APPLICATION LAYER** | Surveillance | eGovernance | Traffic Utilities

SERVERS ONPREMISE - ON PRIVATE CLOUD (IAAS/SAAS/PAAS)

NETWORK LAYER – WIRED or WIRELESS


Smart Mobility


Traffic Management & Navigation

Smart Parking


Smart Energy/Grid Management


Environmental Sensors


Smart Building

New Cyber Security Challenges

5G / Mobility Workforce

INDUSTRY 4.0
Evolution Challenges

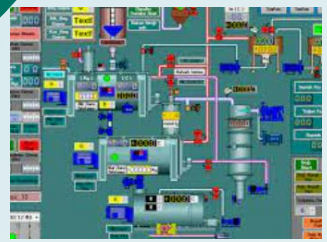
Cloud and Data

IT Security

OT Security

Emerging
Sensors & IOT

Emerging Threats
& Nation States

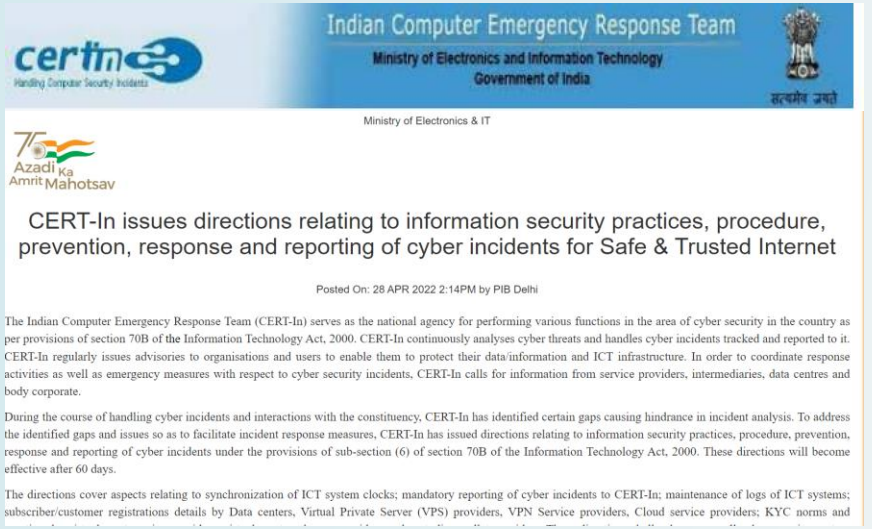


Air Gapped
SCADA
Systems

The Need for Zero Trust in Critical Infrastructure

ZTX – Across pillars

NIST ZTA Guideline



certin
Handling Computer Security Incidents

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

Ministry of Electronics & IT

Azadi Ka Amrit Mahotsav

CERT-In issues directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet

Posted On: 28 APR 2022 2:14PM by PIB Delhi

The Indian Computer Emergency Response Team (CERT-In) serves as the national agency for performing various functions in the area of cyber security in the country as per provisions of section 70B of the Information Technology Act, 2000. CERT-In continuously analyses cyber threats and handles cyber incidents tracked and reported to it. CERT-In regularly issues advisories to organisations and users to enable them to protect their data/information and ICT infrastructure. In order to coordinate response activities as well as emergency measures with respect to cyber security incidents, CERT-In calls for information from service providers, intermediaries, data centres and body corporate.

During the course of handling cyber incidents and interactions with the constituency, CERT-In has identified certain gaps causing hindrance in incident analysis. To address the identified gaps and issues so as to facilitate incident response measures, CERT-In has issued directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents under the provisions of sub-section (6) of section 70B of the Information Technology Act, 2000. These directions will become effective after 60 days.

The directions cover aspects relating to synchronization of ICT system clocks; mandatory reporting of cyber incidents to CERT-In; maintenance of logs of ICT systems; subscriber/customer registrations details by Data centers, Virtual Private Server (VPS) providers, VPN Service providers, Cloud service providers; KYC norms and

Cert-In Directions for information security

Zero Trust Maturity Model

Identity

Continuous Validation in real time for just in time, just enough access and policy enforcement

- ✓ User Activity Monitoring (UAM)
- ✓ Forcepoint ONE

Device

Constant device security **monitoring and validation**

- ✓ Forcepoint ONE
- ✓ Remote Browser Isolation

Visibility Analytics & Automation

- ✓ Forcepoint Behavioral Analytics (FBA)
- ✓ Forcepoint ONE

Network

Fully distributed ingress / egress micro-perimeters

- ✓ NextGen Firewall (NGFW)
- ✓ Cross-Domain Services
- ✓ Content Disarm and Reconstruction
- ✓ Forcepoint ONE

Application Workloads

Access is authorized continuously

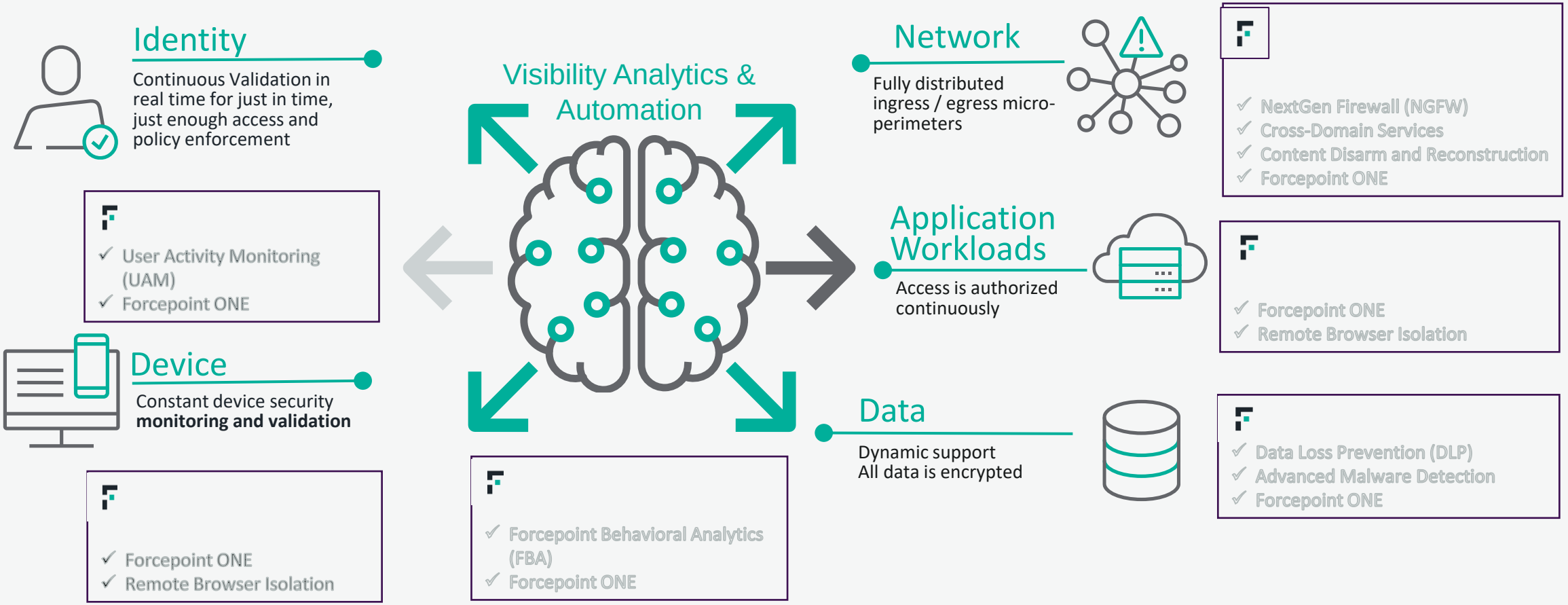
- ✓ Forcepoint ONE
- ✓ Remote Browser Isolation

Data

Dynamic support
All data is encrypted

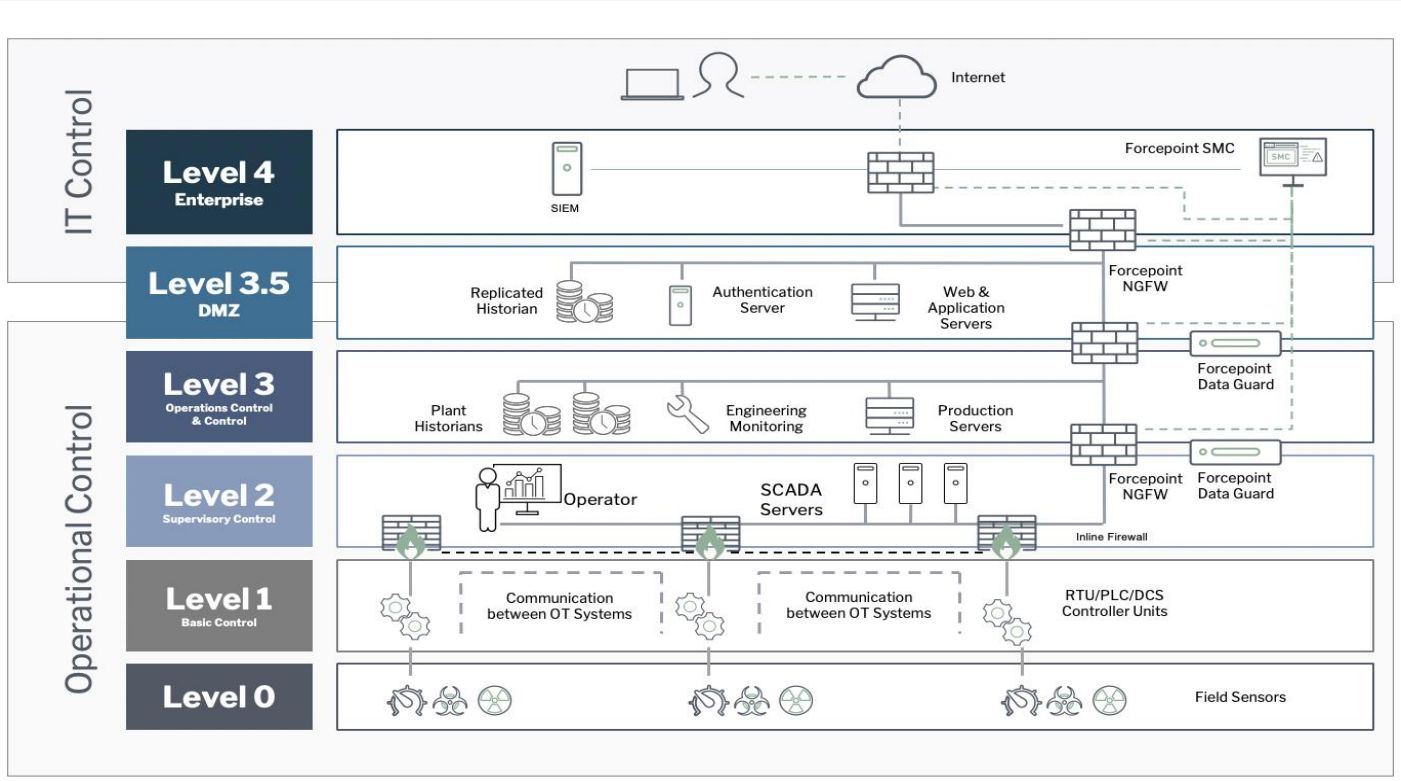
- ✓ Data Loss Prevention (DLP)
- ✓ Advanced Malware Detection
- ✓ Forcepoint ONE

Zero Trust Maturity Model – Forcepoint Portfolio



Use Cases – Critical Infrastructure

The Purdue Model



ICS-Enabled Next Generation Firewall

- DMZ – NGFW for OT/IT boundary protection
- Below the DMZ – Visibility to network traffic, zone creation
- Remote Access – Secure vendor connections

Forcepoint Data Guard

- High Assurance – Transmission of data with ability to sanitize cross-domain
- Deep Content Inspection – Ability to inspect deeply into industrial protocols

Insider Threat

- DMZ – Detailed monitoring of ICS/HMI user activity

CDR - Threat Removal

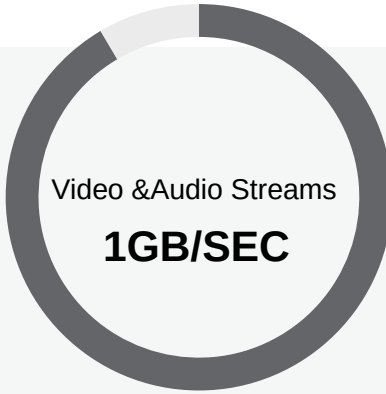
Content Disarm and Reconstruct – Zero Trust

Use Case: Video Surveillance

Business Problem & Context: Need a solution which could secure the video surveillance network by deep inspection of ONVIF messages between VMS and Cameras with end of end audit trail and logging.

Benefits

- Validate Metadata, Profiles, Sources
- Validate PTZ for Cameras



How does Video Surveillance works?

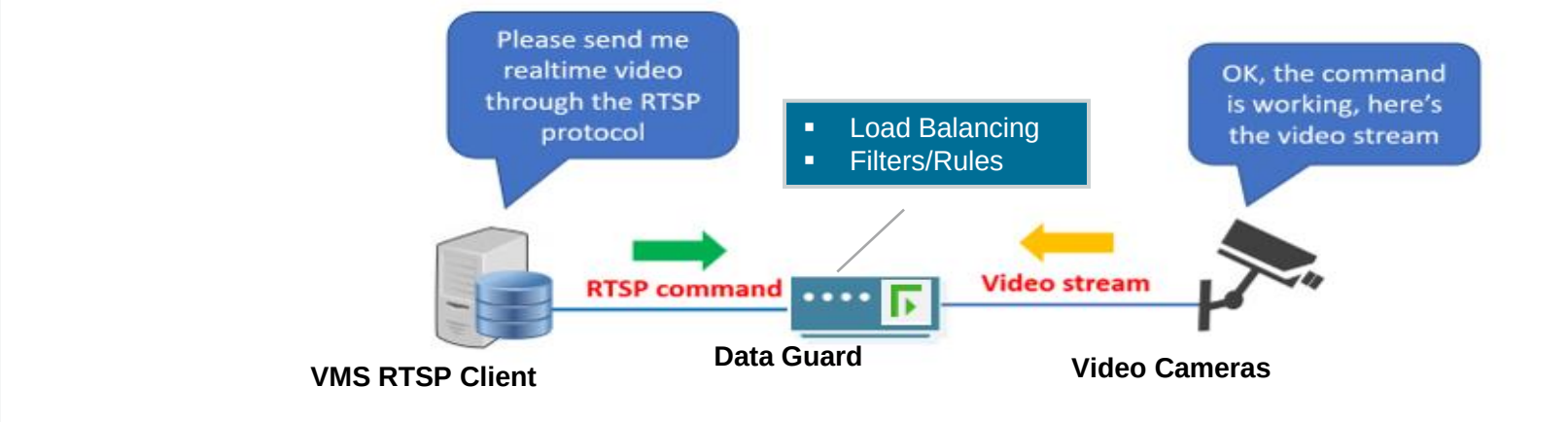
Deploy Data Guard
Data Guard, Video Adaptor

01 **Write Rules & Filters**
Customize data validation Rules & Filters through Lua or Policy Engines

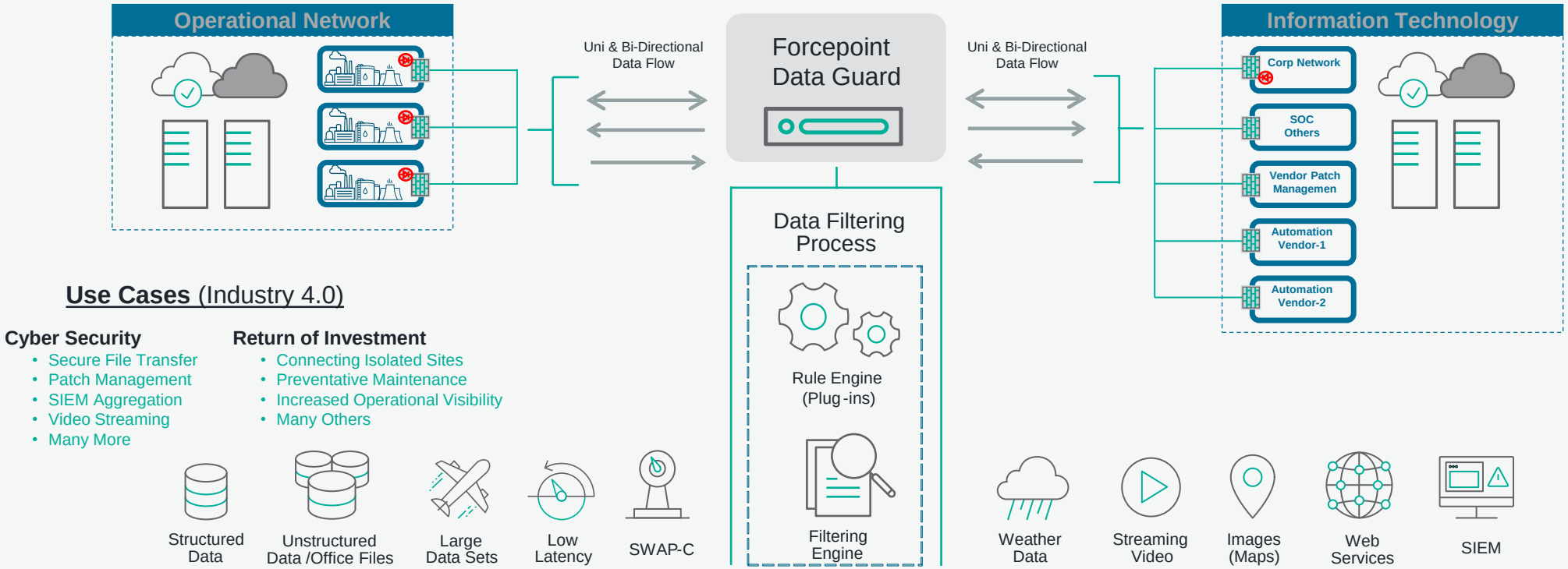
02 **Take Action**
Monitor ONVIF protocol messages

Monitor Real-time
Monitor real-time results of inspections

Solution Overview: Data Guard performs byte-level content inspection and sanitization, with customizable rules to handle even the most specialized data types and protocols before messages are exchanged between VMS and Cameras



Forcepoint Data Guard



- Addresses specific high assurance security requirements typically found in government environments
- Enhance Cyber Security, Improve Return of Investment, Optimize Processes
- Enables cyber secure bi-directional, automated movement of structured data between multiple networks
- Delivers byte-level deep content inspection, data validation and filtering
- Full customization of inspection capabilities with Policy Implementation Engine

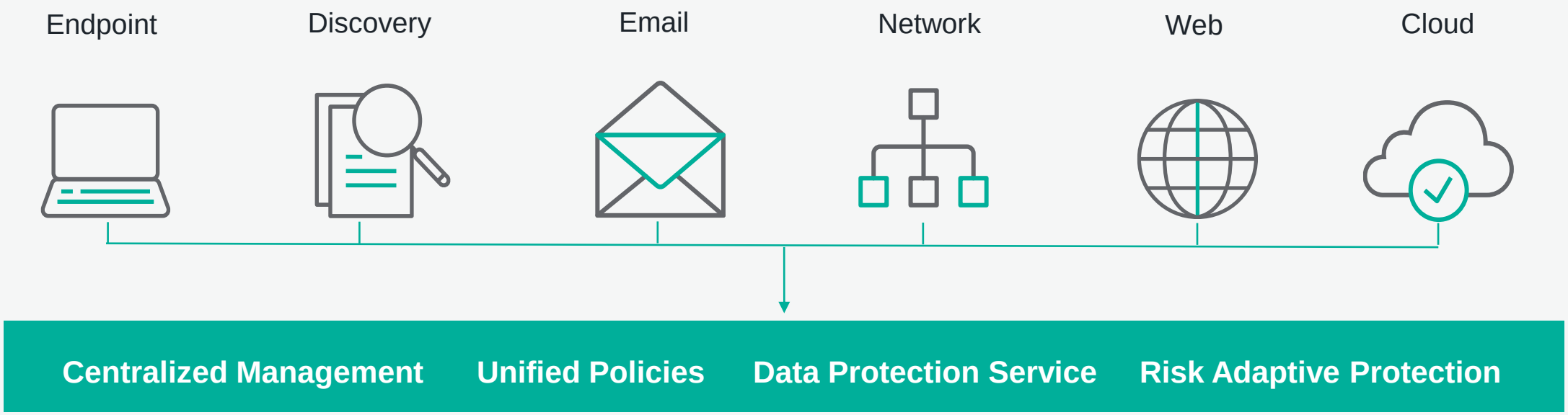
Antivirus

Sandbox

ZT CDR

IT'S TIME TO THINK DIFFERENTLY for Threat

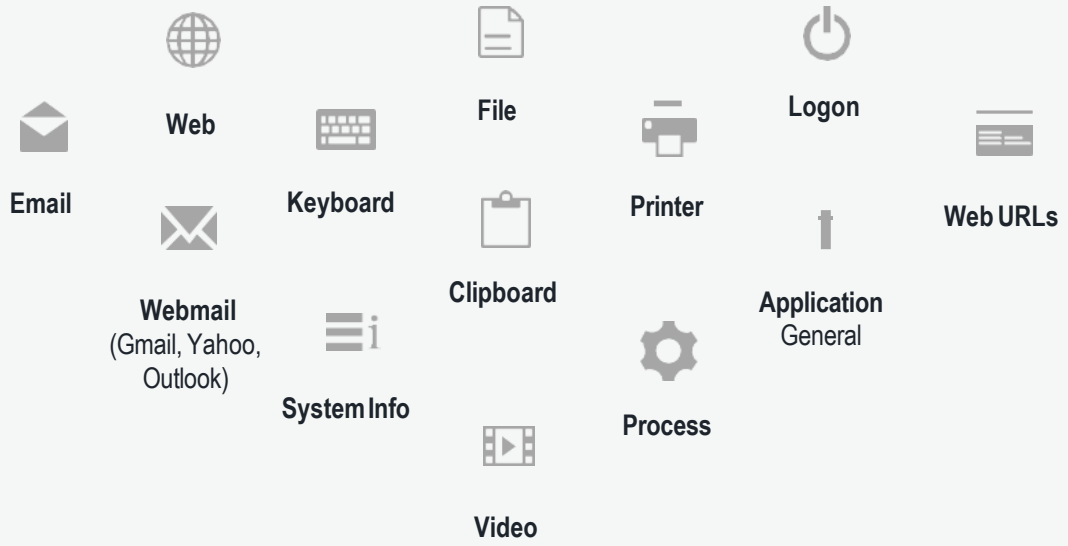
Zero Trust Data Protection – Everywhere

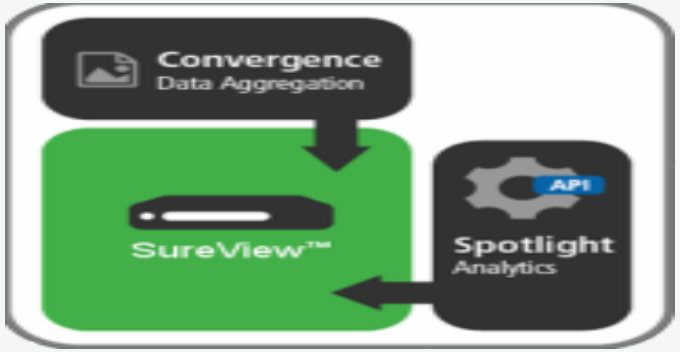


Data exfiltration protection – Anywhere / Anytime

Building Context with User Activities

Endpoint Data Collection Sources





RICH META DATA

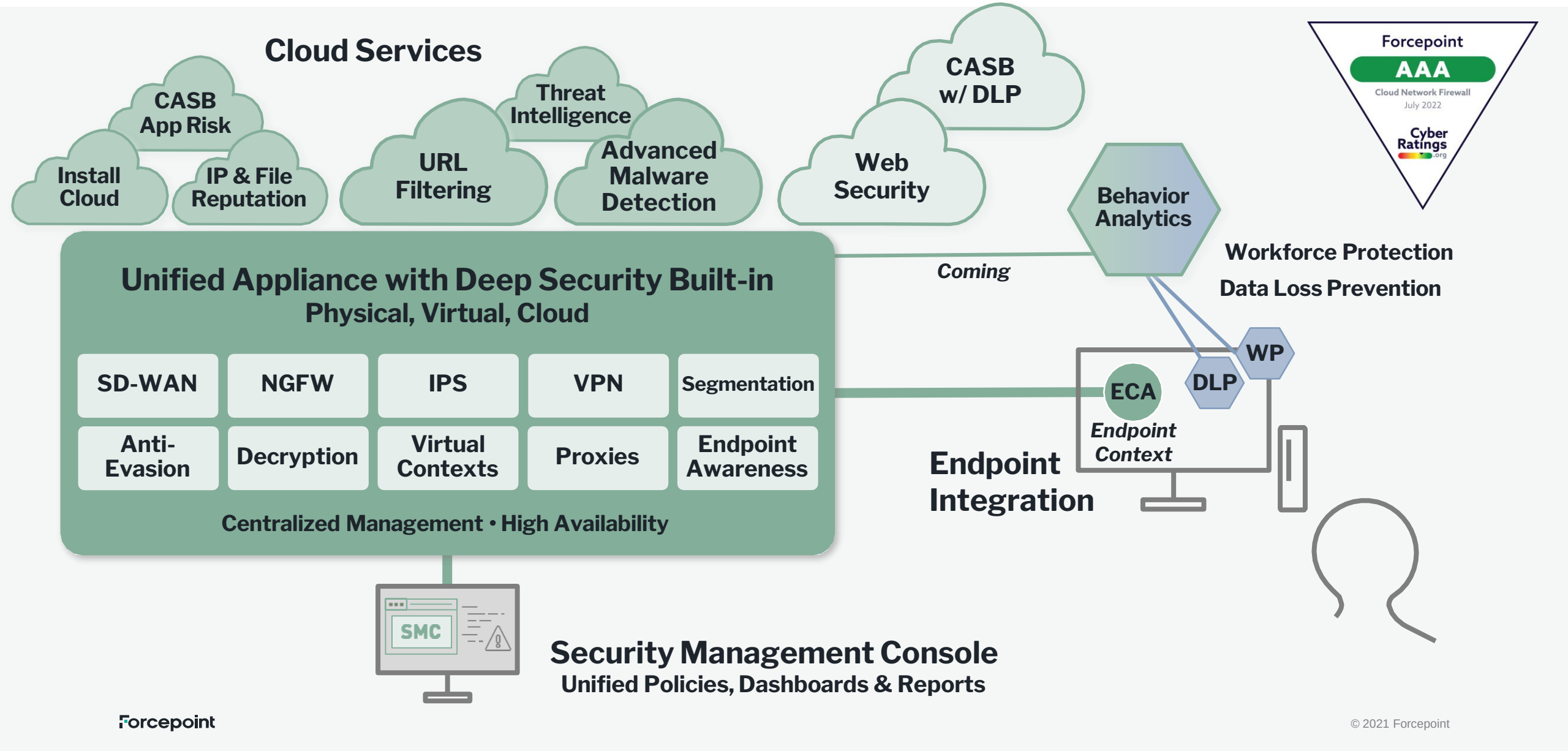
COPIES OF WEBSITES BROWSED-
Full copies of HTML rendered

COPIES OF EMAILS-*Both sent and received*

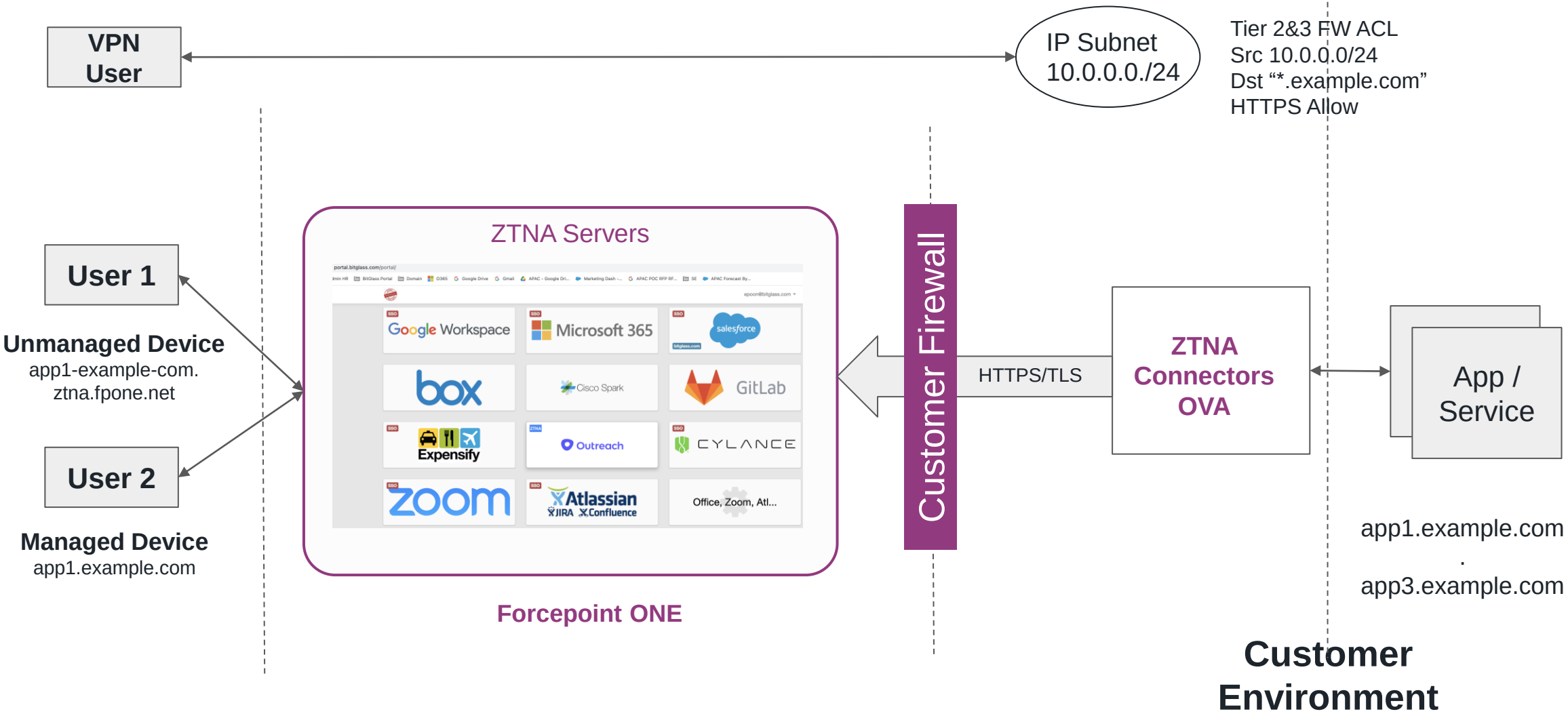
COPIES OF FILES- *Uploads, downloads, email attachments, copied to clipboard, files created/copied/moved*

DESKTOP VIDEO REPLAY

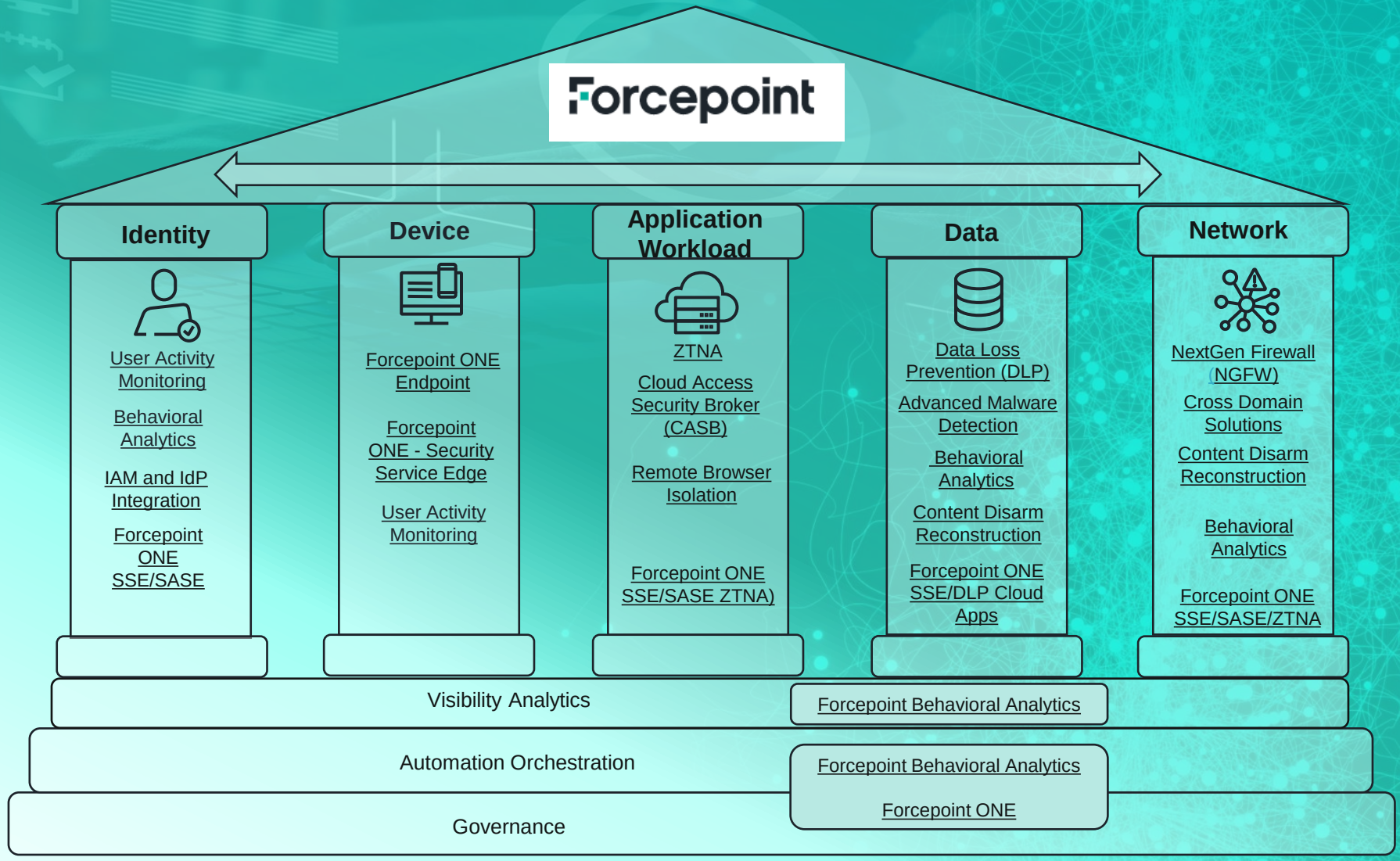
SDWAN – NGFW & IPS



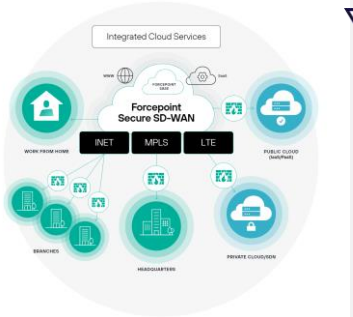
Architecture - Zero Trust Network Access (ZTNA)

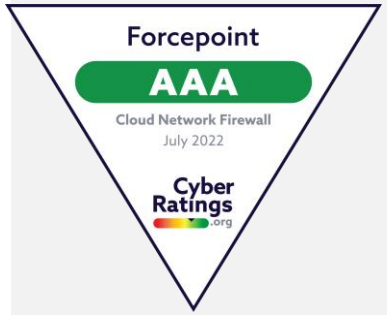


Forcepoint Zero Trust | Family of Solutions

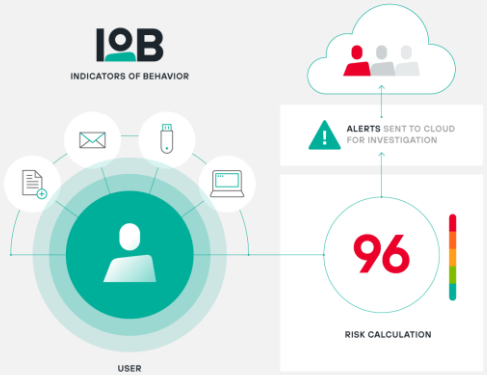


Forcepoint Zero Trust | IT & OT Security

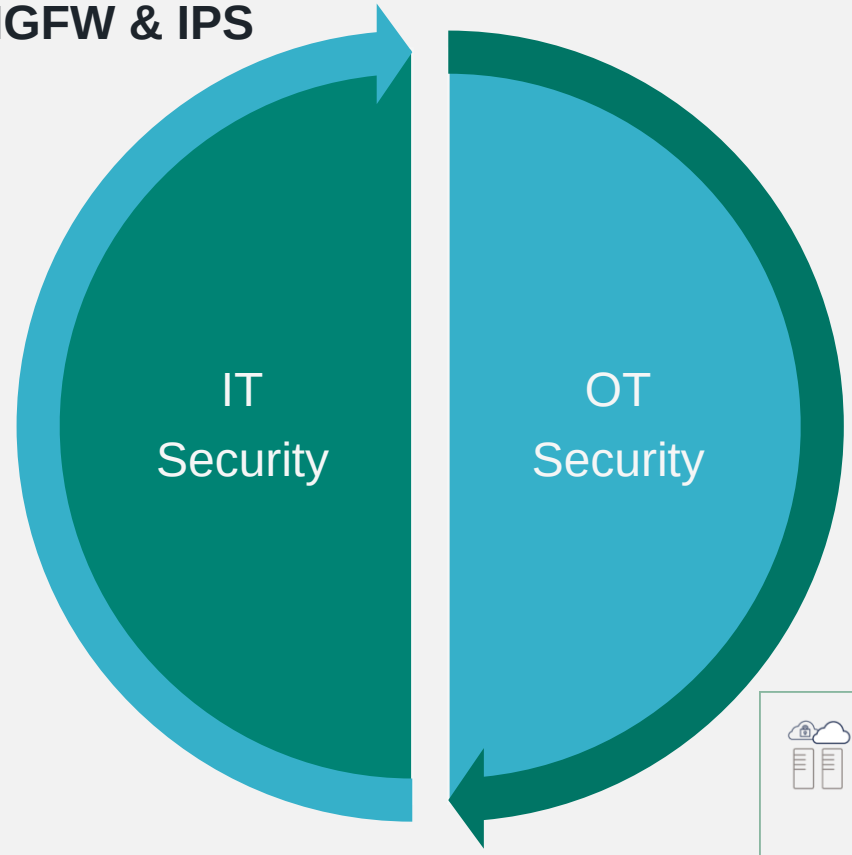


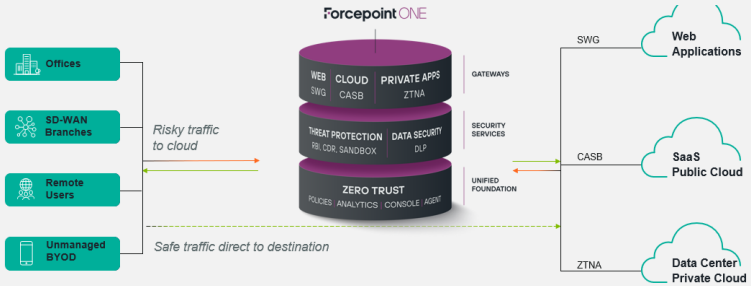


Secure-SDWAN
NGFW & IPS



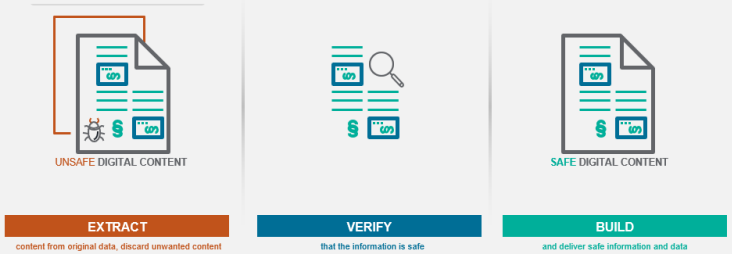
Risk-Adaptive Data Protection



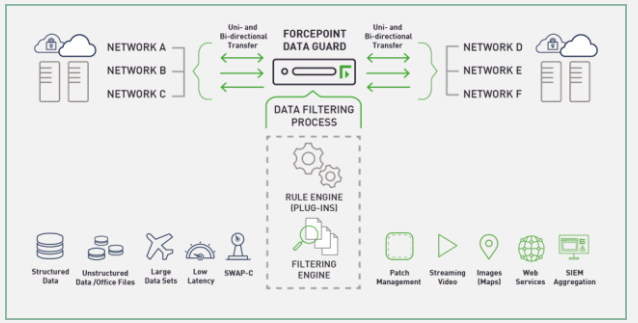


ZTNA& SASE

Forcepoint
Insider Threat



Content Disarm & Reconstruct



Air-Gapped Security
Data Guard

Learn & Win

Forcepoint Booth