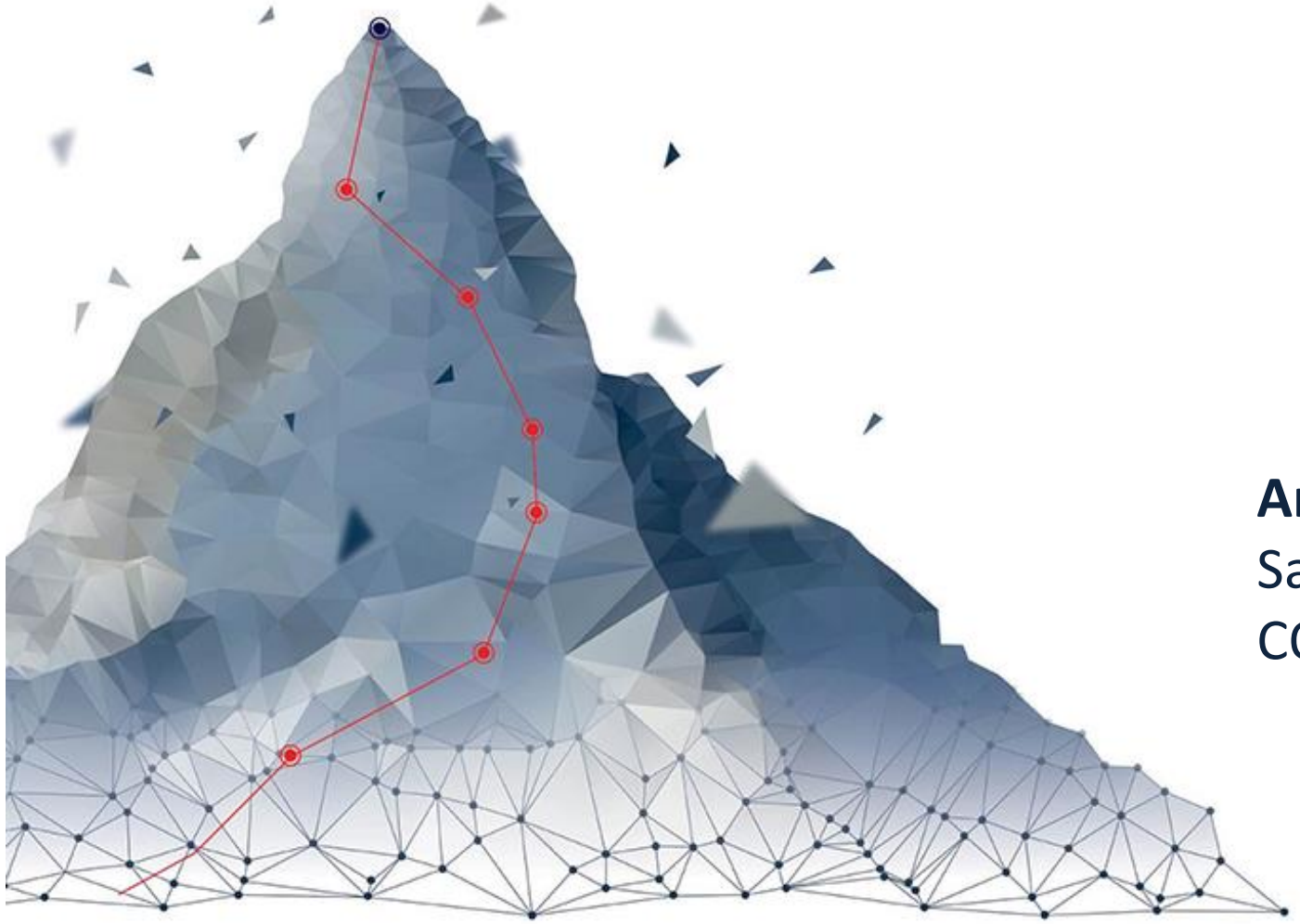
www.comp.com.pl

Praktyczne implementacje na styku z RODO: PGP, DLP, CASB, IDM

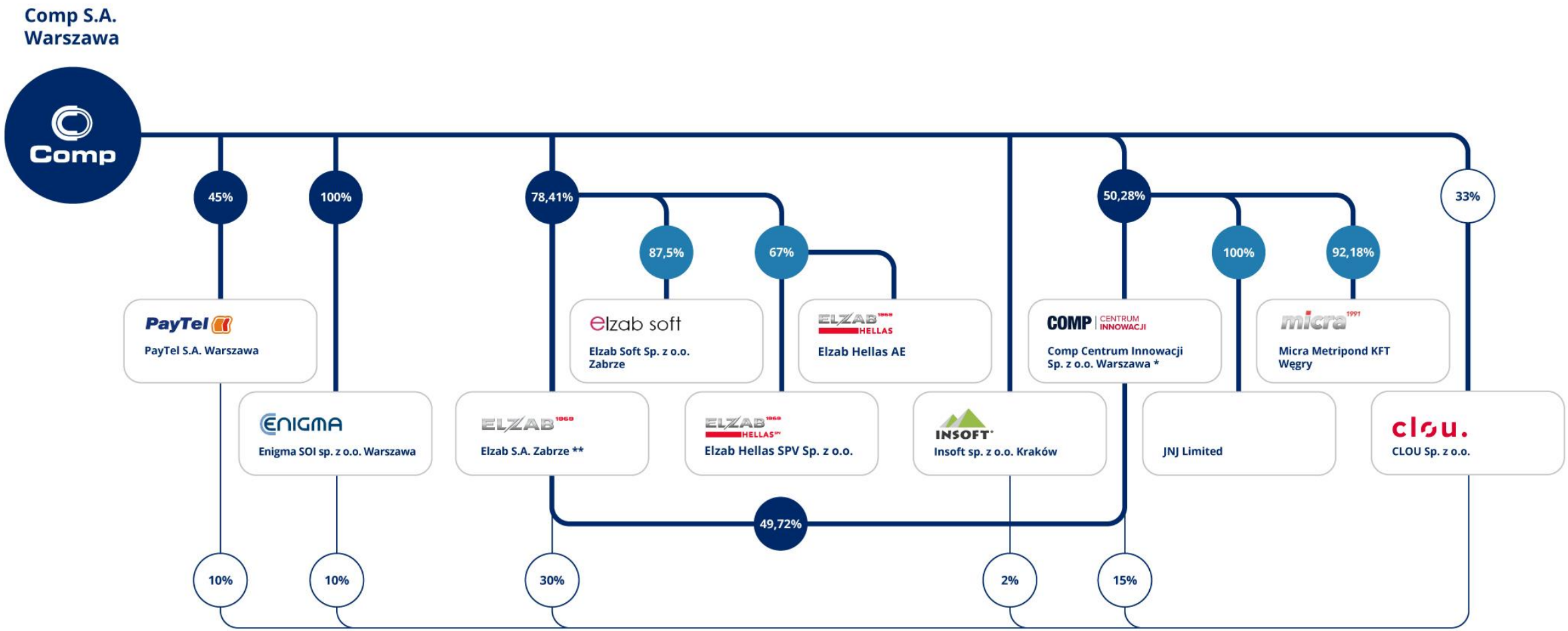


Artur Drobiecki
Sales Director Finance&Insurance Sector
COMP SA

Warszawa, maj 2019

Comp GRUPA KAPITAŁOWA | COMP CENTRUM INNOWACJI | ELZAB 1969 | ENIGMA | INSOFT | PayTel | NOVITUS | CSS CENTRUM USŁUG IT | clou.

SCHEMAT GRUPY



* - 100% udziałów w Comp Centrum Innowacji Sp. z o.o. posiadają wspólnie Spółki: COMP S.A. (50,3%) oraz Elzab S.A. (49,7%)

** - pośrednio wraz z akcjami własnymi Elzab S.A.

- Ponad 27 lat obecności na polskim rynku IT
- Ponad 1000 wysoce wykwalifikowanych pracowników
- Grupa Kapitałowa złożona z 12 spółek, „zbalansowany” biznes segmentów Retail i IT
- Comp S.A. i Elzab S.A. notowane na GPW
- Świadectwo Bezpieczeństwa Przemysłowego pierwszego stopnia, koncesje MSWiA, Certyfikat ISO 9001:2008
- Własne centra R&D oraz innowacji (utworzone w dedykowanym podmiocie Grupy)
- Specjalizacja w obszarze budowy systemów zapewnianiających cyberbezpieczeństwo (zarówno korporacyjne jak i kwalifikowane), co jest jednym z priorytetów rządu i dużych przedsiębiorstw
- Wiodący producent rozwiązań ochrony kryptograficznej dla przetwarzających informacje niejawne

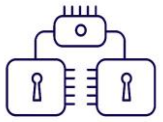
Grupa Comp koncentruje się na działalności w kilku atrakcyjnych niszach rynkowych, bazując na unikalnych kompetencjach oraz wysokich barierach wejścia do każdej z nich:

- Bezpieczeństwo elektroniczne oraz informatyczne, stanowiące trzon segmentu IT — IT
- Usługi dla małych i średnich przedsiębiorstw oraz produkcja urządzeń fiskalnych, stanowiące trzon segmentu retail — RETAIL

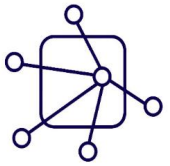
Identyfikujemy sprzyjające uwarunkowania zewnętrzne w każdej z głównych nisz swojej działalności, tzn.: w dziedzinie cyberbezpieczeństwa, w tym bezpieczeństwa specjalnego.

SEGMENT IT

W ramach **SEGMENTU IT** wyodrębnia się następujące grupy rozwiązań i specjalizacji:



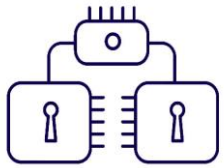
- **Bezpieczeństwo Korporacyjne i Sieci**
  Dostarczanie zoptymalizowanej i wydajnej infrastruktury, zapewniającej nieprzerwane funkcjonowanie procesów biznesowych przedsiębiorstwa oraz bezpieczeństwo w dostępie do danych, aplikacji, systemów oraz sieci.



- **Rozwiązania Systemowe**
  Dostarczanie systemów informatycznych przeznaczonych do obsługi kluczowych procesów biznesowych klientów. Działalność Grupy obejmuje projektowanie i wdrażanie dedykowanych systemów informatycznych zarówno w zakresie sprzętu jak też aplikacji i integracji w centrach przetwarzania danych.

- **Bezpieczeństwo Specjalne i Kryptografia**
  Realizacja projektów związanych z bezpieczeństwem teleinformatycznym, począwszy od projektowania i produkcji urządzeń kryptograficznych oraz oprogramowania, poprzez wdrożenia i szkolenia, na zarządzaniu bezpieczeństwem kończąc.

Comp GRUPA KAPITAŁOWA | COMP CENTRUM INNOWACJI | ELZAB 1969 | ENIGMA | INSOFT | PayTel | NOVITUS | CSS CENTRUM USŁUG IT | clou.



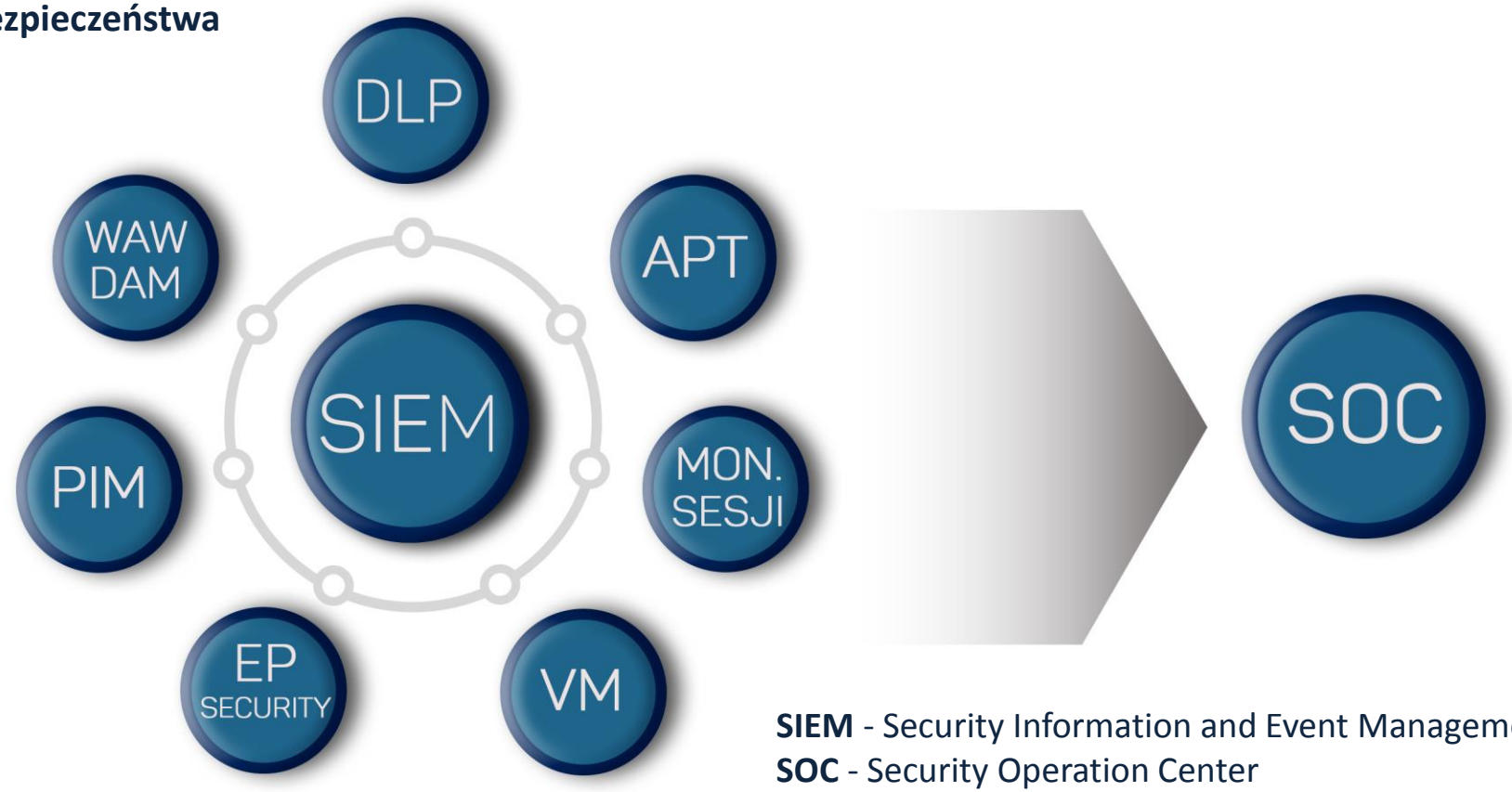
Pion Systemów Sieciowych – zapewnia efektywne i nieprzerwane funkcjonowanie procesów biznesowych sieci operatora oraz przedsiębiorstwa, a także ochronę danych i zapewnienie odpowiednich warunków środowiskowych.

Pion Cyberbezpieczeństwa i Zarządzania Ryzykiem – zespół inżynierów, konsultantów i audytorów odpowiedzialnych za implementację Security Operations Center (SOC), złożonego z technologii SIEM oraz dziedzinowych systemów bezpieczeństwa.

Kluczowe kompetencje:

- Bezpieczeństwo sieciowe:
  - NGX Firewall, Intrusion Prevention System (IPS), rozwiązania klasy ATP, rozwiązania VPN, rozwiązania klasy DLP, Systemy Web Gateway, Systemy Email Gateway, Systemy WAF/DAM, Zabezpieczenia DDoS, Zabezpieczenia DNS/DHCP, rozwiązania NAG.
- Security Operations Center (SOC):
  - Monitorowanie kluczowych zasobów IT w celu zabezpieczenia przed atakami cybernetycznymi.
- Systemy SIEM:
  - HP ArcSight, IBM Qradar, Splunk, McAfee SIEM, Elasticsearch, GreyLog, RSA.
- Audyty technologiczne/pentesty/testy aplikacji.
- Konsulting i usługi dodatkowe.

Portfolio technologii bezpieczeństwa



SIEM - Security Information and Event Management
SOC - Security Operation Center
DLP - Data Loss Prevention
APT - Advanced Persistent Threat
Mon. Sesji - Monitorowanie sesji

VM - Vulnerability Management
EP - EndPoint
PIM - Privileged Identity Manager
WAF - Web Application Firewall
DAM - Database Activity Monitoring

Usługi w zakresie ochrony informacji w oparciu o unikatową wiedza na polskim rynku. Integralną częścią oferowanych rozwiązań jest szeroko pojmowane bezpieczeństwo specjalne. Dotyczy ono zarówno rozwiązań sprzętowych i aplikacyjnych, jak i całego obszaru architektury i realizacji wdrożenia.

- Podstawą systemów tworzonych przez firmę Enigma **są własne kryptograficzne rozwiązania sprzętowe i aplikacyjne**.
- Atutem tych rozwiązań jest zastosowanie **wysoko rozwiniętych technologii i algorytmów szyfrowych**.
- Wysoką jakość oferowanych urządzeń i aplikacji kryptograficznych potwierdza ponad **40 certyfikatów ABW i SKW z zakresu przetwarzania informacji niejawnych** od klauzuli „Zastrzeżone”, przez „Poufne” i „Tajne” do „Ściśle tajne”.
- Systemy IT oparte na urządzeniach kryptograficznych Enigmy oznaczone są **marką CompCrypt** i przetwarzają informacje o szczególnym znaczeniu dla bezpieczeństwa narodowego.

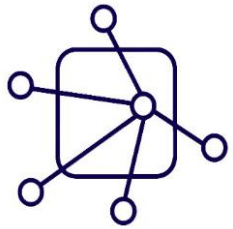
- **PKI i Podpis elektroniczny (również kwalifikowany)**
  Ponad 40 zrealizowanych systemów, w tym m.in.: Policja, SG, MSW, MON, MSZ, NBP, KDPW, mBank. Na wyróżnienie zasługują: system BIO PKI w GetinBank, oraz wydzielony system PKI dla ePaszportów PWPW/MSW.

- **Zarządzanie Tożsamością / Uwierzytelnienie**
  Ponad 10 zrealizowanych systemów, w tym m.in.: Policja, SG, MSW, MF, GSG, Societe Generale.

- **Bezpieczeństwo Informacji**
  Systemy bezpieczeństwa korporacyjnego, zabezpieczenia sieciowe, bezpieczna poczta elektroniczna, itp.

- **Urządzenia Kryptograficzne**
  Wyk. biurowe i polowe N7, N11; certyfikaty SKW i ABW.

URZĄDZENIA SZYFRUJĄCE



Budujemy dedykowane systemy informatyczne w warstwie aplikacyjnej i infrastrukturalnej, zarówno on-premise jak i w chmurze.

Dostosowujemy technologie do potrzeb klienta i koordynujemy współpracę interdyscyplinarnych zespołów.

Posiadamy kompetencje z wielu obszarów IT, nie uzależniamy się od jednego producenta i jednej technologii – potrafimy je powiązać.

Główne obszary działalności

- **Usługi integratorskie** - scalamy wiele elementów (własnych, klienta, firm trzecich) w jednolicie działające systemy. Obejmujemy przy tym pełen cykl życia systemu: od prac koncepcyjnych, przez projekt, dobór komponentów, dostawę i wdrożenie, po serwis, utrzymanie i rozwój.
- **Wsparcie w drodze do chmury** - wspieramy naszych klientów w przenoszeniu biznesu do modelu chmury prywatnej, hybrydowej, publicznej poprzez wszystkie etapy od IaaS, przez PaaS i SaaS do BaaS.
- **Wdrożenia i zarządzanie infrastrukturą fizyczną IT** - współpracujemy z największymi producentami sprzętu, u wielu z nich posiadamy najwyższe stopnie certyfikacji sprzedażowej i serwisowej. Należą do nich między innymi: Brocade, Cisco, Dell EMC, Emulex, Fujitsu, Hitachi Data Systems, HP, Huawei, IBM, Intel, Lenovo, NetApp, Oracle, Qlogic.

- **Software House** - nasz dział budowy oprogramowania, w oparciu o wieloletnie doświadczenie, dostarcza rozwiązania z obszarów:


Cyfrowe usługi


Digitalizacja


ZSI

Business Intelligence

CRM

- **Wirtualizacja** - wirtualizacja serwerów, desktopów, pamięci masowych, infrastruktury sieciowej w oparciu o rozwiązania VMware vSphere, VMware Horizon (VDI), VMware NSX, OpenStack, Citrix Xen, RedHatEV, OracleVM, HDS G-series, IBM SVC, NetApp V-series, Dell EMC vPlex.

- **Zarządzanie Bezpieczeństwem Informacji** - analiza środowisk IT oraz dostosowanie istniejących procedur i rozwiązań technicznych do nowych wymagań w zakresie Ochrony Danych Osobowych **(RODO)** – włączając w to **autorskie oprogramowanie** wspierające RODO.

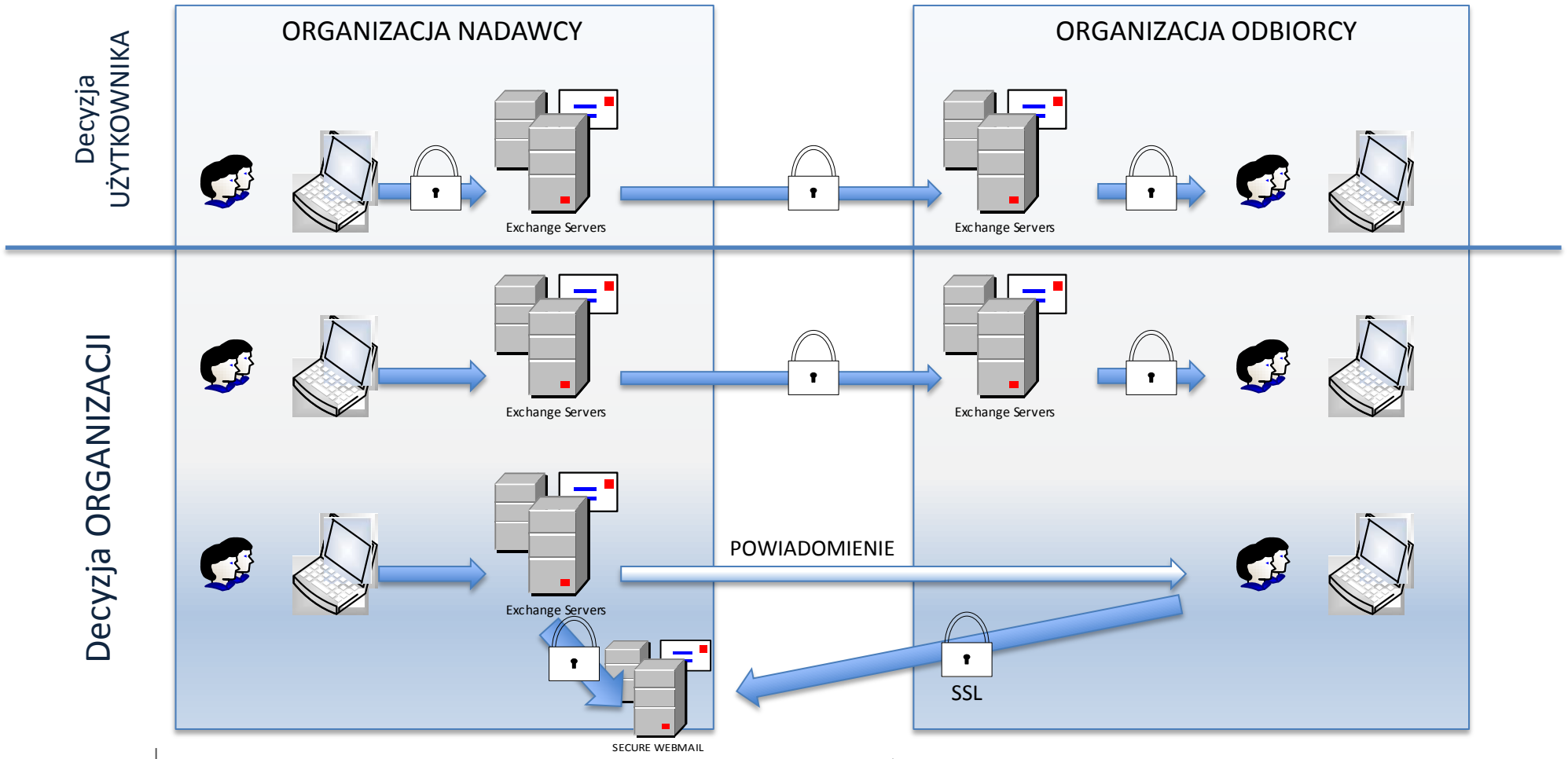
- **Doradztwo i outsourcing** - w ramach usługi świadczymy pełną analizę i niezależną ocenę zasobów IT organizacji oraz wskazujemy obszary, których przekazanie na zewnątrz będzie efektywne i bezpieczne dla organizacji klienta.

Praktyczne implementacje na styku z RODO

- Kontrola nad całą korespondencją email – integracja DLP i PGP Email Gateway.
- Zarządzanie tożsamością – IDM.
- Kalsyfikacja dokumentów – element konieczny w drodze do chmury.

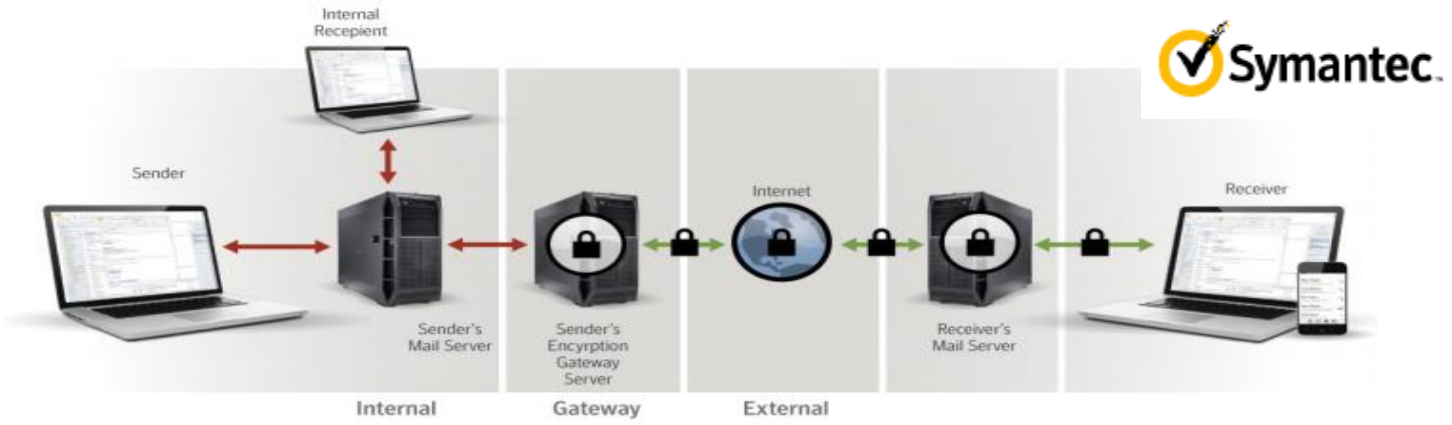
Szyfrowanie poczty

Szyfrowanie poczty email



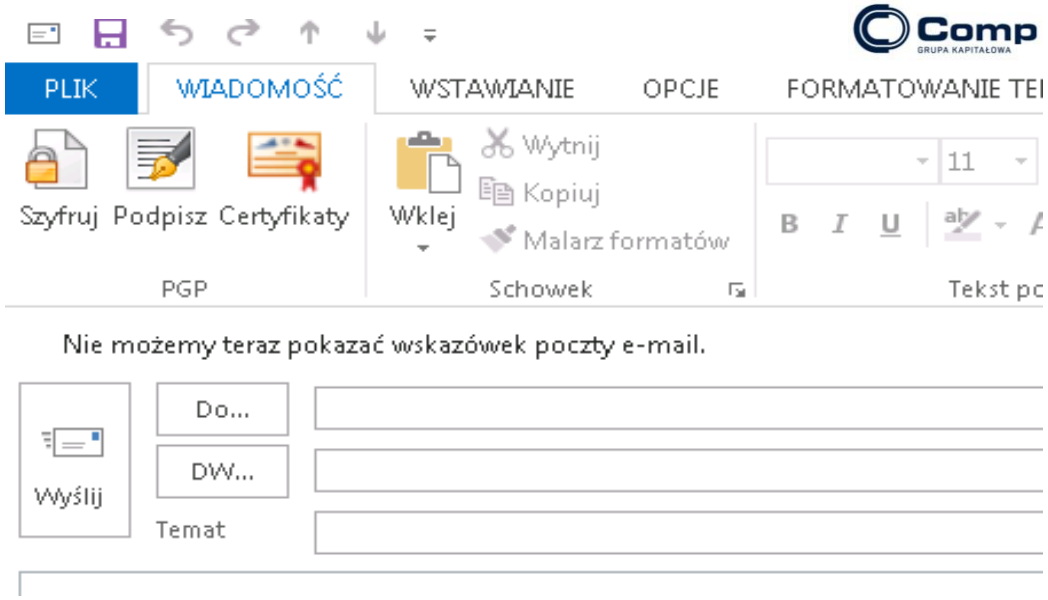
Korzyści dla organizacji wynikające z zastosowania PGP Email Gateway:

- System DLP ma dostęp do treści korespondencji i możliwość weryfikacji przed opuszczeniem przez nią organizacji
- Materiał kryptograficzny jest przechowywany w centralnym miejscu.
- Obsługa odbiorców nieposiadających materiału kryptograficznego (Secure WebMail i Secure PDF).



Unikalne cechy wdrożonego systemu:

- Użytkownik podejmuje decyzję w swoim outlook: *szyfruj, podpisz, załącz swój certyfikat*.



- DLP może autonomicznie podjąć decyzję o zaszyfrowaniu korespondencji.

- Dwa tryby pracy:
  - Lekki – szyfrowanie;
  - Pełny – pełna funkcjonalność w oparciu o publiczny certyfikat.

- Automatyzacja wydania certyfikatu publicznego przez DIGICERT.

- Integracja i automatyzacja z systemem zarządzania tożsamością.

Zarządzanie tożsamością

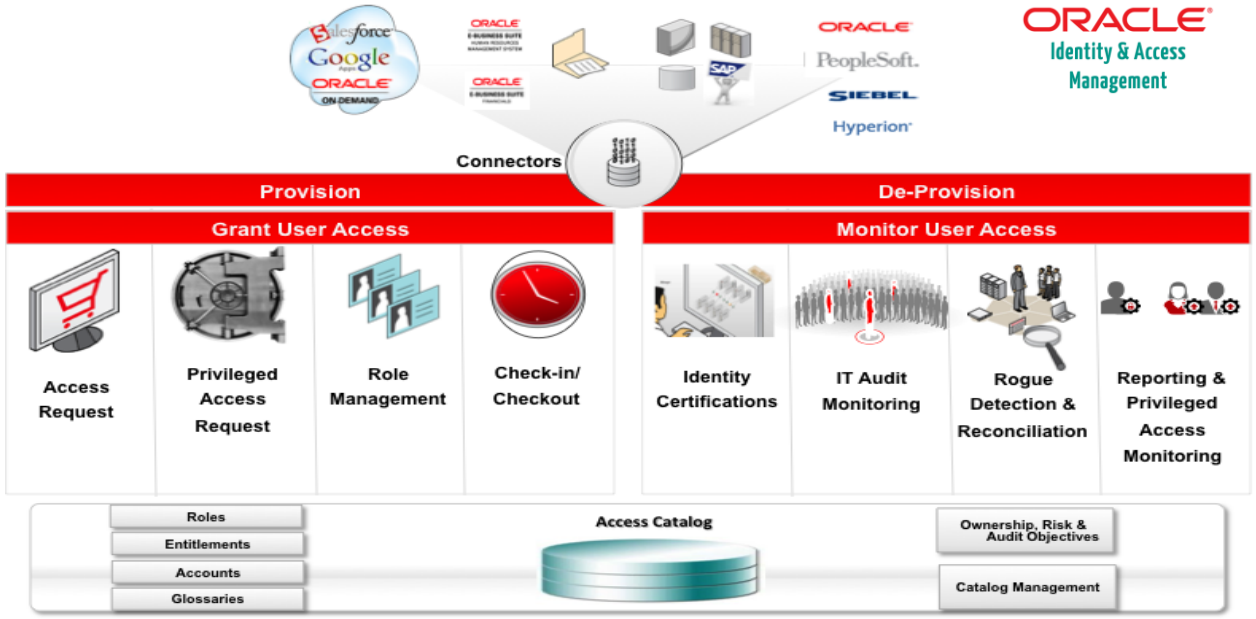
IDM – dlaczego zarządzać tożsamością

- Lista zadań czy również hasło do systemu HR?
- Czy Pani Zosia ma uprawnienia takie jak Pan Waldek?
  czy „do wszystkiego co potrzeba”? Kto o tym zdecydował?
- Kto ma najwyższe uprawnienia w Twojej organizacji?
  Administrator? CFO? CSO?
  A może programista, z którym rozstaliście się w zeszłym roku?
- Ile kosztuje ręczne zarządzanie dostępami i zgodnością z regulacjami?
  - NIC – nikogo nowego nie zatrudnialiśmy
  - Nie pytaj…
  - Nie wiem…

…czy IDM się zwróci?

….czy IDM się zwróci?

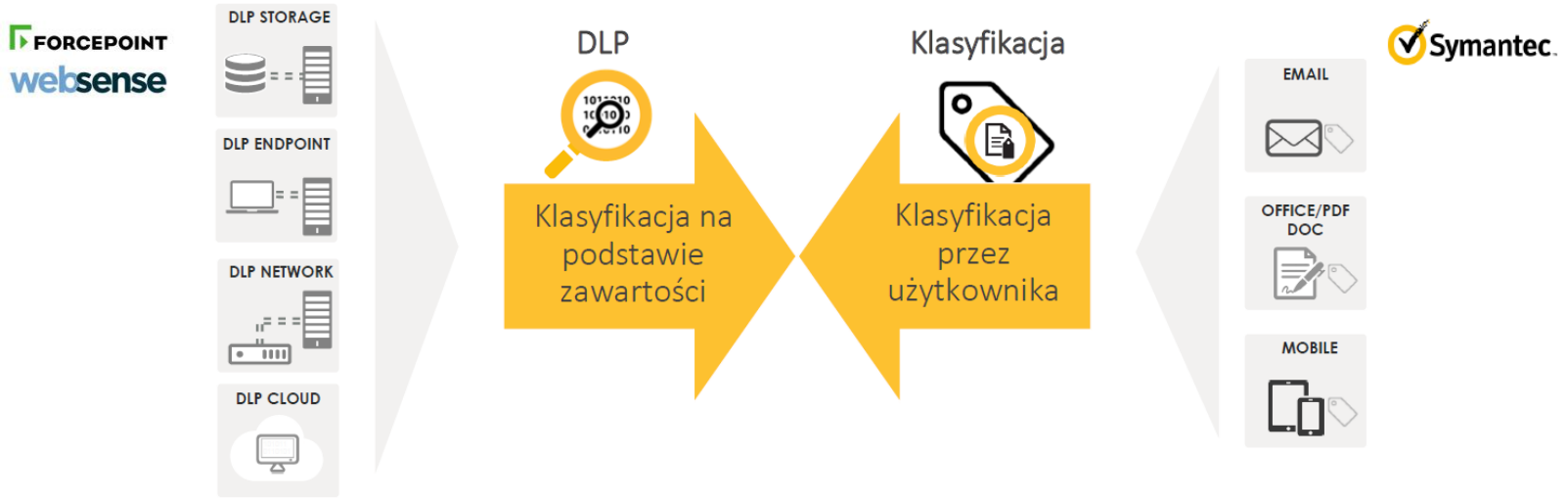
- Zarządzanie rolami, a nie użytkownikami i atomowymi uprawnieniami (centralne bezpieczeństwo)
- Użytkownik samodzielnie wnioskuje o dostęp (odciążenie helpdesk)
- Audytowalność nadawania uprawnień (wymagania regulatora i służb)
- Integracja ze środowiskiem IT i systemami korporacyjnymi (automatyzacja procesów)

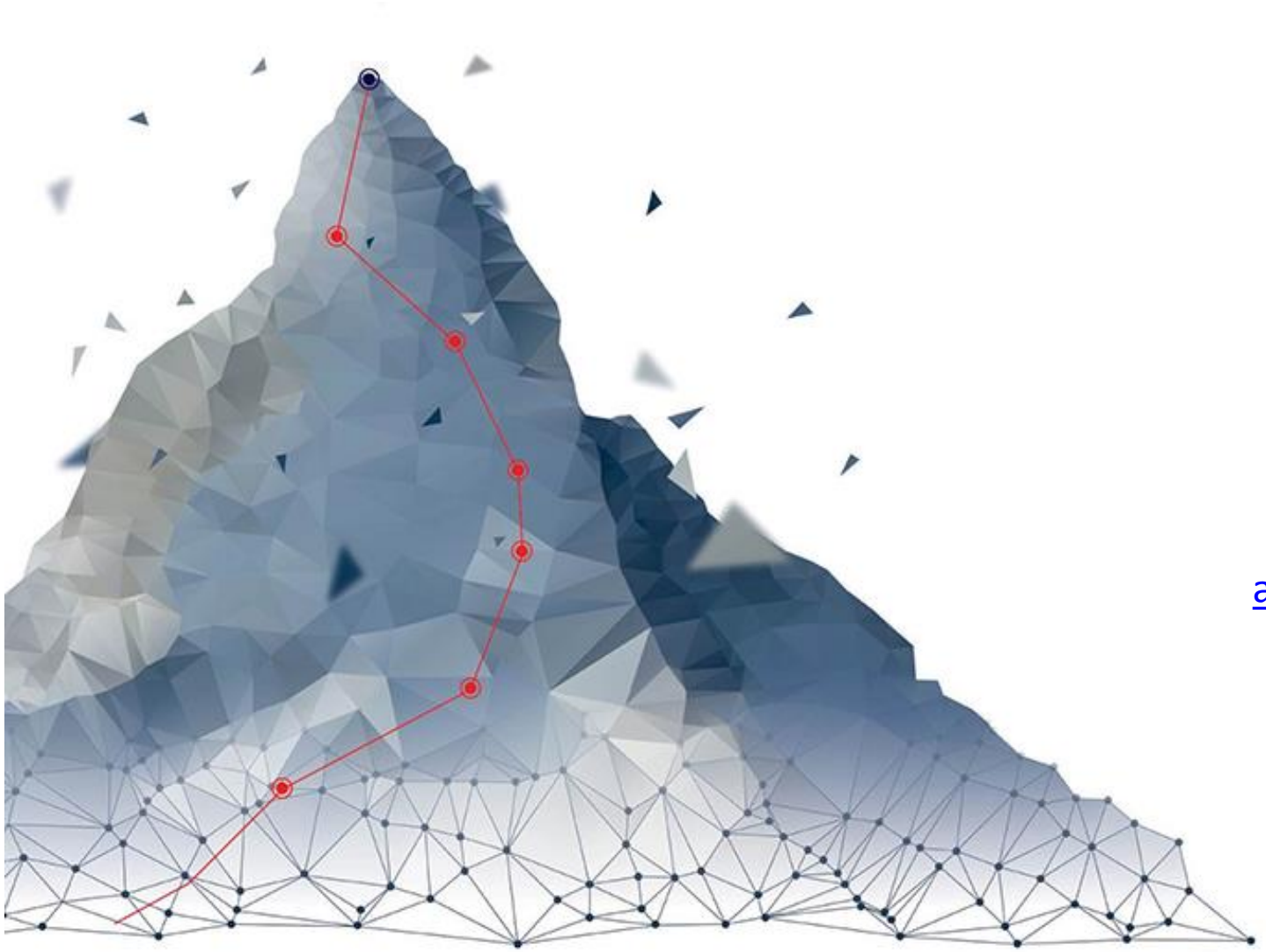


Klasyfikacja treści

Bezpieczeństwo dokumentów, czyli element konieczny w migracji do chmury.

- Automatyczna klasyfikacja będzie kompletna w połączeniu z potwierdzeniem autora dokumentu.
- Własny klasyfikator uniezależnia organizację od dostawców chmury.
- Ochrona przed wyciekiem, zarządzanie uprawnieniami i audyt dokumentów na zasobach sieciowych, na urządzeniach mobilnych.





DZIĘKUJĘ

Artur Drobiecki
artur.drobiecki@comp.com.pl