ISSS

Ochrana citlivých dokumentů

v prostředí státní správy

Tomáš Hlavsa

Atos

1

Je to reálný problém?

….trápí to někoho?

Sobotka opět terčem hackerů. Neo jeho soukromou poštu

AKTUALIZOV

Hackeri si všimli Slovensko. Udreli na nitriansku

cu

Pravda 15.05.2017 20:00

Uložiť na Facebook | Páči sa mi to 9

ČEZ se nepodařilo zjistit, kdo vynesl informace o prodeji jeho majetku

26. listopadu 2018 10:01

Společnost ČEZ nevypátrala viníka úniku informací o prodeji jejích bulharských aktiv. Firma se to podle Českého rozhlasu snažila zjistit dotazníkovým šetřením, k ničemu ale nedospěla. Únik b

E-maily a hesla stovek politiků a úředníků lze koupit

T-Mobile dostal pokutu za obří únik dat o klientech. Utekly adresy nebo výše plateb

AKTUALIZOVÁNO 16. 8. 2016

Úřad prověřuje další možné úniky osobních úd

17. 8. 2018 – Úřad pro ochranu osobních údajů prověřuje v polovi úniku osobních dat významného počtu lidí.

Jedním z nových případů, který prověřuje Úřad, je ohlášení porušen oznámila únik dat klientů, ke kterému mělo dojít chybným elektro uložených v tabulce, na adresy 147 jiných osob.

„Řešíme také únik desítek tisíc přihlašovacích údajů, které měly počítačových a konzolových her," uvedl tiskový mluvčí ÚOOÚ Tomáš Paták. Podle prvních zjištění Úř pravděpodobně nezaslal ohlášení o porušení zabezpečení.

Lupa.cz » Hackeři úspěšně napadli e-mailové účty ministerstva zahraničí. Měsíce stahovali data

Hackeři úspěšně napadli e-mailové účty ministerstva zahraničí. Měsíce stahovali data

včera

Na kauzu upozornil server Neovlivní. Ministerstvo okamžitě svolalo rychlou tiskovou konferenci, kde ministr zahraničí útok potvrdil.

NÁZORŮ

jeden z útoků byl částečně úspěšný, zahájit ministr zahraničí Lubomír Zaorálek (ČSSD) narychlo svolanou tiskovou konferenci.

Sněmovní bezpečnostní výbor vyzval ministerstva vnitra a spravedlnosti, aby jednala o opatřeních proti únikům ze spisů, zejména v přípravných řízeních. Informaci mají oba ministři podat poslancům podle usnesení do konce září. Policejní ředitel

Zabezpečení osobních údajů

Článek 32

Zabezpečení zpracování

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kont
různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob,
vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající dar

a) pseudonymizace a šifrování osobních údajů;

b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a slu

c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzického

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených techni
pro zajištění bezpečnosti zpracování.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která př
náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění před
zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

3. Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1
schváleného kodexu chování uvedeného v článku 40 nebo uplatňování schváleného mech
uvedeného v článku 42.

4. Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická
správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní
pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

§ 19

Správa a ověřování identit

(1) Povinná osoba používá nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému.

(2) Nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací zajišťuje

a) ověření identity před zahájením aktivit v informačním a komunikačním systému,

b) řízení počtu možných neúspěšných pokusů o přihlášení,

c) odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití,

d) ukládání autentizačních údajů ve formě odolné proti offline útokům,

e) opětovné ověření identity po určené době nečinnosti,

f) dodržení důvěrnosti autentizačních údajů při obnově přístupu a

g) centralizovanou správu identit.

(3) Povinná osoba pro ověření identity uživatelů, administrátorů a aplikací využívá autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.

(4) Do doby splnění požadavku podle odstavce 3 musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, používat autentizaci pomocí kryptografických klíčů a zaručit obdobnou úroveň

e) neumožňující uživatelům a administrátorům

1. zvolit si nejčastěji používaná hesla,

2. tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a

3. opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel a

f) pro povinnou změnu hesla v intervalu maximálně po 18 měsících, přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie.

(6) Povinná osoba v případě používání autentizace pouze účtem a heslem dále

a) vynutí bezodkladnou změnu výchozího hesla po jeho prvním použití,

b) bezodkladně zneplatní heslo sloužící k obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 60 minut od jeho vytvoření a

c) povinně zahrne pravidla tvorby bezpečných hesel do plánu rozvoje bezpečnostního povědomí podle § 9.

§ 20

Řízení přístupových oprávnění

Povinná osoba používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění

a) pro přístup k jednotlivým aktivům informačního a komunikačního systému a

Ochrana citlivých / hodnotných informací

- Naplnění povinností Správce / Provozovatele vůči 181/2014 resp. 82/2018 Sb.
- Naplnění povinností Správce / Zpracovatele vůči GDPR
- Hrozba pokut /sankcí, pokud pokud neplním, viz výše
- Reputační riziko (média, sociální sítě, tisk)
- Osobní odpovědnost (dle pracovního řádu a interních směrnic)
- Vznik reálné škody při úniku citlivé informace a související dopady

2

SIEM / DLP / EDR / SOC

….. kdo se v tom má vyznat

Položte si 5 jednoduchých otázek

- Smlouvy
- Návrhy dokumentů
- Zadávací dokumentace
- Osobní složky

- Na Vašem PC/NB
- Na síťovém disku
- V cloudu
- Mobilní zařízení
- USB disk

- Vy
- Správce
- Váš kolega
- Externí firma

- Neoprávněný přístup
- Únik před zveřejněním
- Neautorizovaná změna
- Podvržený dokument
- Ztráta
- Neúmyslné odeslání

- Chránit, ale jak?
- Jak klasifikovat?
- Jaká pravidla jsou nutná?
- Jaká pravidla Vás budou brzdit?
- Vaše stávající politika

Máte klasifikační směrnici? ….. a dodržujete ji? ….. a kontrolujete její dodržování? ☺

9. Klasifikace obchodních tajemství a důvěrných informací

9.1 Obchodní tajemství a důvěrné informace Společnosti jsou v průběhu procesu popsaného v článku 8.2 této směrnice klasifikovány následujícím způsobem do 3 stupňů utajení:

A. „Přísně tajné" jsou informace, jejichž únik může ohrozit dlouhodobé strategické cíle nebo i samotné přežití společnosti. Přísně tajné informace vyžadují nejvyšší stupeň utajení a řízení.

B. „Tajné" informace jsou informace, jejichž únik může mít významný krátkodobý dopad na provoz společnosti nebo může ohrozit krátkodobé taktické cíle společnosti „Tajné informace vyžadují vysoký stupeň utajení a řízení.

C. „Důvěrné" informace jsou informace, které nejsou běžně dostupné mimo Společnost a jejich únik může způsobit menší provozní nebo komunikační problémy. Důvěrné informace jsou informace, které vyžadují obecný stupeň utajení a řízení.

9.2 Podrobnosti týkající se klasifikace stupně utajení dokumentů musí být v souladu se standardy a postupy Společnosti.

9. Classification of Trade Secrets and Confidential Information

the leakage of which could cause minor operational or communication concerns. "Confidential" information is such information that requires a general level of restriction and control.

9.2 The details concerning document classification levels must be in compliance with the standards and procedures of the Company.

8.2 Klasifikácia informácií

Cieľom je zabezpečiť, aby informácie dostali dôležitosti pre organizácii.

8.2.1 Klasifikácia informácií

(1) Pre potrebu ochrany informácií platí ich nas

a) citlivé,

b) interné,

c) verejné.

(2) **Citlivé** - sú chránené informácie, a to

a) osobné údaje poistencov,

b) osobné údaje zamestnancov,

c) osobné údaje tretích strán,

d) mzdové náležitosti zamestnancov a poist

Information Owner

All Atos information requires an owner, who is responsible for classifying the information at time of creation.

Owners of Atos information are Atos management or representatives of Atos management, under whose responsibility the information has been created. Owners determine where, how and by whom Atos information may be used. Atos information owners may delegate authority to grant access to the information to other Atos employees.

The owner must be careful not to over-classify information. Over classification may slow down the business process due to the extra processes required for secure handling and storage. Information that is over classified may cause employees to disregard the classification system, rendering ineffective the Atos information protection procedures.

.

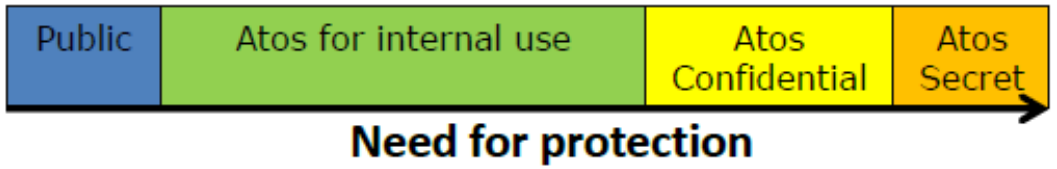
Information Classification Scheme

This document specifies the classification attached to Atos Information and how it must be treated through its life from creation to disposal. Atos staff who handle classified documents belonging to customers must handle them in accordance with the customer's classification standard. When a security policy, procedure or process is absent at a customer location, staff should propose to the customer to follow this standard.

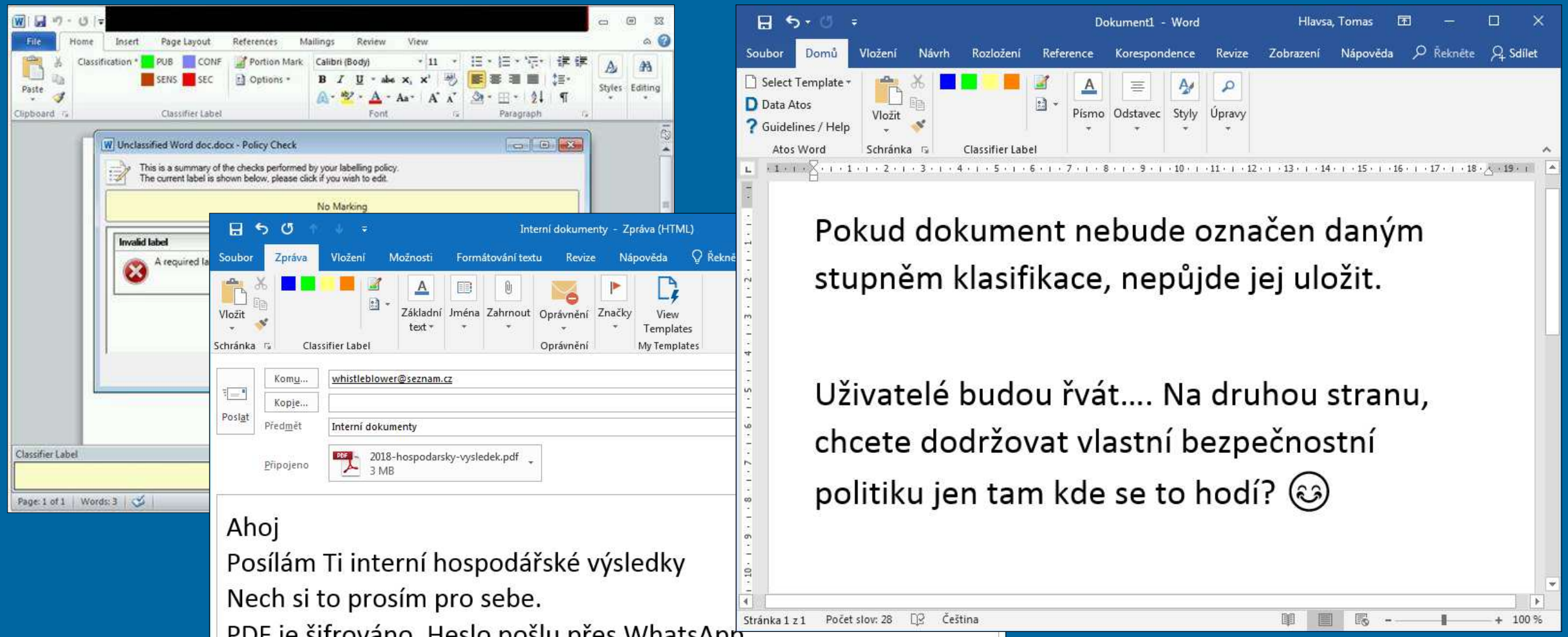
All information must be classified by the owner or author as either:

1. Public;
2. Atos for internal use;
3. Atos Confidential;
4. Atos Secret.

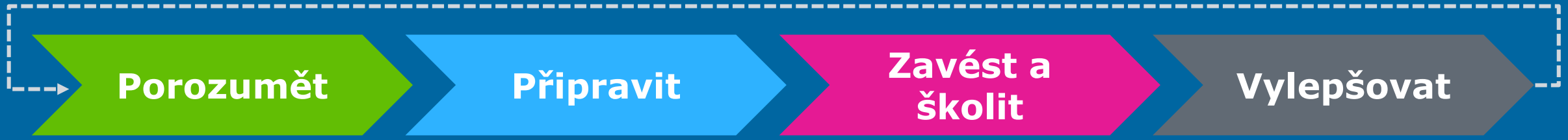
By default, any information whose classification is not explicitly defined is presumed to belong to the "Atos for internal use" classification.



Vynucujete označování klasifikace dokumentů? .... a u emailů?



Plán ochrany dat, nejen citlivých dat



- Jaká data chráníme
- Jakým hrozbám čelíme

- Politiky a pravidla
- Na základě reálného používání

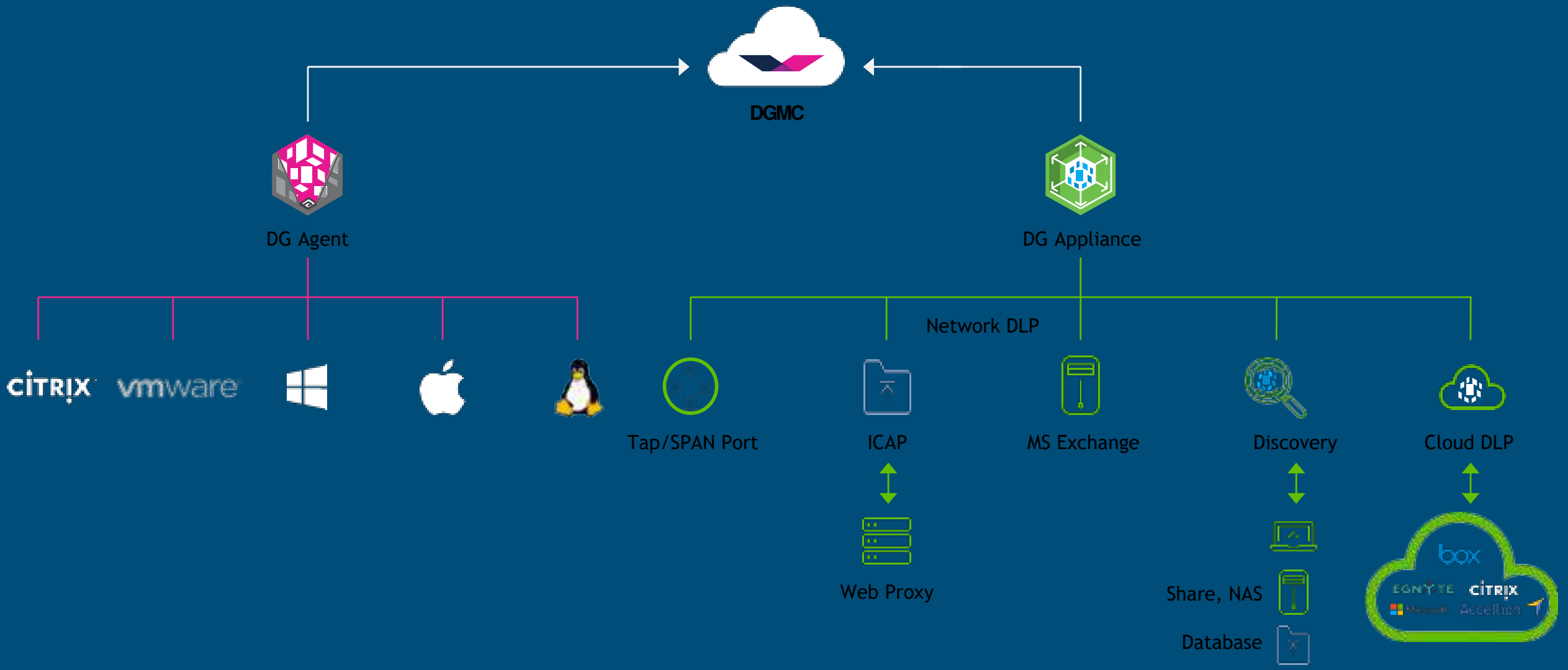
- Adaptivní a automatizovaná kontrola
- Varování v reálném řase zvyšuje bezpečnostní povědomí uživatelů

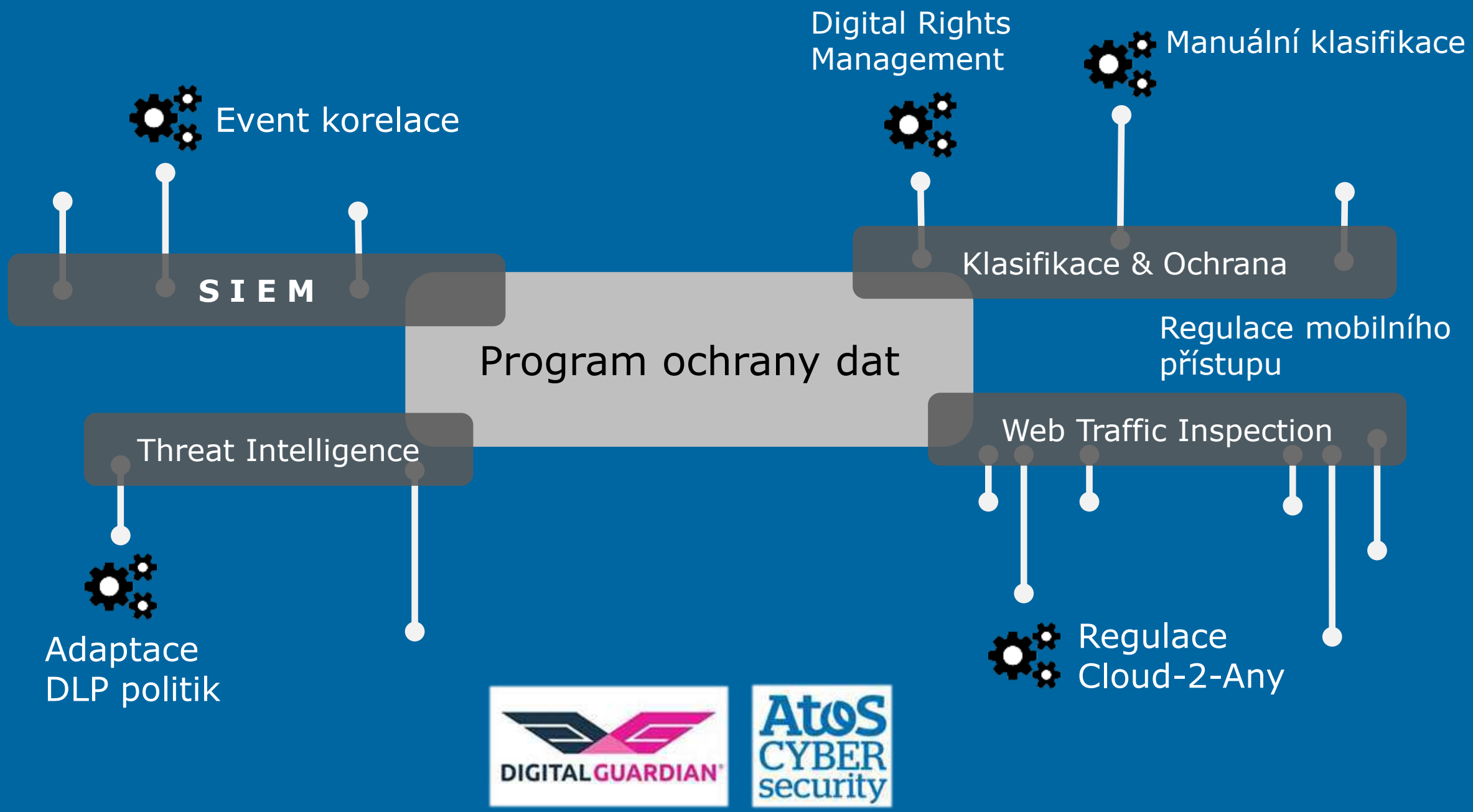
- Pokročilá analytika a reporting
- Rozhodnutí o dalším zvyšování bezpečnosti (EDR, SIEM, SOC)

3

ATOS a ochrana dat

Standardní přístup přestává stačit

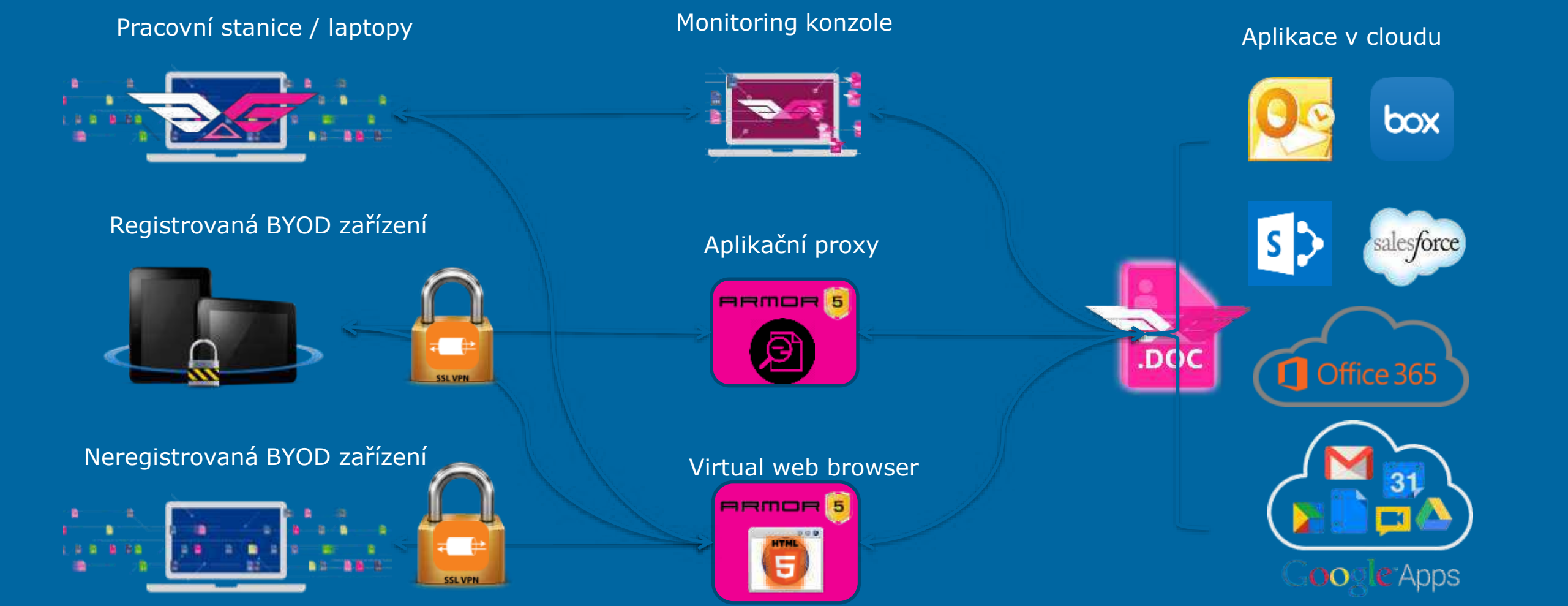


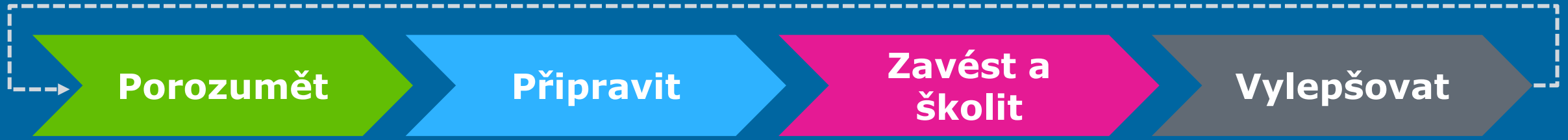

Digital Rights Management
Manuální klasifikace
Event korelace
SIEM
Klasifikace & Ochrana
Program ochrany dat
Regulace mobilního přístupu
Threat Intelligence
Web Traffic Inspection
Adaptace DLP politik
Regulace Cloud-2-Any
DIGITAL GUARDIAN
Atos CYBER security

Co chceme řídit a kde nám mohou data utéci.

- View & Open
- Network Upload
- USB Devices
- Application Launch
- Burn to CD DVD
- Print Screen
- Attach to Email
- Cut & Paste
- Delete & Recycle
- File Encrypt
- File Create
- Connect Device
- Email
- Cloud Application
- Remote Drives
- Save to Local Drive
- Send to Printer

Komplikovaná věc ta ochrana dat





- Jaká data chceme chránit
- Jakým rizikům čelíme

- Politiky a jejich pravidla
- Na základě reálných situací
- Vždy v návaznosti na Vaše činnosti

- Přizpůsobivá pravidla
- Popup upozornění uživatelům je upozorní na možná pochybení

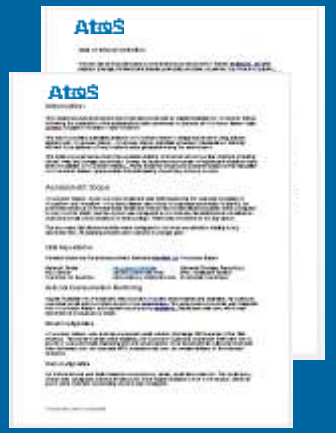
- Vypilovaný reporting
- Integrace do SIEMu, další krok směrem k SOC?

ATOS program ochrany dat

…a teď jednoduše …

ATOS chrání data svých zákazníků.

Klasifikace



Soulad s bezp. politikou

Funkční technické řešení

Bezpečnostní monitoring

Školení

Zlepšování

Trusted partner for your Digital Journey

Tomáš Hlavsa

Tomas.Hlavsa@atos.net