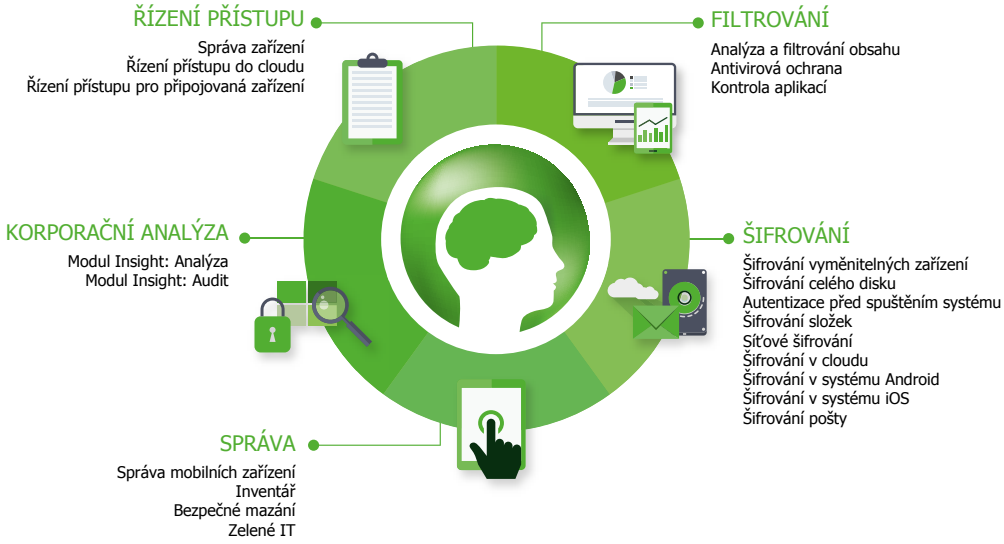
FUNKCE SYSTÉMU EGOSECURE



KORPORAČNÍ ANALÝZA

MODUL INSIGHT: ANALÝZA

Aby bylo možno optimálně zavést ochranná opatření, zjistí modul Insight nejprve celkovou bezpečnostní situaci uživatele ve firemní síti. Výsledky této analýzy jsou pak zpracovány podle potřeb správců a zobrazeny ve formě grafů a tabulek. Modul Insight tak poskytuje reálný obraz zabezpečení firmy či organizace. Zobrazení je souhrnné, nelze tedy činit závěry o aktivitách jednotlivých uživatelů. Z uvedených údajů lze optimálně určit, jaká ochranná opatření jsou skutečně potřeba.

MODUL INSIGHT: AUDIT

Tento modul zajišťuje podrobnou viditelnost toku údajů, přičemž zobrazuje potenciální slabá místa v nastavení zabezpečení. Lze tak získat i informace pro vyšetřování. Možnost tyto informace získat významně pomáhá splnit legislativní požadavky na informační technologie. Například německý federální zákon o ochraně osobních údajů stanoví povinnost vést protokol. Modul EGOSECURE Insight navíc znemožňuje narušení práva zaměstnanců na soukromí, protože přístup k zaznamenávaným údajům je chráněn metodou 4 nebo 6 očí.

ŘÍZENÍ PŘÍSTUPU

SPRÁVA ZAŘÍZENÍ

Tato funkce umožňuje jasně definovat, kdo může používat jaká zařízení (například flash disky, CD média, TV tuner) a jaká rozhraní (například WLAN, Firewire, USB) a v jaké míře. Všechna tato zařízení tedy lze používat bez rizika zneužití nebo ztráty dat. Systém také zabraňuje v tom, aby skrze tato rozhraní do firemní sítě pronikl škodlivý software. Správa zařízení zajišťuje účinnou ochranu před „vnitřními útočníky".

ŘÍZENÍ PŘÍSTUPU DO CLOUDU

Využití cloudu je velmi výhodné díky větší flexibilitě práce, protože k datům lze přistupovat odkudkoli. Zvláště citlivá data by však neměla být v cloudu ukládána a ukládání některých typů údajů do cloudu je dokonce zakázáno zákonem. Zvláště v takzvaných třetích zemích. Funkce Řízení přístupu do cloudu kontroluje, kteří zaměstnanci mají povoleno používat které cloudové služby a v jaké míře.

ŘÍZENÍ PŘÍSTUPU PRO PŘIPOJOVANÁ ZAŘÍZENÍ

V dnešní době lze data přenášet nejenom oficiálními způsoby prostřednictvím firemní sítě, ale také například pomocí technologií Bluetooth, WiFi, pomocí modemu a jinými metodami. Firma by však měla mít kontrolu nad tím, jakými cestami z ní data odcházejí. Funkce Řízení přístupu pro připojovaná zařízení kontroluje, kteří zaměstnanci mají přístup k jakým službám pro přenos dat.

FILTROVÁNÍ

ANALÝZA A FILTROVÁNÍ OBSAHU

Součástí integrované celkové koncepce zabezpečení musí být i analýza obsahu a odfiltrování tajných informací z dat opouštějících společnost, ale i blokování nepřijatelných informací v datech příchozích. Funkce Analýza a filtrování obsahu zajišťuje podrobnou a spolehlivou ochranu firemních datových komunikací, aniž by ovlivňovala pracovní postupy uživatelů a oprávněné přenosy dat.

ANTIVIROVÁ OCHRANA

Antivirové řešení zajišťuje osvědčenou ochranu proti anonymním útočníkům z internetu. Abyste dokázali velmi rychle reagovat na nové viry a trojské koně, potřebujete vysokou míru detekce. EGOSECURE DATA PROTECTION obsahuje integrované antivirové řešení, které podle mnoha testů patří mezi přední řešení na trhu a vysoká míra detekce je u něj potvrzena.

KONTROLA APLIKACÍ

Tato funkce kontroluje, kteří uživatelé jsou oprávněni spouštět které programy. Tak lze například zabránit spouštění her a nelicencovaného softwaru a vyhnout se tak potenciálním postihům a ekonomickým škodám. Zablokovat lze i většinu virů, a to ještě před jejich odhalením antivirovými programy.

ŠIFROVÁNÍ

ŠIFROVÁNÍ VYMĚNITELNÝCH ZAŘÍZENÍ

Přenosná úložná média, například flash disky, jsou stále menší a jejich výkon přitom roste. To však také znamená, že je lze mnohem snáze ztratit nebo ukrást. Díky šifrování výměnných zařízení nemůže dojít ke zneužití dat neoprávněnými osobami.

Šifrování a dešifrování pomocí hesla lze provést na libovolném počítači se systémem Windows a pro oprávněné uživatele zcela transparentně. Systém šifruje po jednotlivých souborech, k dispozici je navíc několik druhů šifrování, které lze používat i současně na jednom médiu.

ŠIFROVÁNÍ CELÉHO DISKU

Tato funkce zajišťuje komplexní ochranu na všech zařízeních. Šifruje celé disky nebo jejich oddíly na úrovni sektorů. V případě potřeby lze zajistit i ověřování uživatelů ještě před spuštěním operačního systému. Automatická detekce nových pevných disků v integrovaném šifrovacím čipu, bleskové počáteční zašifrování a centrální správa zajišťují bezproblémovou integraci do stávající infrastruktury IT.

AUTENTIZACE PŘED SPUŠTĚNÍM SYSTÉMU

Tato funkce zabraňuje tomu, aby někdo obešel či zmanipuloval přihlášení do systému Windows a související šifrovací funkce, například šifrování disku, pomocí konvertování pevných disků, spuštěním systému z USB nebo CD média nebo výměnou operačního systému. Přihlášení k terminálu se provádí okamžitě po načtení systému BIOS a tedy ještě před spuštěním operačního systému. Kromě hesel je podporováno i přihlášení pomocí mnoha typů chytrých karet. K dispozici jsou i podnikové funkce, například linka podpory a vlastní nastavení výchozích hodnot. Přihlašovací obrazovky lze přizpůsobit podle přání zákazníka.

ŠIFROVÁNÍ SLOŽEK

Šifrování složek chrání data na ztracených přenosných počítačích a pevných discích, ale i jednotlivě definované citlivé údaje na počítačích, k nimž má přístup více uživatelů. Například vysoce citlivé managementové údaje lze chránit proti přístupu zaměstnanců s rozsáhlými oprávněními, jako jsou pracovních IT.

SÍŤOVÉ A CLOUDOVÉ ŠIFROVÁNÍ

Pomocí šifrování v síti a v cloudu lze šifrovat složky v cloudu nebo v jakékoli síti. Šifrovací klíč zůstává ve firmě a nikdy není uložen v cloudu, což je zřejmá výhoda proti šifrovacím řešením, která poskytují sami provozovatelé cloudových úložišť.

ŠIFROVÁNÍ V SYSTÉMECH ANDROID/IOS

Transparentní šifrování v reálném čase pro zařízení se systémem Android a iOS zajišťuje ochranu souborů v interních úložištích, na paměťových kartách a na cloudových účtech mobilních zařízení využívaných aplikacemi. Soubory jsou dešifrovány po zadání hesla.

ŠIFROVÁNÍ POŠTY

Šifrování pošty zajišťuje bezpečnou výměnu e-mailů. Nevyžaduje instalaci softwaru na odesílající ani přijímající počítač. Šifrované e-maily s elektronickým podpisem lze posílat a číst v prostředí, na které je uživatel zvyklý. Lze navíc snadno šifrovat a přenášet i e-maily značné velikosti.

SPRÁVA

SPRÁVA MOBILNÍCH ZAŘÍZENÍ

Stále větší rozšíření mobilních zařízení, například tabletů a chytrých telefonů, se musí odrazit i ve firemní bezpečnostní architektuře. Správa mobilních zařízení zajišťuje inteligentní začlenění mobilních zařízení včetně podpory pro operační systémy Android a iOS.

INVENTÁŘ

Šifrování pošty zajišťuje bezpečnou výměnu e-mailů. Tento modul umožňuje sledovat, jaký hardware a software je instalován v počítačích ve firemní síti. Mnohem důležitější je však to, že pomocí něj lze sledovat a analyzovat změny. V případě, že ke změně dojde, lze poslat upozornění. Můžete si též prohlížet stav hardwaru a spolehlivě tak odhalit případné problémy.

BEZPEČNÉ MAZÁNÍ

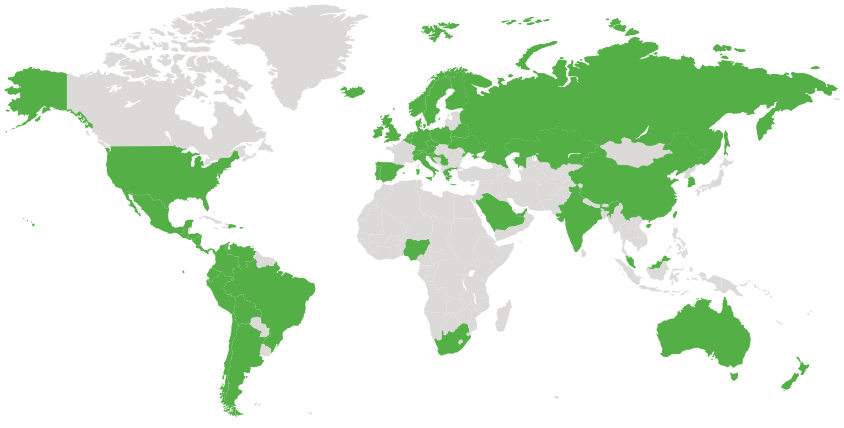
Díky této funkci není možné obnovit smazané soubory, ať se nacházejí na interním pevném disku nebo na externím úložném médiu. Uživatelé mohou zvolit mezi různými způsoby mazání. Mají možnost dokumenty bezpečně mazat okamžitě nebo nenávratně likvidovat smazané soubory v naplánovaných časech. Díky bezpečnému mazání si také můžete být jisti, že při prodeji nebo vyřazení hardwaru dáváte z ruky skutečně jen hardware.

ZELENÉ IT

Inteligentní správa napájení zajišťuje efektivní provoz zařízení. Počítače tedy spotřebovávají energii pouze v případě, že jsou skutečně používány. Funkce Zelené IT snižuje provozní náklady a zároveň přispívá k omezení dopadu společnosti na životní prostředí. Navíc zrychluje návratnost investic do zavedení systému EGOSECURE DATA PROTECTION.

+ FAKTA

- + VÍCE NEŽ 2000 SPOKOJENÝCH ZÁKAZNÍKŮ
- + VÍCE NEŽ 1,4 MILIONU SPRAVOVANÝCH KLIENTŮ
- + VE VÍCE NEŽ 40 ZEMÍCH PO CELÉM SVĚTĚ



FREEDIVISION
for safety reasons

FreeDivision s.r.o.
Rektorská 50/52
108 00 Praha 10, Česká republika
Telefon: +420 220 972 426
E-mail: info@freedivision.com
Web: www.freedivision.com