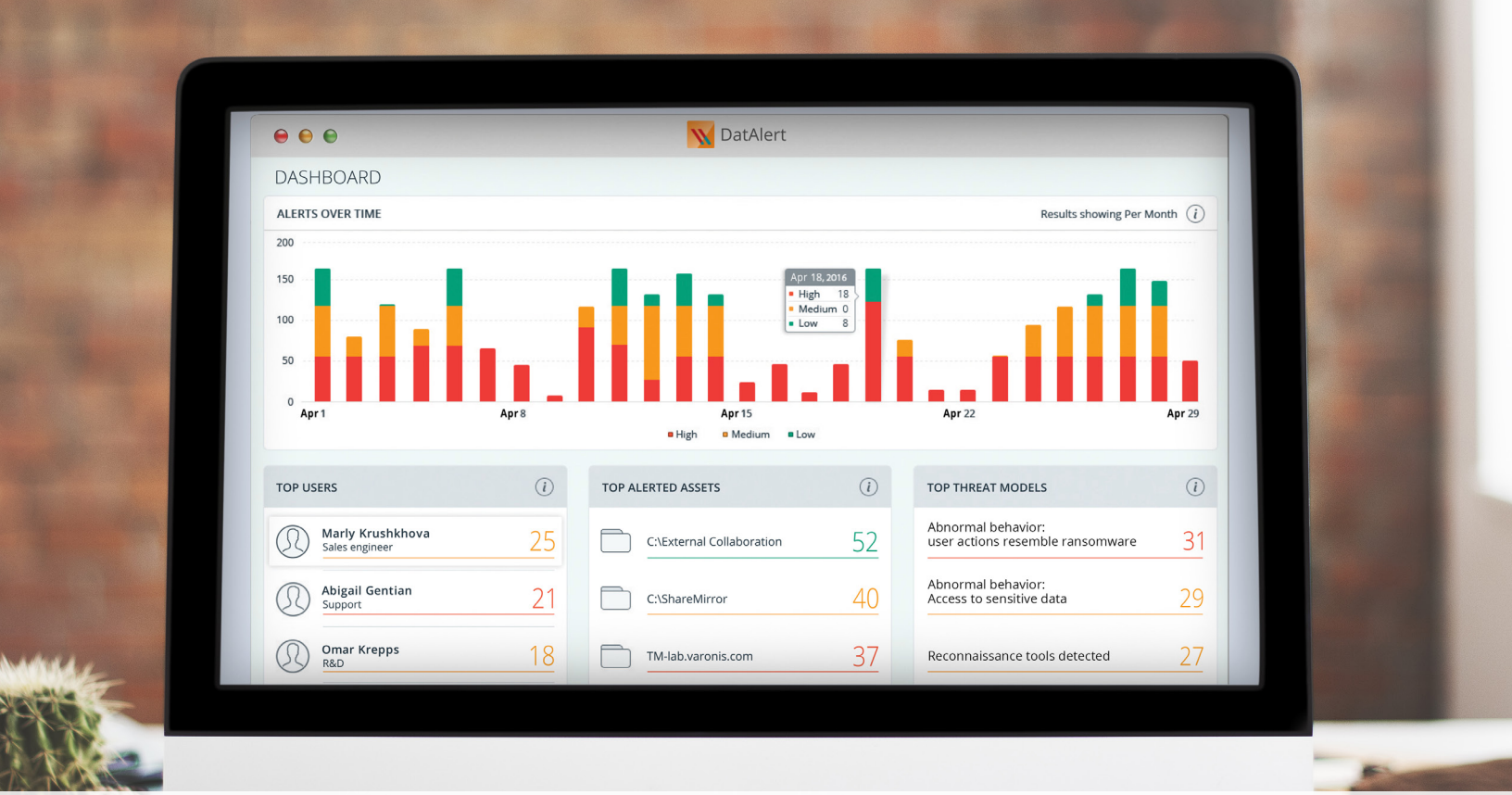


ZASTAVTE RANSOMWARE.

Varonis je výkonná softwarová sada, která vás chrání před kybernetickými útoky i hrozbami zevnitř.

Varonis funguje v celé organizaci – pracuje v naší infrastruktuře, našem Active Directory, na všem hardwaru a softwaru, který máme. Díky němu vidíme, co kde je a co se kde děje.

Nákazu ransomwarem jsme dokázali odhalit a zlikvidovat za 10 minut po napadení.

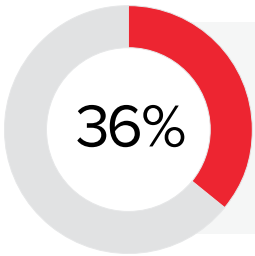
– Wade Sendall | viceprezident IT, Boston Globe

The Boston Globe

www.varonis.cz

VARONIS

ŘEŠENÍ PRO OCHRANU PŘED RANSOMWARE



36 % zákazníků společnosti Varonis odhalilo pomocí nástroje DatAlert ransomware

PODÍVEJTE SE, CO ŘÍKAJÍ JINÍ ZÁKAZNÍCI

Jak to funguje?

Varonis detekuje ransomware ve vašich hlavních systémech IT: na souborových serverech, NAS a v cloudu, kde se nachází terabyty vašich nejdůležitějších dat. Útok pak zastaví hned v počátcích.

Naše architektura obrany před ransomwarem je navržena tak, aby chránila podniková data před dosud nepopsanými útoky. Zachytí tedy i ransomware, který tradiční zabezpečení perimetru neodhalí.

Odhalte ransomware

Zachyťte malware, hrozby ze strany vlastních zaměstnanců i kybernetické útoky zevnitř.

Monitorujte a nechte se upozorňovat na podezřelou aktivitu a chování uživatelů připomínající ransomware pomocí prediktivních modelů hrozeb. Spouštějte automatické reakce, které útok zastaví dřív, než bude pozdě.

Předejděte škodám

Model nejmenších nutných oprávnění omezí rozsah škody, kterou může napadený uživatel napáchat.

Omezte prostor pro útok ransomwaru vyhledáním a zablokováním příliš slabého či chybně nastaveného řízení přístupu, které ransomware a útočníci často zneužívají.

Rychle napravte škody

Zjednodušte obnovu po napadení díky úplným záznamům všeho, co bylo zašifrováno.

Vyšetřujte podezřelé chování a bezpečnostní incidenty a hledáním v komplexním záznamu všech kontaktů se soubory najděte dotčené soubory, uživatele a zařízení.

Proč Varonis?

- Analyzujte chování a aktivitu napříč různými platformami. Odhalujte podezřelou činnost a potenciální úniky dat pomocí hloubkové obrany.

- Odhalte zbytečně široce přístupná citlivá data a globální skupiny, které zpravidla způsobují zbytečně velkou zranitelnost a vážnost infekcí ransomwarem.

- Omezte přístup k citlivým a regulovaným datům a postupujte při nápravě podle priorit. Automatizujte nastolení a udržení modelu nejmenších nutných oprávnění.

- Využívejte modely hrozeb navržené speciálně jako obranu proti malwaru: od detekce šifrování velkého počtu souborů přes vzorce připomínající chování známého ransomwaru až po akce naznačující aktivitu automatizovaného malwaru.

- Zajistěte si nejnovější obranu proti malwaru díky specializované výzkumné laboratoři s odborníky na zabezpečení a datovými vědci, kteří průběžně vyvíjejí nové modely hrozeb, které pomáhají odhalovat i ten nejméně nápadný, dosud nepopsaný malware.

Pokryté platformy

Chraňte svá nejcennější data, ať jsou uložena kdekoli.

ŘEŠENÍ PRO OCHRANU PŘED RANSOMWARE

Praktická ukázka

Nainstalujte systém Varonis ve svém vlastním prostředí a zjistěte, jak se ubránit ransomwaru a chránit svá data.

www.varonis.cz

Analýza bezpečnosti dat

Získejte svůj rizikový profil, zjistěte, zda jste zranitelní, a napravte skutečné bezpečnostní problémy.

www.varonis.cz

Chtěli jsme mít možnost sledovat a zastavit jakýkoli útok ransomwaru a malwaru. DatAlert nám to snadno umožňuje.

Velmi rychle se ukázalo, že tento produkt skutečně funguje – Varonis dělá přesně to, co o sobě tvrdí.

– Ron Mark | manažer inovací a IT, Gas Strategies

Pomáháme tisícům zákazníků chránit se před úniky dat.