NetEvid

Keep your network activities

CENTRALIZES LOGS MANAGEMENT

ระบบจัดเก็บข้อมูล Logs
ตาม พรบ. คอมพิวเตอร์แบบรวมศูนย์

เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เรื่องหลักการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ซึ่งเป็นกฎหมายฉบับหนึ่งที่ผู้ที่มีหน้าที่เกี่ยวข้องไม่สามารถปฏิเสธความรับผิดชอบเพราะถือเป็นหน้าที่และในพระราชบัญญัติดังกล่าว โดยที่ผู้ให้บริการต้องเก็บข้อมูลทางการจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วัน แต่ในกรณีจำเป็นเจ้าหน้าที่สามารถสั่งให้เก็บข้อมูลไว้ได้นานที่สุดคือ 2 ปี

NetEvid เป็นอุปกรณ์ Appliance ที่ออกแบบมาเพื่อจัดเก็บข้อมูล Log ในระบบคอมพิวเตอร์แบบรวมศูนย์ สามารถรองรับ Log จากอุปกรณ์ที่หลากหลาย เช่น Firewall, Router, Switch, IDS, IPS, VPN, Web server, Email server, Database server และระบบปฏิบัติการต่างๆ โดยแสดงผลอยู่ในรูปแบบเดียวกันได้เป็นอย่างดี และมีความสามารถในการบริหารจัดเก็บ Log ปริมาณมากๆ เป็นเวลาระยะยาวนานภายในระบบ อีกทั้งยังมีความสามารถในการค้นหาและสรุปรายงานได้ภายในตัวเอง โดยที่ NetEvid จัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ได้ไม่ต่ำกว่า 90 วัน โดยมีการตรวจสอบความ ครบถ้วนถูกต้องของข้อมูล (Data Integrity) มีความเชื่อมั่น และยืนยันได้ ตรงตามหลักเกณฑ์การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ตาม พ.ร.บ. คอมพิวเตอร์ นอกจากนี้ NetEvid ยังได้การรับรองมาตรฐานของศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560) อีกด้วย

www.netevid.com

Head Office : 18/369 The Primary Ultimate, Soi Nuan chan 28, Bueng kum, Bangkok, 10230 Thailand

Tel: +662 363 8678
Fax: +662 363 8679

www.vrcomm.net

support@vrcomm.net

BEST PERFORMANCE IN EVERYANGLE

ระบบที่มีประสิทธิภาพสูงในการทำงาน
และมีความยืดหยุ่น

รับรองมาตรฐานโดยศูนย์อิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (มศอ. 4003.1-2560)

NetEvid เป็นอุปกรณ์ที่ออกมาแบบการจัดเก็บข้อมูลในรูปแบบ NoSQL โดยที่ข้อดีของ NoSQL คือ สามารถขยายระบบได้ง่าย รองรับข้อมูลขนาดใหญ่ และมีความยืดหยุ่นสูง ทำให้ NoSQL ถูกนำไปใช้กับข้อมูลที่มีขนาดใหญ่ ข้อมูลที่ไม่มีโครงสร้างที่ชัดเจน เช่น การจัดเก็บข้อมูล log นอกจากนี้อุปกรณ์ NetEvid ใช้การค้าหาข้อมูลด้วยการสร้างดัชนี (Index) และใช้การค้นหาแบบ Full Text Search ซึ่งช่วยเพิ่มประสิทธิภาพในการจัดเก็บและการค้นหาให้รวดเร็วยิ่งขึ้น

โดยที่อุปกรณ์ NetEvid สามารถรองรับการใช้งานเพื่อตอบโจทย์การเก็บข้อมูลจราจรคอมพิวเตอร์ให้กับทางลูกค้าได้ครอบคลุมได้ทั้งองค์กรขนาดเล็กไปจนถึงองค์กรขนาดใหญ่ ตามขนาดของตัวอุปกรณ์(Hardware) ที่สามารถรองรับ log ได้ตั้งแต่ 1,500 EPS จนถึงอุปกรณ์ที่รองรับ log ได้ถึง 60,000 EPS

นอกจากนี้สำหรับองค์กรที่ต้องการเสถียรภาพในการทำงานอุปกรณ์ NetEvid สามารถรองรับการทำงานในลักษณะ High-Availability (HA) ได้อีกด้วยและสามารถรองรับการขยายเพิ่มเติมในอนาคตได้

ข้อมูลที่จัดเก็บมีความปลอดภัยสูงสุด

NetEvid ถูกออกแบบให้ข้อมูลที่ถูกจัดเก็บมีการเข้ารหัส และ Hash ด้วยกระบวนการ SHA-256 ป้องกันการเปลี่ยนแปลงแก้ไข ลบ ข้อมูล เพื่อความสมบูรณ์ของข้อมูลที่ถูกจัดเก็บ และสอดคล้องกับข้อกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ด้วยอัตราส่วนการบีบอัดข้อมูลได้มากถึง 15 ต่อ 1 ทำให้สามารถเก็บข้อมูลได้นานกว่า 90วันตามข้อกำหนดของพระราชบัญญัติฯ และสามารถขยายการจัดเก็บข้อมูลได้สูงสุดถึง 2 ปี

ระบบปฏิบัติการของ NetEvid ถูกออกแบบให้มีความแข็งแกร่ง มีระบบไฟร์วอลล์ป้องกันจากการโจมตีผ่านช่องโหว่ เพื่อให้ข้อมูลที่ถูกจัดเก็บมีความคงทนสูง ไม่สูญหาย และพร้อมใช้งานตลอดเวลา

สามารถรับ Log ได้หลายรูปแบบ

NetEvid สามารถจัดเก็บ Log ช่องทางหลัก โดยสามารถจัดเก็บผ่านทาง Protocol syslog standard ซึ่งอุปกรณ์เกือบทุกชนิดส่วนใหญ่จะส่ง Log ผ่านทางช่องทางนี้เป็นหลัก ไม่ว่าจะเป็น Router, Switch, Firewall, System, Application เป็นต้น

NetEvid ยังสามารถจัดเก็บ Log จากช่องทางอื่น ๆ ในกรณีที่อุปกรณ์ไม่สามารถส่ง syslog ได้ ซึ่งมีเพียงอุปกรณ์บางยี่ห้อเท่านั้นที่จะส่ง Log ผ่านทาง OPSEC Platform และ FTP Protocol อุปกรณ์ NetEvid ได้พัฒนาให้มี OPSEC Agent และ FTP Agent เพื่อทำการรับ Log จากอุปกรณ์นั้น ๆ ได้

สามารถส่ง Log ต่อไปยังอุปกรณ์อื่นได้

NetEvid สามารถทำงานในลักษณะเป็นคนส่ง Log ที่ได้รับมาแล้วไปให้กับอุปกรณ์รับ Log ยี่ห้ออื่น ๆ เช่น ส่งต่อให้ SIEM นำ Log ไปวิเคราะห์เพิ่มเติม หรือให้ NetEvid ทำหน้าที่เป็น caching โดยการเก็บ Log ไว้ก่อน แล้วจึงเลือกส่ง Log บางประเภทไปให้ SIEM ทำการวิเคราะห์ต่อไป ซึ่งจะช่วยลดปริมาณข้อมูล Log ที่จะส่งไปให้กับ SIEM เป็นต้น

สามารจัดทำรายงานได้หลายรูปแบบ

NetEvid มาพร้อมกับความสามารถในการจัดทำรายงานจาก Log ที่ได้รับจากอุปกรณ์ต่าง ๆ เช่น Firewall, Proxy, Active Directory, Exchange มาสรุปเป็นรายงานของแต่ละอุปกรณ์ เช่น Top N ต่าง ๆ และยังสามารถปรับแต่งรูปแบบการแสดงรายงานได้หลายรูปแบบ เช่น PDF, RTF, XML, XLSX, CSV, HTML, XHTML, text, DOCX, และ OpenOffice เป็นต้น

NetEvid สามารถสร้างรายงานแบบรายครั้ง (ad-hoc report) ในรูปแบบ รายวัน, รายสัปดาห์ หรือรายเดือน โดยสามารถ filter อุปกรณ์บางตัวที่ต้องการให้แสดงในรายงานได้ และยังรองรับการตั้งเวลาล่วงหน้าในการจัดทำรายงาน พร้อมทั้งจัดส่งรายงานที่ทำเสร็จแล้วไปยัง E-mail ของผู้ดูแลระบบได้

คุณสมบัติหลัก

- บริหารจัดการ Log แบบรวมศูนย์ได้ตามข้อกำหนด
- เก็บรวบรวม Log ได้รวดเร็วและครบครัน
- ค้นหา Log ได้รวดเร็วด้วยการมีสารบัญ Log
- รองรับการบันทึกข้อมูลและค้นหาได้สูงสุดถึง 2 ปี
- มีความปลอดภัยสูงด้วยการจัดเก็บแบบ Hashing SHA-256 และจัดเก็บแบบถาวร
- สามารถปรับแต่งรูปแบบของรายงานได้หลากหลาย
- สามารถออกรายงานแบบ On Demand และแบบตั้งเวลาส่ง
- HTTPS CLI SSH รองรับการทำงานผ่าน HTTPS , command line interface และ SSH
- LDAP รองรับการตรวจสอบสิทธิ์ด้วย LDAP
- สามารถควบคุมการเข้าถึงข้อมูลได้โดยการกำหนดตามสิทธิ์ของการอนุญาตโดยแบ่งการเข้าถึงเป็นผู้ดูแลระบบและผู้ดูแลข้อมูล และไม่จำกัดจำนวนผู้เข้าใช้งาน
- รองรับการส่งต่อ Log ไปยังอุปกรณ์อื่นได้
- รองรับการบันทึกข้อมูล กับ อุปกรณ์จัดเก็บข้อมูลภายนอก เช่น External storage หรือ DVD ได้
- มีความสามารถในการค้นหาที่มีประสิทธิภาพ โดยสามารถรองรับเงื่อนไขในการค้นหาได้หลายเงื่อนไข ทั้งในรูปแบบ Wildcard expressions, Boolean expressions และ Regular expressions
- มีความสามารถแจ้งเตือนผ่าน E-mail ไปยังผู้ดูแลระบบเมื่อมีเหตุการณ์ผิดปกติของตัวอุปกรณ์ หรือตรงตามเงื่อนไขที่ตั้งไว้
- % สามารถแสดงค่าเฉลี่ยของการรับ Log (Average EPS) และแสดงจำนวน Log ที่รับสูงสุด (Peak EPS) ในแบบรายวัน รายสัปดาห์ และรายเดือนได้
- มีความสามารถตรวจสอบสถานะของอุปกรณ์ที่ส่ง Log เข้ามาว่ายังทำงานอยู่ได้
- มีความสามารถแจ้งเตือนไปยังผู้ดูแลระบบผ่าน E-mail เมื่อไม่มี log ส่งเข้ามายังระบบ และบอกวันสุดท้ายของ Log ที่ส่งเข้ามายังระบบได้
- มีความสามารถแยกการเก็บ Log ตามหน่วยงานและแยกสิทธิ์การเข้าถึงได้
- IPv4 IPv6 สามารถค้นหาข้อมูล Log จากอุปกรณ์ที่ส่ง Log ผ่านทาง IPv4 และ IPv6
- NTP สามารถทำงานเป็น NTP Server ให้กับอุปกรณ์อื่นๆ ภายในเครือข่ายได้

Product Specification

NetEvid
Keep your network activities

	V120	V320	V520	V720	V1200
Software Specification					
Management	HTTPS,SSH	HTTPS,SSH	HTTPS,SSH	HTTPS,SSH	HTTPS,SSH
Performance(EPS)	1,500 EPS	3,500 EPS	5,500 EPS	7,500 EPS	15,000 EPS
No. of Users	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Devices support	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Notification	Email, Syslog, Line	Email, Syslog, Line	Email, Syslog, Line	Email, Syslog, Line	Email, Syslog, Line
Log retention	90 days+	90 days+	90 days+	90 days+	90 days+
Report	Yes	Yes	Yes	Yes	Yes
Hardware Specification					
Processor	Single Processor	Dual Cores	Quad Cores	Quad Cores	Quad Cores
Memory	4 GB	8 GB	8 GB	8 GB	16 GB
Harddisk	1TB HDD, 7.2K RPM	4TB HDD, 7.2K RPM	4TB HDD, 7.2K RPM	4TB HDD, 7.2K RPM	2 x 4TB HDD, 7.2K RPM
RAID	No	Optional	Optional	Optional	0, 1
Network	10/100/1000 BaseTX	2x10/100/1000 BaseTX	2x10/100/1000 BaseTX	2x10/100/1000 BaseTX	2x10/100/1000 BaseTX
Serial Port	No	Yes	Yes	Yes	Yes
Dual Power Supply	No	No	No	No	No
Chassis from factor	211 x 116 x 28 mm.	19" 1U	19" 1U	19" 1U	19" 1U

	V3200	V3200-S	V6200
Software Specification			
Management	HTTPS,SSH	HTTPS,SSH	HTTPS,SSH
Performance (EPS)	30,000 EPS	30,000 EPS	60,000 EPS
No. of Users	Unlimited	Unlimited	Unlimited
Devices support	Unlimited	Unlimited	Unlimited
Notification	Email, Syslog, Line	Email, Syslog, Line	Email, Syslog, Line
Log retention	90 days+	90 days+	90 days+
Report	Yes	Yes	Yes
Hardware Specification			
Processor	Octa Cores	Octa Cores	Dual Processors 8 Cores
Memory	32GB	32GB	64GB
Harddisk	2 x 8TB HDD, 7.2K RPM 2 x 480GB SSD	2 x 8TB HDD, 7.2K RPM 2 x 480GB SSD	8 x 4TB HDD, 7.2K RPM 2 x 480GB M.2 SSD
Harddisk Hot Swap	Yes	Yes	Yes
RAID	0,1,5,10	0,1,5,10	0,1,5,10
Serial Port	Yes	Yes	Yes
Network	2 x 10/100/1000 BaseTX	2 x 10/100/1000BaseTX	2 x 10/100/1000BaseTX, 2 x 10GbE (up to 6 Interfaces)
Dual Power Supply	No	Yes	Yes
Chassis from factor	19" 1U	19" 1U	19" 2U

VM series	
Support	VMware-ESX, Hyper-V, Virtual Box