



SOFTNIX LOGGER

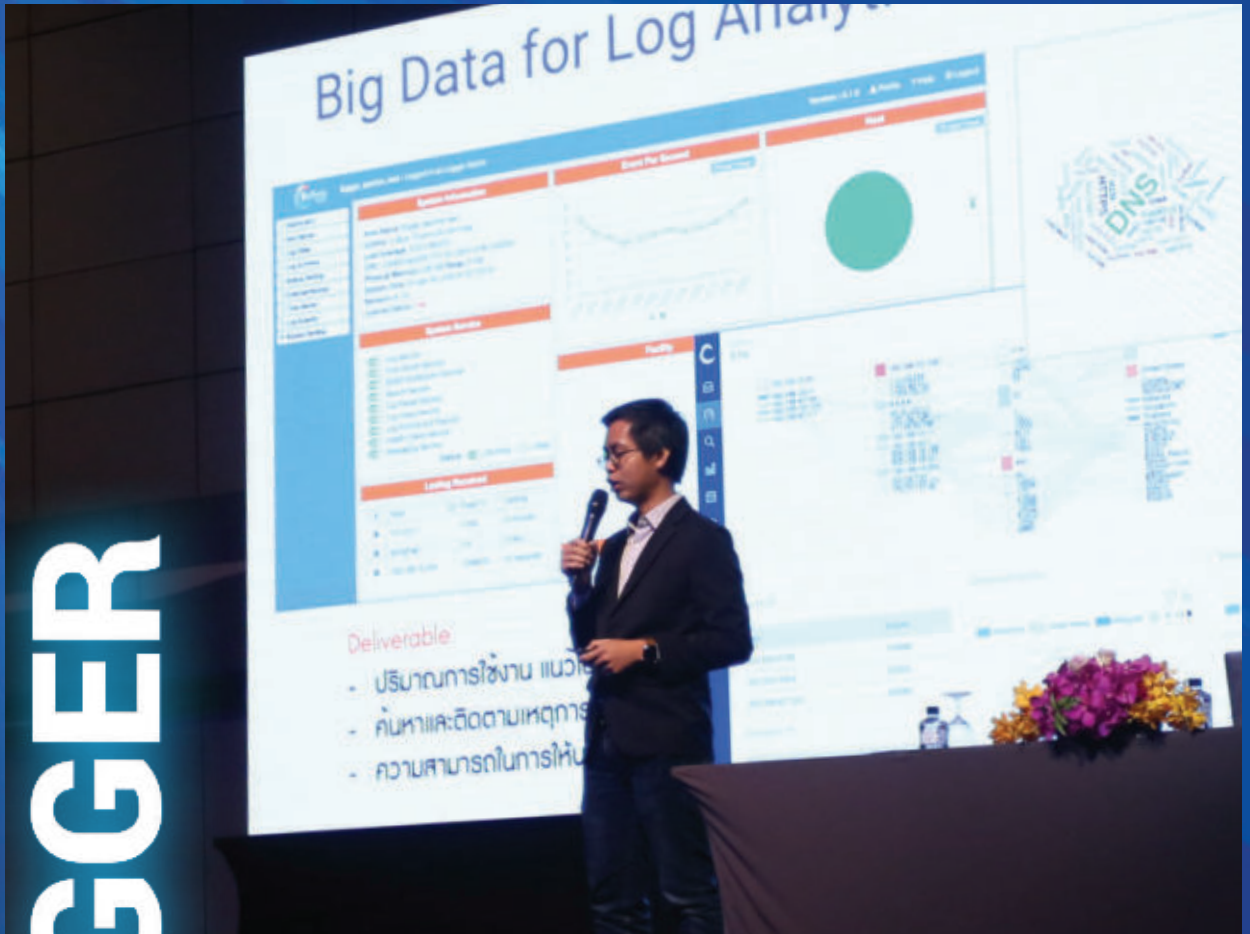
Centralized Log
Management



ผ่านการรับรองมาตรฐาน
ที่องค์กรชั้นนำเลือกใช้

SOFTNIX LOGGER

คืออะไร



SOFTNIX LOGGER

เป็นระบบจัดเก็บล็อกไฟล์หรือข้อมูลจราจรทางคอมพิวเตอร์แบบรวมศูนย์โดยทำงานเป็น SYSLOG SERVER เพื่อรวบรวมล็อกไฟล์ที่เกิดจาก SERVER และอุปกรณ์ในเครือข่ายคอมพิวเตอร์ที่เป็น APPLIANCE และ NON APPLIANCE เพื่อปฏิบัติตามกฎหมาย พ.ร.บ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.2560 ซึ่งประกาศไว้ใน

“ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม”
เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ โดยผลิตภัณฑ์ SOFTNIX LOGGER ได้ผ่านมาตรฐาน มคอ.4003.1-2560 โดยมีรายงานผลการทดสอบอย่างถูกต้อง



การบริหารจัดการ

SOFTNIX LOGGER บริหารจัดการผ่านเว็บเบราว์เซอร์ ในโหมดการเข้ารหัส SSL หรือ HTTPS ผู้ดูแลระบบสามารถตรวจสอบการทำงานปริมาณคือไฟล์ สถิติ รายงานการตั้งค่าแจ้งเตือนอัตโนมัติ กำหนดสิทธิ์ในการเข้าถึงข้อมูลในลักษณะ: ROLE BASED – ACCESS CONTROL ได้ อาทิเช่นผู้ที่ดูแลข้อมูลสามารถเห็นเฉพาะข้อมูล LOG เท่านั้นและกำหนดผู้ดูแลระบบที่เข้าถึงได้เฉพาะการตั้งค่าของระบบเท่านั้น



การรักษาข้อมูลและความถูกต้อง

SOFTNIX LOGGER มีระบบจัดเก็บคือไฟล์อย่างปลอดภัยสูงสุดโดยมีกระบวนการ HASHING 3 วิธี คือ MD5, SHA1 และ SHA-256 โดยเราสามารถตรวจสอบในภายหลังได้ว่าข้อมูล LOG มีความถูกต้องหรือไม่ ด้วยการเปรียบเทียบรหัส HASHING สำหรับด้านการรักษาข้อมูล ระบบมีการป้องกัน การลบ แก้ไข ทำลายในการเข้าถึงข้อมูลนั้นจะต้องกำหนดสิทธิ์ AUTHORIZATION ก่อนเสมอทุกครั้งที่มีการส่งออก EXPORT ข้อมูลจะมีการบันทึก LOG ไว้เสมอ



คุณค่าในการลงทุน

SOFTNIX LOGGER เราพัฒนาขึ้นตามข้อปฏิบัติตามข้อกำหนดกฎหมายประเทศไทย โดยเฉพาะ เราจึงพร้อมที่พัฒนา อับเดทผลิตภัณฑ์ให้สอดคล้องตามกำหนดที่มีการเปลี่ยนแปลงอยู่เสมอ การลงทุนในผลิตภัณฑ์ของเราจึงเรียกได้ว่าคุ้มค่า พิสูจน์ได้จากลูกค้าของเราที่มีอยู่ทุกกลุ่มธุรกิจมั่นใจในการเลือกใช้ผลิตภัณฑ์ของเราในการจัดเก็บรักษา LOG FILE ตาม พ.ร.บ.คอมพิวเตอร์ ทำให้เราเป็นผู้นำระบบบริหารจัดการ LOG แบบรวมศูนย์ ตามข้อกำหนด พ.ร.บ.คอมพิวเตอร์ในปัจจุบัน



อันดับ1 ระบบจัดเก็บ LOG FILE แบบรวมศูนย์ ตาม พ.ร.บ.คอมพิวเตอร์ 2560 ที่องค์กรชั้นนำเลือกใช้

SOFTNIX LOGGER เหมาะสำหรับองค์กรทั่วไปเพื่อจัดเก็บ LOG FILE ของ SERVER, ROUTER, SWITCH, FIREWALL, VPN SERVER และอุปกรณ์เครือข่ายตามพ.ร.บ.คอมพิวเตอร์กำหนด หรือองค์กรขนาดใหญ่ที่มี SERVER จำนวนมากต้องการระบบรวบรวมข้อมูล LOG เพื่อง่ายต่อการวิเคราะห์ปัญหาของระบบ IT OPERATION ที่มีความสำคัญต่อธุรกิจอย่างมากในปัจจุบัน

SOFTNIX LOGGER ยังมีส่วนของการรายงาน LOG USAGE REPORT แสดงปริมาณ EPS PER HOST, STORAGE PER HOST, EVENT PER HOST และ TOP 10 โดยสามารถ EXPORT เป็นไฟล์สกุล PDF, CSV และ JSON ซึ่งเป็นรายการสรุปข้อมูลสำคัญ



ระบบค้นหาที่ง่าย และ ทรงพลัง

SOFTNIX LOGGER มีเทคโนโลยีการค้นหาข้อมูล (SEARCH) ได้จากทุกเนื้อความในข้อมูล LOG ที่ส่งเข้ามาได้ ทั้งแบบ KEYWORD, FIELD, BOOLEAN EXPRESSION, REGULAR EXPRESSION และสามารถ INDEX ข้อมูล LOG เพื่อประสิทธิภาพในการค้นหา โดยรองรับทั้งแบบ Full-Text Search และแบบกำหนด Field ในการค้นหาโดยสามารถระบุเงื่อนไขในการค้นหาได้เช่น AND, OR, Wildcard และกำหนดช่วงเวลาในการค้นหาได้ในระดับวันที่ เวลา ได้เป็นอย่างดี และเงื่อนไขในการค้นหาสามารถบันทึกไว้เพื่อทำการค้นหาภายหลังที่ต้องการได้ และระบบ INDEX รองรับการทำงานแบบ ACTIVE - ACTIVE เป็น HA MODE เพื่อรองรับความต้องการ INDEX ข้อมูลปริมาณมากๆ เพื่อใช้ในด้านการวิเคราะห์เหตุการณ์



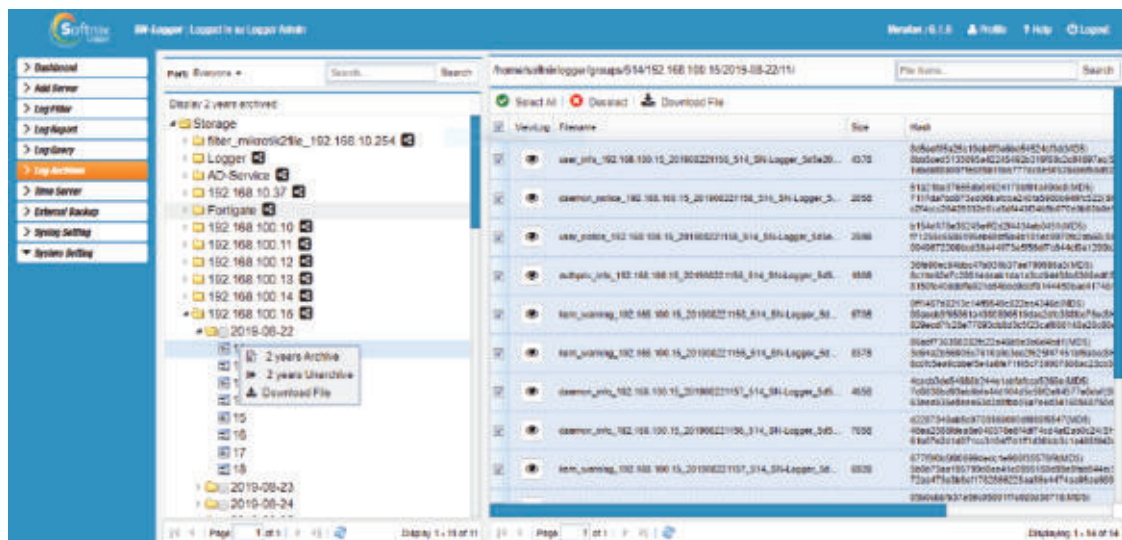
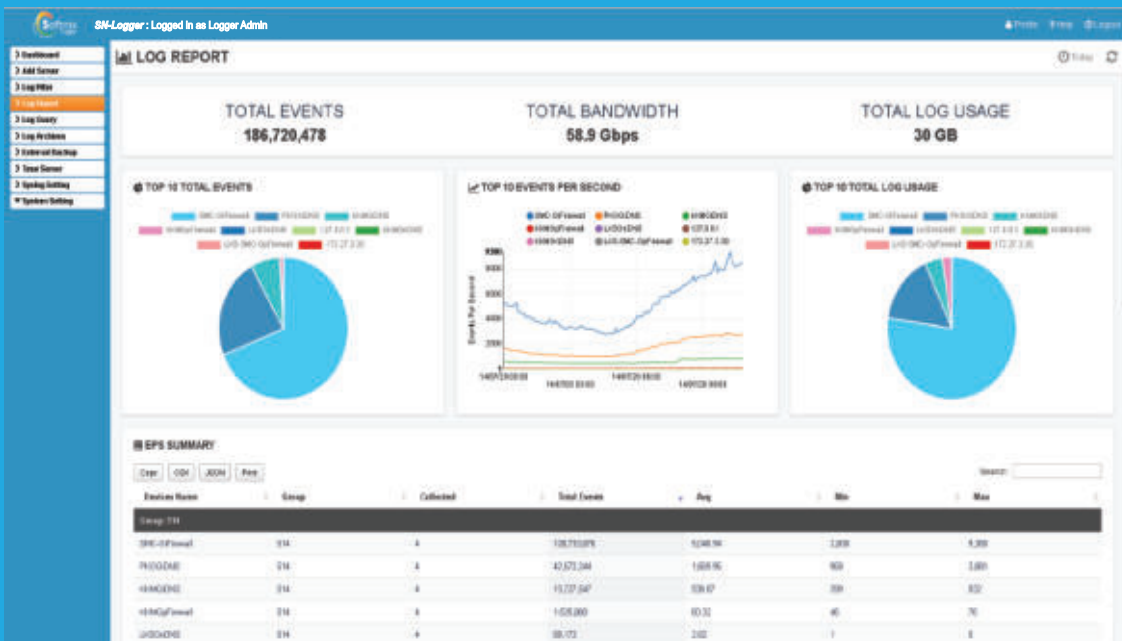
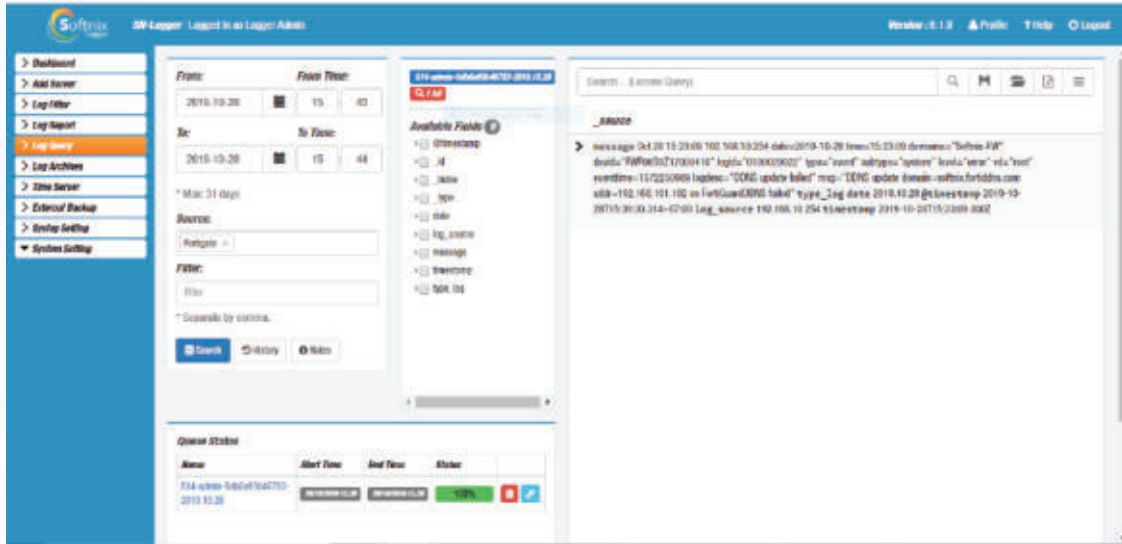
รายงานสถิติการใช้งาน

SOFTNIX LOGGER มีรายงานอยู่ 2 ชนิด ได้แก่ รายงานผลการจัดเก็บข้อมูลคือไฟล์ อาทิเช่นปริมาณข้อมูล จำนวนเหตุการณ์ ระยะเวลาที่จัดเก็บกลุ่มของอุปกรณ์และชนิดของรายงานคือ รายงานสถิติตามเหตุการณ์ โดยขึ้นอยู่กับชนิดของข้อมูลคือ เช่น ล็อกจากอุปกรณ์ FIREWALL เราสามารถสร้างรายงาน TOP N จาก IP ADDRESS, USERNAME, SERVICES APPLICATION, WEBSITE, BANDWIDTH ขึ้นอยู่กับว่าล็อกมีข้อมูล จำเป็นมากน้อยเพียงใด รูปแบบรายงานเราสามารถ PREDEFINED REPORT ไว้ล่วงหน้าตามความต้องการ โดยกำหนดรูปแบบได้ทั้งแบบกราฟ ตารางข้อมูล และแฮช หรือ ส่งออก ข้อมูลในรูปแบบ CSV, PDF และ JSON นอกจากนี้ยังรองรับ API สำหรับการเชื่อมต่อกับระบบอื่นๆได้อีกด้วย เรารองรับการสร้างรายงานจากเหตุการณ์ ครอบคลุมอุปกรณ์ หรือ ระบบต่างๆดังต่อไปนี้ FIREWALL, WINDOWS OS, LINUX OS, MAIL SERVER, PROXY, WEB SERVER และอื่นๆมากมายโดยปรับแต่งได้ตามความต้องการ



จัดเก็บรักษาข้อมูลตามระยะเวลาที่ต้องการ

ระบบ LOG ARCHIVE คือส่วนจัดเก็บรักษา RAW DATA ที่สำคัญพร้อมกับรหัสยืนยันความคงสภาพ (INTEGRITY) โดยวิธีการ MD5, SHA-1 และ SHA-256 โดยสามารถกำหนดระยะเวลาจัดเก็บได้ไม่ต่ำกว่า 90 วัน หรือ 2 ปี ได้ตามความต้องการโดยมีโครงสร้างการจัดเก็บข้อมูลเป็นรายอุปกรณ์ ปี-เดือน-วัน ที่ง่ายต่อการเข้าถึง

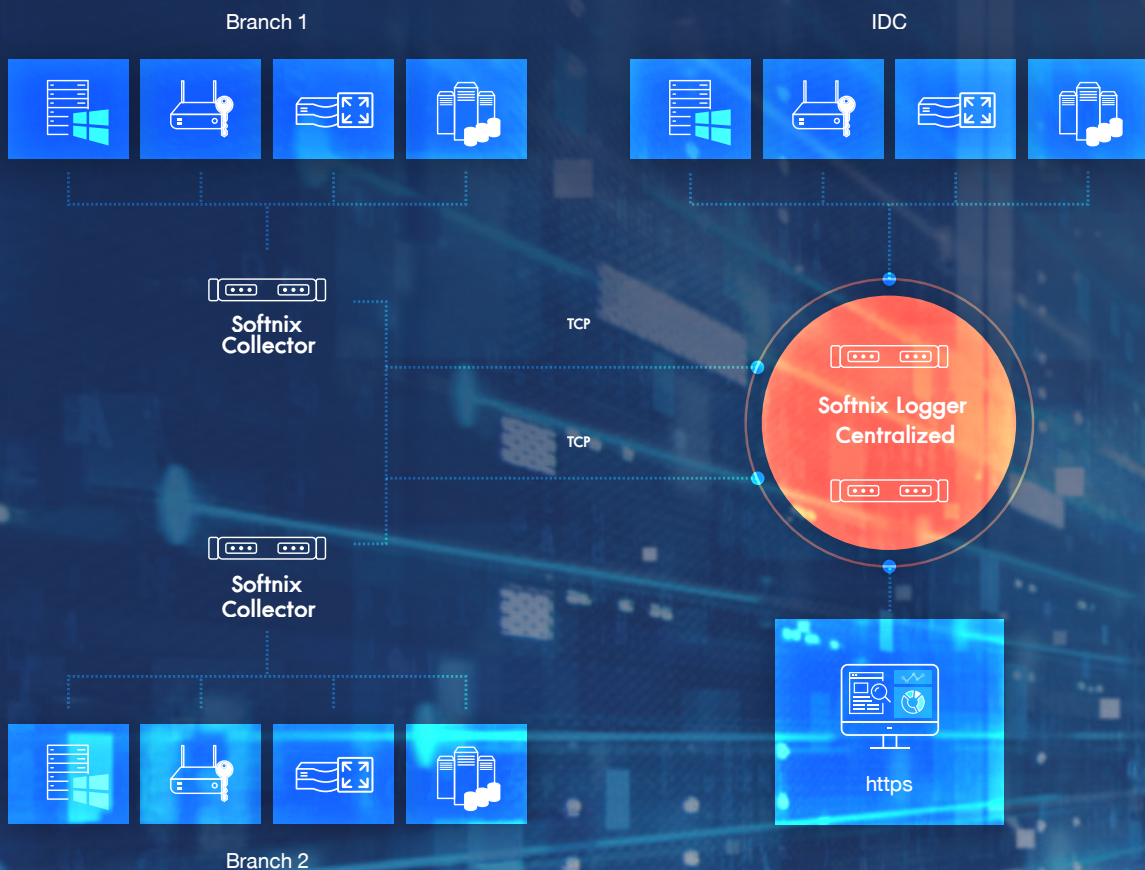


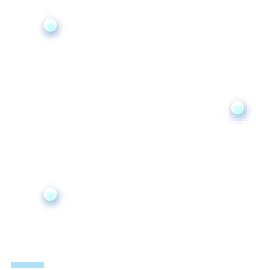
ยืดหยุ่นในการติดตั้งและใช้งาน

มีผลกระทบต่อระบบเครือข่ายเดิมน้อยที่สุด

การบริหารจัดการข้อมูลแบบรวมศูนย์

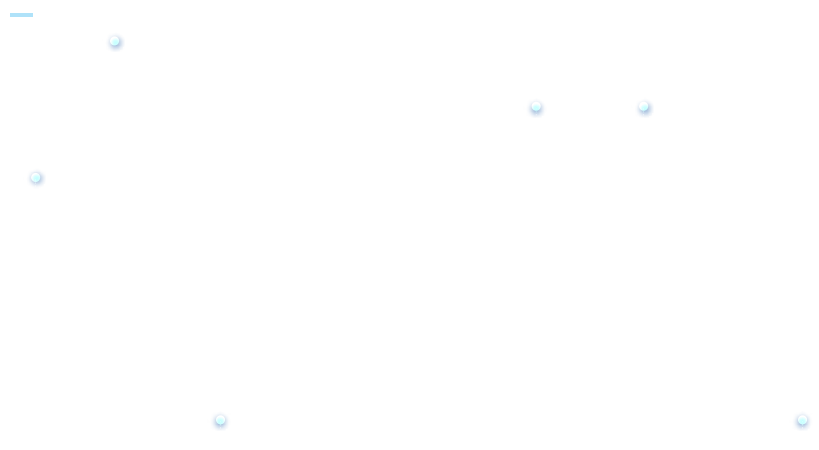
Softnix Logger รองรับการติดตั้งแบบ Collector Mode หรือ Forwarder Mode สิ่งที่แตกต่างกันระหว่าง 2 Mode นี้คือ Collector Mode จะไม่จัดเก็บ Log File ที่ตัวเองแต่จะ Buffer หรือ Caching ในกรณีที่ไม่สามารถเชื่อมต่อกับส่วนกลางได้ละส่งต่อไปยัง Server ที่ทำงานเป็น Centralized Mode นอกจากนี้ระบบยังรองรับ Fault-Tolerance Guarantees ในกรณีที่ส่งไปยัง Centralized Server เพื่อให้มั่นใจได้ว่าข้อมูลครบถ้วนและสมบูรณ์ที่สุด ตัวอย่างการใช้งาน Collector Mode ได้แก่ การติดตั้ง Collector Server ไว้ยังสำนักงานสาขา เพื่อจัดเก็บ Log File มาเก็บยัง Centralized Server ที่สำนักงานใหญ่เพื่อง่ายต่อการบริหารจัดการ





การขยายระบบ (Scalability)

การขยายระบบสามารถทำได้ 2 วิธีคือ Vertical Scalability และ Horizontal Scalability โดย Hadoop ได้จัดทำให้ออกจากระบบเดิมและเพิ่มโหนดเพื่อเก็บข้อมูลได้อีกด้วย

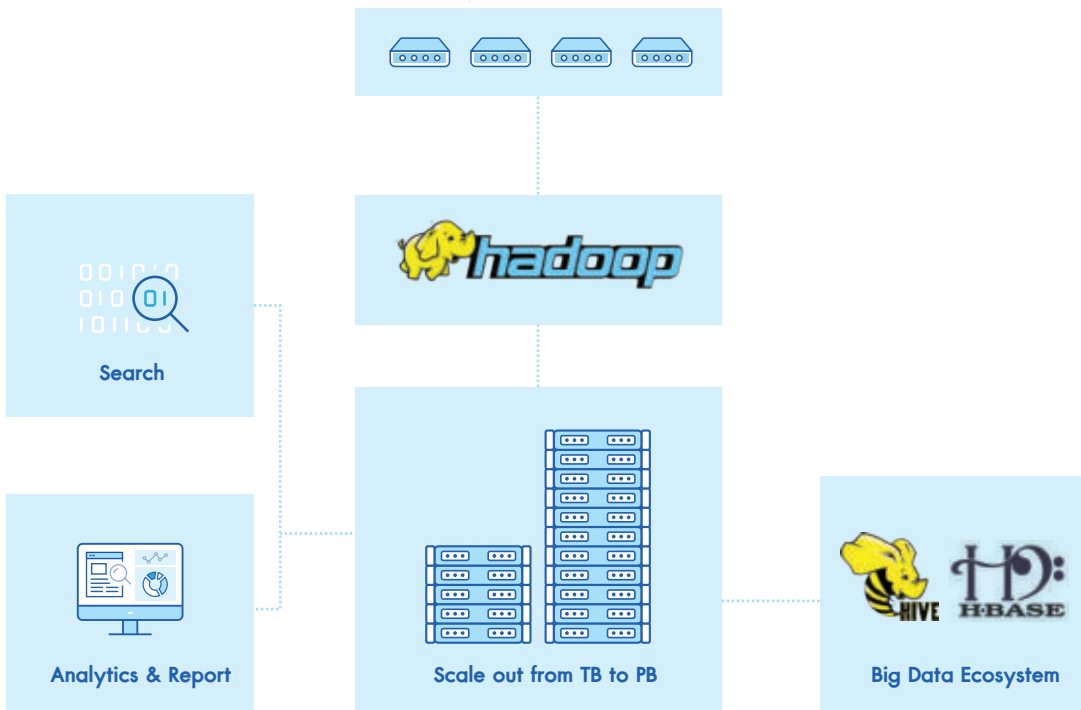




โซลูชันระบบจัดเก็บล็อกไฟล์

สำหรับ CARRIER GRADE เหมาะสำหรับ ISP,
ผู้ให้บริการโทรคมนาคมและ ผู้ให้บริการเครือข่ายขนาดใหญ่

SOFTNIX LOGGER รองรับการจัดเก็บ LOG CGNAT ของผู้ให้บริการอินเทอร์เน็ต
ซึ่งมีปริมาณ LOG มหาศาล เรามีประสบการณ์และเข้าใจลูกค้าว่าต้องการประมวลผล
ข้อมูลมหาศาลพร้อมทั้งยังสามารถค้นหาข้อมูลสำคัญใน NAT EVENTS เช่น PUBLIC IP,
PRIVATE IP, SRCIP, DSTIP, PORT, USERNAME/MSISDN และอื่นๆตามความต้องการได้



SOFTNIX LOGGER EDITION

	BR- 1	BR- 2	SLG-SA 1	SLG-SA 2	SLG-SA 3	SLG-SA 4	ENTERPRISE SOFTWARE
USER ENVIRONMENT	Small Branch	Medium-Large Branch	Small-Medium Enterprise	Medium Enterprise	Large Enterprise	Telco/ISP	Flexible
PROCESSOR	Quad Core 2.0 GHz	Intel Core i3 4160	Intel Xeon E-2100	Intel Xeon E-2100	Intel Xeon E-2100	Intel Xeon 4200	Minimum CPU Intel Xeon Multi-core
DEVICE SUPPORT	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
EPS RATE	3,000	5,000	10,000	15,000	30,000	60,000	-
MEMORY	4GB	8GB	8GB	16GB	32GB	64GB	Minimum 4GB
NETWORK INTERFACE	4x1 Gigabit LAN Ports	6x1 Gigabit LAN Ports	2x Gigabit NIC	2x Gigabit NIC	2x Gigabit NIC	4x 10Gigabit NIC	1 Gigabit NIC
INTERNAL STORAGE	120 GB	240 GB	500 GB	1TB	2TB - 8TB	10TB - 28TB	Custom
EXTERNAL STORAGE	Support	Support	Support	Support	Support	Support	Custom
STANDARD	FCC, CE	FCC, CE	FCC, CE, RoHS, UL	FCC, CE, RoHS, UL	FCC, CE, RoHS, UL	FCC, CE, RoHS, UL	N/A
REDUNDANT POWER	N/A	N/A	N/A	N/A	Redundant	Redundant	N/A
MAINTENANCE SUPPORT	1 year maintenance support include installation, onsite 3 time/year, helpdesk by phone, remote, email, customer portal system						
DIMENSIONS	Height 134 mm Width 126 mm Depth 36 mm	Height 440 mm Width 250 mm Depth 44.5 mm	Height 1.7"(43mm), Width 17.2"(437mm), Depth 19.8" (5.3mm). Supported Rack 19" Standard			Height 3.5"(89mm), Width 17.2"(437mm), Depth 25.6" (648mm). Supported Rack 19" Standard	N/A

เหตุผลที่ลูกค้า

ไว้วางใจเลือกเรา

เหตุผลทางด้านธุรกิจ



ความเหมาะสมและคุ้มค่าในการลงทุน

ด้วยบทกโทษปรับไม่เกิน 500,000 บาทสำหรับผู้ไม่เก็บรักษาข้อมูลไฟล์ตามข้อบังคับและเราคือผลิตภัณฑ์ที่มีราคาตรงตามข้อกำหนดราคาตามกรมบัญชีกลาง และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



ความยืดหยุ่น

เนื่องด้วยเราคือผู้พัฒนาซอฟต์แวร์ เราจึงสามารถรับรายงานปัญหา และแก้ไข ได้อย่างทันที พร้อมทั้งการปรับปรุงผลิตภัณฑ์เพื่อให้ตอบสนองต่อการ ใช้งานได้ง่าย



การค้นหาข้อมูลที้ง่ายและรายงานเชิงสถิติ

ธุรกิจต้องการการตัดสินใจที่รวดเร็ว การวิเคราะห์ปัญหาอย่างรวดเร็ว และการเข้าถึงข้อมูล ICT เชิงสถิติ สามารถนำไปสู่การตัดสินใจทางธุรกิจได้อย่างถูกต้อง



ประหยัดต้นทุนในการใช้สต่อเรขขนาดใหญ่

STORAGE เป็นทรัพยากรที่มีต้นทุนที่แปรผันตามปริมาณความจุของข้อมูล ด้วยระบบบีบอัดที่ทรงพลัง จะช่วยลดค่าใช้จ่ายได้หลายเท่า



มาตรฐานและความเชื่อมั่น

ผลิตภัณฑ์เราผ่านการตรวจสอบคุณสมบัติจนได้รับมาตรฐาน มคอ.4003.1-2560 อ้างอิงรายงานหมายเลข63-0001 อีกทั้งประสบการณ์ในการพัฒนาซอฟต์แวร์ระบบการจัดการสื่อ คลื่นรวม ศูนย์มาตั้งแต่ก่อตั้งบริษัท ปี ค.ศ. 2007 จนถึงปัจจุบันอย่างต่อเนื่อง จึงเป็นสิ่งชี้ให้เห็นว่าเรามีความมุ่งมั่นเพียงใดในสิ่งที่เราทำ

คุณสมบัติทั้งหมด

- เสถียรภาพ มั่นคง และปลอดภัย
- ไม่จำกัดจำนวนอุปกรณ์และผู้ใช้
- บริหารจัดการผ่านเว็บและ COMMAND LINE INTERFACE (SSH)
- รองรับ SYSLOG (RFC 3164, 5424) และ NON SYSLOG
- รองรับ FTP, SFTP, OPSEC, SNMP TRAP และ SYSLOG AGENT
- ทำหนดระยะเวลาในการจัดเก็บข้อมูล 90 วันค่าเริ่มต้น หรือ 2 ปี
- ระบบ DATA HASHING MD5, SHA-1, SHA-256
- สามารถกำหนดชื่ออุปกรณ์ที่ส่ง LOG ได้ (ALIAS NAME)
- ระบบแจ้งเตือนอัตโนมัติเมื่อไม่มีสื่อส่งเข้ามา
- ระบบ INDEX ค้นหาข้อมูล
- แสดงผลจากการค้นหาในรูปแบบเดียวกันตามมาตรฐาน RFC3164, 5424
- กำหนด LOG FILTER และตั้งค่าแจ้งเตือน
- รองรับ INTERNAL CACHING ป้องกันข้อมูลสูญหาย
- รองรับ ACTIVE DIRECTORY, LDAP AUTHENTICATION และ TWO FACTOR AUTHENTICATION
- ระบบออกรายงานตามประเภทของสื่อไฟล์ (เชิงสถิติ)
- รองรับ TIME SERVER
- เชื่อมต่อกับ EXTERNAL BACKUP เช่น EXTERNAL STORAGE NAS, TAPE BACKUP, SAN
- รองรับ ARCHIVE DATA
- รองรับการเข้ารหัส (ENCRYPT) LOG ด้วย ALGORITHM IIU AES-256
- รองรับการติดตั้งแบบ HIGH AVAILABILITY
- รองรับการจัดเก็บ LOG แบบ SYSLOG ที่เกิดขึ้นจากอุปกรณ์เครือข่าย และ NON-SYSLOG ที่เกิดจากระบบปฏิบัติการผ่าน SOFTNIX AGENT

เหตุผลทางด้านเทคนิค

ฟังก์ชันที่เรียบง่ายและสมบูรณ์ของเรา ประสิทธิภาพของระบบเรา จากการผ่านการใช้งานมาแล้วจากลูกค้าของเรา ดังนี้

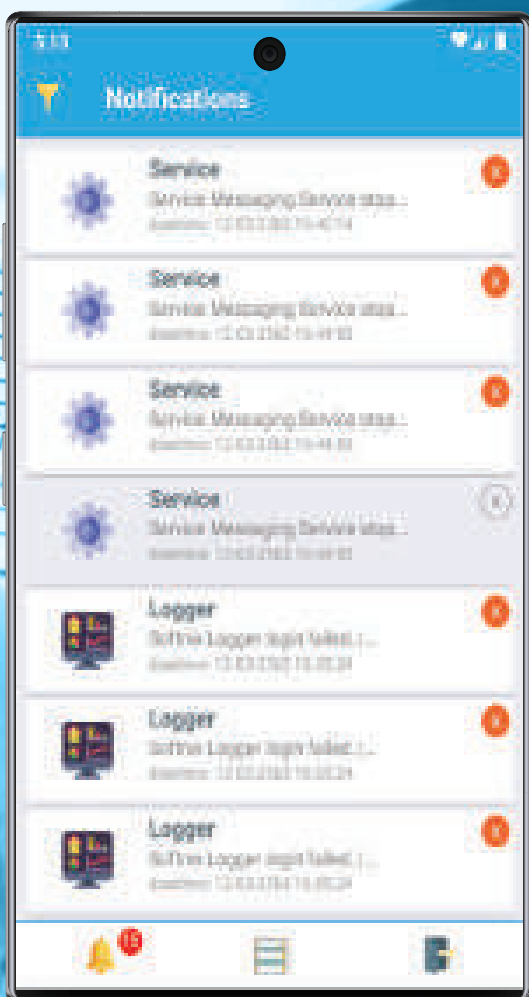
- กราฟฟิคสื่อ 180,000 MESSAGE ต่อวินาที ต่อเซิร์ฟเวอร์
- จัดเก็บและบริหารสื่อไฟล์ไม่น้อยกว่า 1.25 TB ต่อวัน
- ระบบบีบอัดข้อมูล 10 : 1 เท่า ขึ้นกับชนิดและรูปแบบข้อมูล

ใช้ได้แล้วแบบเต็มจอ

ทุกที่ ทุกเวลา

แจ้งเตือนทุกเหตุการณ์สำคัญ

หนึ่งในคุณสมบัติที่มาพร้อมกับระบบ คือ application Softnix Logger ซึ่งถือว่าเป็นฟีเจอร์ที่รองรับการทำงานผ่าน Mobile Devices โดยมี การแจ้งเตือนประสิทธิภาพการทำงานของระบบ แจ้งเตือนเหตุการณ์สำคัญ เช่น ไม่มีการส่ง Log File เข้ามาในระบบ แจ้งเตือนการใช้งานระบบและเหตุการณ์ต่างๆ เพื่อความสะดวกและเพิ่มประสิทธิภาพการตรวจสอบความถูกต้องให้ผู้ดูแลระบบไอทีที่มีเครื่องมือเพื่อช่วยในการแจ้งเตือนโดยจะมี notification แจ้งเตือนไปยังมือถือของคุณทันที ช่วยให้ผู้ดูแลระบบไอที สามารถระบุ แก้ไขปัญหา และตอบสนองต่อปัญหาใดๆ ในการดำเนินงานและปัญหาที่เกิดขึ้นแบบเรียลไทม์ได้อีกด้วย



(รองรับ ANDROID DEVICE เท่านั้น)

CONTACT US

หลายช่องทางติดต่อ สอบถามได้ทุกรายละเอียด



บริษัท ซอฟท์นิกซ์ เทคโนโลยี จำกัด
731 อาคารพีเอ็ม ทาวเวอร์ ชั้น 12
ถ.วิภาวดีรังสิต - ดินแดง แขวงดินแดง
เขตดินแดง ก.ก.ม. 10400



โทร 02 245 4942-43
แฟกซ์ 02 245 4944



www.softnix.co.th



sales@softnix.co.th