ISSUE 04 | SEPTEMBER 2019

BULWARK THE SHIELD

PROTECTING YOUR INFORMATION

GEARED FOR THE FUTURE

CYBER SECURITY FOR THE DIGITAL AGE

A SPECIAL SUPPLEMENT WITH

CXO INSIGHT Middle East

Complete Solution to Your Security Needs

SOPHOS
Unified Threat Management/ Endpoint Security

MAILSTORE
E-mail Archival

ESET
Endpoint Security/Antivirus

EnGenius
Networking Access Points/Switches /Routers

SecurEnvoy
Two Factor Authentication

iStorage
Secure Encrypted Flash Drives & Hard Discs

sendQuick
Appliance Based Gateways for Enterprise Mobility

EKRAN
User Behavior & Insider Threat Prevention

NetSupport
Classroom Management

42GEARS
Enterprise Mobile Management

BULWARK
PROTECTING YOUR INFORMATION

TRAPX SECURITY
Deception Technology

Accellion
Enterprise File Sync & Share

Aarcon
Predict | Protect | Prevent
Privileged Access Management Suite

lastline
Advanced Malware Protection

radware
Application Delivery /DDoS Protection

netwrix
User Behaviour Analysis & Risk Mitigation

CYBERBIT
PROTECTING A NEW DIMENSION
SOC Automation/SCADA Security

mimecast
Email Security / Archival

GO ANYWHERE
A HelpSystems Solution
Managed File Transfer

utimaco
Hardware Security Module

acunetix
Web Application Vulnerability Scanner

ENDPOINT PROTECTOR
Data Loss Prevention

BULWARK Technologies
www.bulwark.biz

For Further Details, please contact us:
710, IT Plaza, Dubai Sillicon Oasis,
Dubai - UAE | Phone : +971 4 326 2722
E-mail : info@bulwark.biz
www.bulwark.biz

BULWARK Distribution
www.bulwarkme.com

Issue 04 | September 2019

BULWARK THESHIELD

PROTECTING YOUR INFORMATION

05 **MD's message**
Bulwark Technologies MD Jose Thomas Menacherry discusses key trends and drivers of the regional cybersecurity market and how partners can cash in on new opportunities.

07 **Mimecast**
Jeff Ogden, General Manager – Middle East & India, Mimecast, on what you need to know about keeping your data safe in the cloud.

09 **MailStore**
A new level of security and simplified archiving of cloud services

11 **SendQuick**
Interview with Ashok Kumar, Chief of Business Development EMEA & SAARC, TalariaX

12 **CoSoSys**
Cristina Pop, Director of Sales and Business Development at CoSoSys, on how data loss prevention technology provides value to an organisation.

13 **ESET**
A primer from Dimitris Raekos, General Manager of ESET on the technologies and processes for data protection.

15 **Directors' note**
Jessy Jose, Director of Bulwark Technologies, reveals plans to unlock exponential value for channel partners through industry- leading solutions and comprehensive strategies for growth.

16 **News**
Bulwark completes 20 successful years in the region

17 **The Team**
The people behind the success of Bulwark Technologies

18 **What our partners have to say about us**
High praise from some of the key partners of Bulwark Technologies

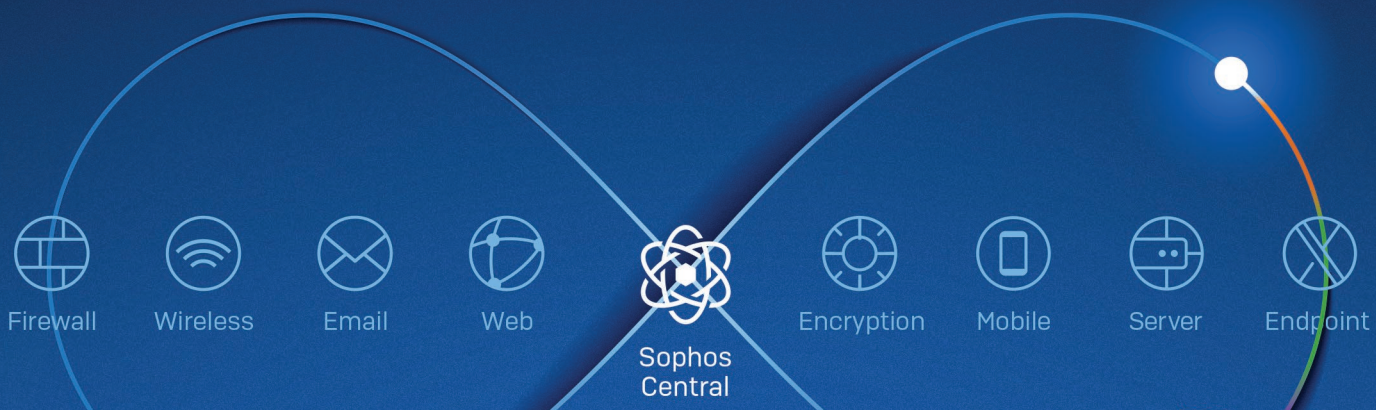
19 **What our customers say about us**
Bulwark Technologies lets their customers do the talking

20 **Blog**
Murali Vellat, Division Manager, Bulwark Technologies, talks about why security plays an important role in the success of digital transformation projects.

24 **Radware**
Nikhil Taneja, MD, India, SAARC & Middle East, Radware, writes about the need to create cyber awareness in the cyber arms race

25 **Utimaco**
Ibrahim Abu Wishah – Regional Sales Manager: South Europe, Middle East & Africa, Utimaco, gives us the low- down on HSMs.

Evolved cybersecurity is synchronized security.



XG Firewall

Intercept X

Synchronized Security is the world's first – and best – cybersecurity system

Next-gen endpoint, network, mobile, Wi-Fi, email, and encryption products, all sharing information in real time and responding automatically to incidents. And with everything controlled through the Sophos Central cloud-based security platform, management is a breeze.

BULWARK Distribution

SOPHOS
Cybersecurity evolved.

Securing your digital future

Jose Thomas Menacherry, Managing Director of Bulwark Technologies, discusses key trends and drivers of the regional cybersecurity market and how partners can cash in on new opportunities.

The regional threat landscape has evolved significantly in the last few years. Only those firms who are in complete sync with the cybersecurity changes/ requirements have successfully thrived in the region. Cybersecurity has become the topmost priority and is increasingly becoming an essential part of boardroom discussions within enterprises today. Security breaches and cyber-attacks are more rampant, as adversaries employ increasingly sophisticated technologies and methods to penetrate an organization's network. Cybersecurity being an ongoing and fast-changing requirement, the focal point of attention needs to be on the latest threats and breaches happening around us. Taking appropriate decisions and actions on time is a crucial aspect of enterprise defense strategies, which also warrant a firm and robust contingency plan to address these challenges. This has led to enterprises paying undivided attention to cybersecurity in order to tackle the latest threat landscape in the region.

Spanning two decades of consistent and successful operations in the region, Bulwark has successfully addressed the security landscape by introducing niche security technologies, resolving key customer requirements and pain areas and providing complete end-to-end-cyber security specialized solutions. Due to the nature and sophistication of threats emerging from time to time, organizations need to implement diverse cybersecurity solutions and take adequate measures to secure their IT environments. Today, proper implementation of these solutions by technology experts is a critical aspect of maintaining security posture. Bulwark, as cybersecurity specialized VAD, has an in-house team of engineers for products/ solutions in our current portfolio. This ensures total commitment towards our customers and channel partners in the region.

In terms of business growth, Bulwark has successfully attained some key milestones in the last 12 months. We have added and deployed in-country resources in some GCC countries, including a strong presence in KSA. We have enhanced our cybersecurity portfolio with the addition of encryption / key management solution. We have introduced and signed up with niche security vendors such as Utimaco, TrapX Security, Cososys and Radware and strengthened our portfolio of products, partner engagement and enablement. We have also strengthened our cloud based offerings and seen many customers opting for cloud model. We are currently celebrating 20 years of cybersecurity excellence and operations in the region, which is a significant feat in itself because, in this market, many players have mushroomed and disappeared.

> "The channel community can offer overall support and solutions, and also provide the necessary services to manage and maintain these requirements in a seamless method. There are always upsell opportunities with their existing clients who are constantly looking for solutions to address their cybersecurity concerns."

One of the key reasons for our sustained businesses success over these years is the fact that we help our channel partners to become trusted advisors to their customers. Over some time, customers might have implemented various security solutions to address the security threats that come up from time to time. Some of the key challenges in selling cybersecurity solutions by the channel community include understanding the business needs of customers, their existing security implementation, and pain areas to position the right products and solutions to satisfy their requirements. We have a team of cybersecurity experts to address channel partners' challenges and assist them through joint visits, conducting product demos, Proof of Concept (POC), implementation and after-sales support.

Despite these challenges, cybersecurity offers lucrative growth opportunities to partners who can provide differentiated solutions and deliver more value. Enterprises find it difficult to get the right technical resources in managing cybersecurity solutions within. The channel community can offer overall support and solutions, and also provide the necessary services to manage and maintain these requirements in a seamless method. There are always upsell opportunities with their existing clients who are constantly looking for solutions to address their cybersecurity concerns.

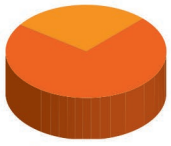
Going forward, we are not going to rest on past laurels and will continue to make efforts to cement our position as the number one security specialized VAD in the region. We have an in-house team of security experts who look for emerging technologies and products coming up in the IT security space and constantly invest in new and proven technologies to provide innovative cybersecurity solutions to customers in the region and gear up for the future.

mimecast®

BULWARK Technologies

Phishing & Impersonation Attacks are Getting Smarter

Ransomware & Email Downtime is Destroying Data, Productivity and Brand Reputations



77%

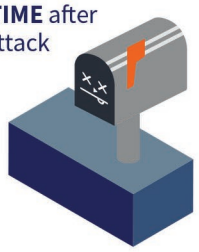
of impersonation attack victims dealt with a **DIRECT RESULTING LOSS** (data, financial or loss of customers)

87%

saw email-based spoofing of business partners or vendors looking to gain access to money, sensitive intellectual property or login credentials **(45% have seen this increase)**

3 days

average **DOWNTIME** after a ransomware attack



Protect your Employees from Human Error with Cyber Resilience for Email

Plan Your Email Security Risk Assessment Today

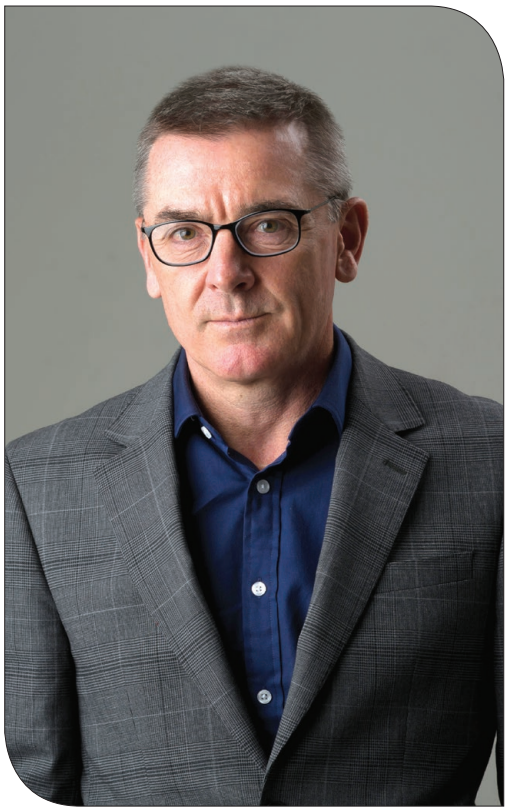
Visit mimecast.com or call 8000 3570 3897

mimecast®

Make Your Email Safer

Email & Web Security | Continuity | Archiving | Awareness Training

* Mimecast The State Of Email Security Report 2019 | www.mimecast.com/the-state-of-email-security-2019



Cloud productivity adoption highlights need for improved cyber resilience

Jeff Ogden, General Manager – Middle East & India, Mimecast, on what you need to know about keeping your data safe in the cloud.

Microsoft's announcement that it has become the first public cloud provider to open datacentres in the UAE is a cause for celebration among the Middle East's business sector. Greater access to cloud infrastructure will be critical to power artificial intelligence and edge computing innovation. The datacentres will offer local access to a range of productivity services, including Office 365 for email. Amazon and Google also have plans to establish local data centres over the next few years.

However, organisations' tendencies to rely exclusively on single cloud service providers for day-to-day operations have exposed them to undue risk. With services such as Office 365, organisations are not only putting all their eggs in one basket: they are putting all their eggs in the same basket that everyone else is putting all their eggs. Criminals know they have only one lock to pick to gain access, so they focus their attention on these cloud services because of the potentially large payoff.

As more businesses move email and data to Office 365, there's an increased need to protect against malicious or accidental loss of data. Mimecast's latest Email Security Risk Assessment (ESRA), an aggregated report measuring the efficacy of widely used email security systems globally, including Office 365, illustrated the scope of the problem. Of the more than 237 million emails inspected, organisations' existing email security systems missed more than 27,000 malware attachments, 55,000 impersonation attacks and 24,000 dangerous file types.

Microsoft offers certain protection-of-data capabilities as part of its Office 365 services, which are designed to protect against data loss caused by its own infrastructure failing. But these services don't always offer protection against accidental deletion, data corruption, advanced cyberattacks, or malicious users or administrators. These can often lead to downtime which can bring business operations to a standstill. Continuity is essential to any modern organisation's efforts to maintain productivity but is not always achievable when all business-critical applications run on a single cloud provider's infrastructure.

It's not only breaches, human error or technical error that can cause downtime for an organisation. Well-reported and widespread Office 365 highlight what can happen when email data becomes unavailable. Outages pose serious productivity risks to users who rely on software-as-a-service monocultures to support their operations. Even more concerning is the possibility that employees will turn to their unsecure personal Gmail or Yahoo Mail accounts when Office 365 goes offline. You then have absolutely no control over email activity.

Important data stored on Office 365 can also be lost due to accidental or malicious deletion or ransomware. If your organisation doesn't have an independent backup in place, and deleted data passes through short term folders such as the Recycle Bin, Deleted Items folders or retention policies without being recovered, it is lost forever.

To mitigate the risks associated with cloud services, organisations should look to improve their cyber resilience. An effective cyber resilience strategy should include layered security protection, independent data storage and alternative access routes to key systems like email, for when the worst does occur. The cyber resilience strategy should further include a backup and recovery plan just as this was a priority when systems were on premise.

Increased adoption of cloud services is a welcome development in the Middle East business sector and will support organisations as they strive for greater agility and scalability. But putting all your eggs in one basket – can leave you exposed to a broad range of new risks. Using a third-party provider and having an effective cyber resilience strategy provides a safety net and enables organisations to quickly return to standard operations without losing critical data or productivity.

V12

The Standard in Email Archiving

Easy. Reliable. Secure.

Email Security Made in Germany

2018 STEVIE GOLD WINNER GERMAN STEVIE AWARDS

MSExchange.org Gold Award

Software Bundesverband IT-Mittelstand Made in Germany 100% Service Quality Future

Advantages of Email Archiving

- Assistance with regulatory compliance
- Help with fulfilling GDPR obligations
- Protection against data loss
- Simplified backup and restore
- Reduced workload of email servers
- Elimination of mailbox quotas

Why MailStore?

- Integrated storage technology
- Flexible archiving
- Fast search access
- Low cost
- Low-maintenance
- Heavily field-tested

Over **60,000 organizations** in over 100 countries already trust in MailStore.
Trust in the **Experts in Email Archiving** for SMBs.

BULWARK Distribution

Bulwark Distribution
Phone: +971-4-326 2722 · Email: info@bulwark.biz
http://www.bulwarkme.com/mailstore

MAILSTORE™

MailStore V12:

A New Level of Security and Simplified Archiving of Cloud Services

MailStore Software GmbH has recently released Version 12 of its well-proven email archiving software MailStore Server. Users benefit from increased security through easier handling and, thanks to MailStore Gateway, from a simpler means of archiving journal emails of cloud services such as Microsoft Office 365. With MailStore V12, email management has become even safer and simpler to use.

"Our customers rely on their archived emails being safe and secure," says Bjoern Meyn, Product Manager at MailStore. "So it goes without saying that we want to continually improve the security aspects of our software and adapt to the increasing demands on email security. It's also important for us to preserve the ease-of-use and positive user experience that are the hallmarks of our software."

Automated Support of *Let's Encrypt*™ Certificates

One innovation in Version 12 of MailStore Server that is particularly worthy of note is the optional automated support of digital certificates of the independent certificate authority Let's Encrypt, which offers digital certificates for Transport Layer Security (TLS) encryption free of charge. With this service, MailStore is providing its customers with a simple means to automatically receive and renew official, trusted certificates so that they can build a safe and secure environment. Where required, MailStore Server can help administrators request and configure Let's Encrypt certificates immediately during installation. What is more, the software takes care of certificate renewal itself so that MailStore Server always has a valid certificate. Alternatively, administrators can use the Installer to create self-signed certificates or access existing certificates.

Simplified Archiving of Cloud Services with MailStore Gateway

MailStore Gateway for MailStore Server and MailStore SPE is a free add-on program to replace MailStore Proxy that will only be available with limited support from now on. In addition to SMTP and POP3 proxy functions, it provides a simple email server that allows emails from cloud services such as Microsoft Office 365 and Google G Suite, or from other email servers, to be archived. Previously necessary external journal mailboxes from third-party providers are now a thing of the past.

Security by Design also applies to MailStore Gateway

All emails stored in MailStore Gateway's mailboxes are protected by strong hybrid encryption. In principle MailStore Gateway also prohibits user names or passwords from being transferred via unencrypted connections. For this reason, servers to which connections are established via the proxy function must support implicit (SMTPS, POP3S) or explicit (SMTP+STARTTLS, POP3+STARTTLS) encryption.

MailStore Gateway's Management Console can be accessed by common browsers such as Microsoft Edge, Microsoft IE 10 (and higher versions), as well as by Google Chrome and Mozilla Firefox.

Continuous Development

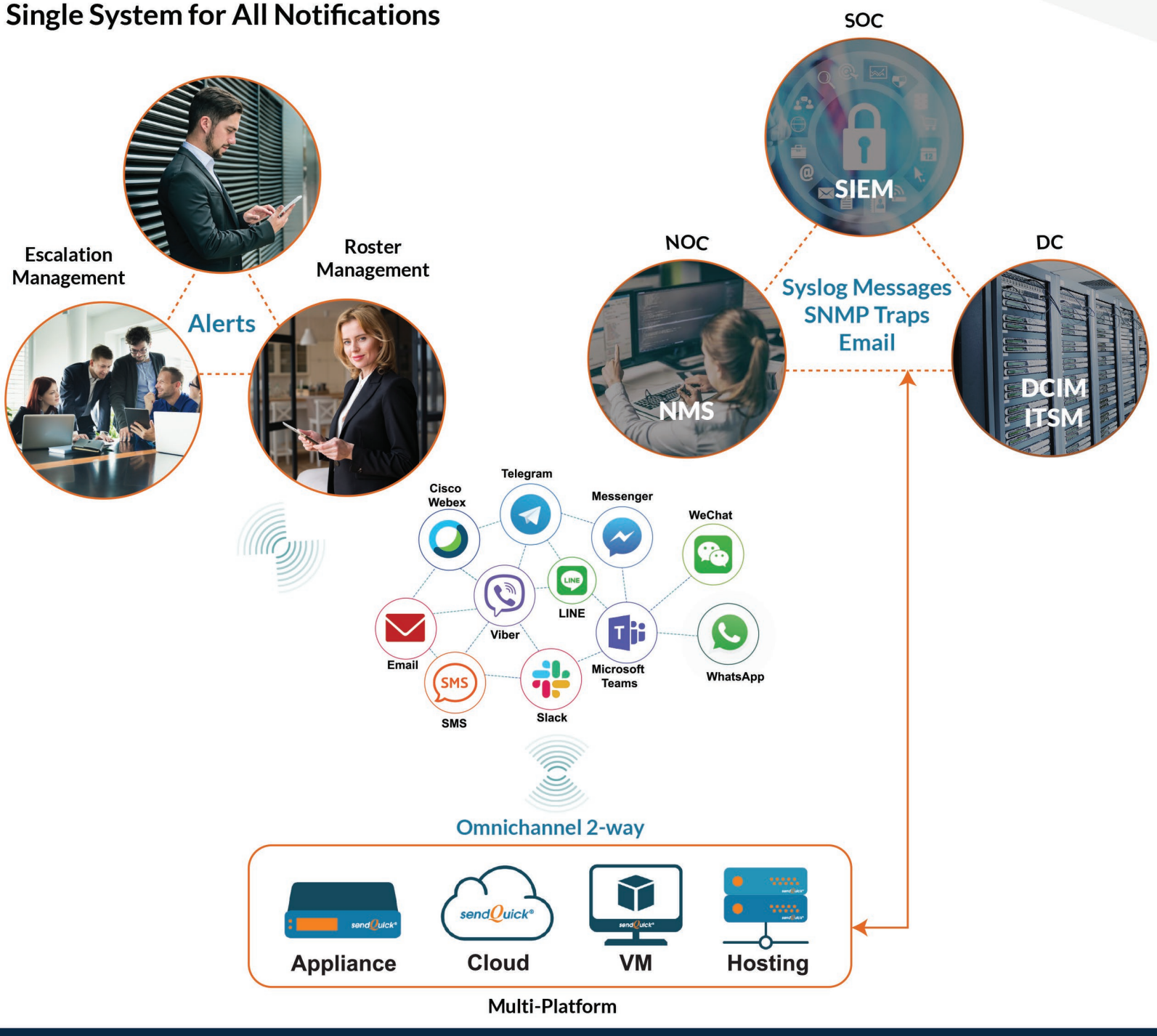
MailStore is continuously improving their software to meet both customer's needs and the ever-changing requirements of the IT market. Features of the new Version 12 like improved security and usability verify this statement, while the advanced development of Gateway proves MailStore to be the leading solution for email archiving – now and for future challenges.

TALARIA X
simplify mobility

sendQuick®

IT Notification Management Platform

Single System for All Notifications



Bulwark Technologies

Narendhran R (*Product Manager*) | +971 56 369 9775 | narendhran@bulwark.biz

Sign up now for additional 2-month warranty. Reference code:

THESHIELD19

Award-winning Messaging Platform for IT Security

Interview with **Ashok Kumar**, Chief of Business Development EMEA & SAARC, TalariaX

What is the product or service that you are offering specifically for IT security?

Our brand sendQuick comprises of self-sufficient, purpose built appliances that cater to Enterprise Mobility and Enhanced Remote Access Security. When it comes to ERAS, we support 2FA via SMS-OTP as well as free-to-download, smartphone based, soft-token generators. Our appliance sendQuick Conexa plugs into an organization's RADIUS based SSL-VPN to facilitate the authentication process. The solution is also available as a cloud based offering. We have other appliances such as sendQuick Alert Plus with HTTP Plugin and sendQuick Alert Plus that work with token generators from RSA, F5, Sophos etc., to deliver SMS. sendQuick appliances are highly interoperable and support a variety of platforms and devices not only within the IT security but the larger landscape of IP-addressable infrastructure as well.

How do you deliver SMS?

sendQuick devices can deliver 2-way SMS via GSM Modem (client has to purchase SIM card from local telco). sendQuick appliances can also integrate with local telco or cloud based third party SMS service providers for SMS delivery (push only) via direct connection through SMPP, HTTP POST, SOAP - that are industry standard protocols.

What happens if SMS delivery fails?

The client may opt to use 2xSIM cards from different telcos in order to ensure route redundancy . OTP may also be sent via email in the event SMS transmission is not possible. Apart from SMS and email, sendQuick also supports social media messengers like WhatsApp, WeChat, LINE, Slack, Telegram, Viber, Facebook Messenger etc., In other words, sendQuick supports omnichannel message delivery and multichannel route redundancy.

Can you explain about the interoperability of sendQuick and how it helps the cause of IT security?

The IT security framework at the SOC (Security Operations Center) comprises of Firewall, Anti-Virus, IDS, IPS, Probes, VA Tools, SIEM etc., sendQuick facilitates integration from each of these components and collectively from SIEM in order to ensure First Fail, Threat Detection, Event Tracking, Incident Response, Orchestration, Fraud and Compliance Monitoring. Popular SIEM Tools are Splunk ES, Solarwinds Log and Event Manager, LogRhythm SIEM, Alien Vault, QRadar, McAfee, Arcsight, Netwitness, Trustware etc.,. sendQuick Admin can set filters to receive incoming alert from devices, applications and users in a variety of ways to message concerned personnel via multiple channels. CISO/IT Security Manager/Security Experts can decide on the type of alert and where it must be sent for information, action, escalation and mitigation. Simply connect sendQuick to the switch and it will be able to receive input from every component detailed above while reverse monitoring IP-addressable assets for platform, application, and service availability.

Is sendQuick some sort of gateway for the Enterprise?

Not a mere gateway. sendQuick is an industry grade, enterprise class, omnichannel Alert Notification Management Platform that assimilates communications from a plethora of devices, applications and users within the organization. This includes messaging interoperability with platforms such as NMS, EMS, SIEM, DCIM, BMS, ITSM, vCenter, IOT, SCADA etc., sendQuick then facilitates 2-way information interchange with mobile stakeholders via various communication channels with fall-back route redundancy.

Who are your clients? Any last words on sendQuick ?

sendQuick appliances come from a singapore based ISO9001:2015 company, TalariaX. sendQuick products are certified CE/FCC/UL/RoHS. 85% of the worlds Fortune 500 companies are our clients among thousands of others across 50 discrete verticals such as Banking and NBFC, Insurance, Hospitality, Healthcare, Manufacturing, FMCG, Services, Govt, Oil & Gas, Defense, R&D, Shipping, Logistics etc., Prospects may contact our Distributor/Channel Partners in the event of interest.

Keeping your data safe

Cristina Pop, Director of Sales and Business Development at CoSoSys, on how data loss prevention technology provides value to an organisation.

Are endpoints one of the biggest attack vectors today?

Nowadays enterprises face a surge in the diversity and number of endpoints to be secured, as any device, such as a smartphone, tablet, or laptop, provides an entry point for threats. Due to practices such as BYOD (Bring Your Own Device) and remote or mobile employees, adopted by an increasing number of businesses, a centralized security solution proves to be no longer adequate for today's ever-shifting and undefinable security perimeter.

In the light of the rise of mobile threats, the need for efficient endpoint security measures has grown significantly. Endpoint security aims to adequately secure every endpoint connecting to a network in order to block access attempts and other risky activity at these points of entry.

Is DLP a mandatory tool in the security arsenal of enterprises?

Data has grown massively in terms of volume and its value has also increased substantially. Data breaches make new headlines every day and if sensitive information falls into the wrong hands it can have drastic consequences for organizations, including financial, reputational and legal ones.

Data Loss Prevention (DLP) products can help companies not only in safeguarding sensitive customer information like name, address or credit card number and intellectual property like trade secrets, trademarks or patents, but also in complying with different national, international and industry-related regulations such as the EU's GDPR, the CCPA and HIPAA in the US or PCI DSS, the global card industry security standard.

What is your main advantage in the DLP market?

Endpoint DLP often intimidates organizations because it is believed that its company-wide implementation is both time consuming and difficult. However, our product, Endpoint Protector is easy to deploy and it can be up and running in 30 minutes or even less. User friendliness is at the top of our priorities, thus the management of all endpoints can be done from a single dashboard and updates can be installed without requiring a restart. Endpoint Protector can be easily run by both technical and non-technical personnel.

Our DLP product also provides feature parity, which means that our customers can get the same features and level of protection for a computer running on Linux or macOS as they do on a Windows endpoint. Many of our customers that run multiple-OS networks are often relieved when they finally find Endpoint Protector, a solution that meets their exact needs.

What should users keep in mind while evaluating DLP tools?

Selecting the right DLP that best matches business needs is always a challenge. Some of the key factors when evaluating and determining what type of DLP tools should be deployed, are the size of the business and the industry. It is important to keep in mind that digital security issues threaten businesses of all sizes. Larger companies have more data at risk, but smaller businesses have less secure networks and usually they become quick and easy targets in the eyes of cybercriminals. Some industries, like healthcare or finance, are more heavily targeted, and they also have specific regulations to comply with. Furthermore, an organization needs to have a good understanding of the types of sensitive data it has, as well as how that data is used and regulated.

Is there a demand for cloud-based DLP? Or do enterprises still prefer on premise implementation?

Cloud-based DLP deployment is becoming more and more popular due to the fact that it provides an easy and rapid solution without additional costs like purchasing and maintaining a hardware.

We have also expanded our deployment options to include various cloud service providers such as Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP) to meet the needs of companies that have taken the plunge into cloud computing. However, organizations that opt for Endpoint Protector can choose between a multitude of deployment options, that includes virtual appliance and hardware appliance as well.

Solid protection for your data

Dimitris Raekos, General Manager of ESET Middle East, gives us a primer covering everything from basic technologies and processes for data protection.

What are the main steps companies need to take for Data Protection?

No business is too big or too small to be a target of attacks. We have long since passed the point where companies should be considering whether they might be breached; it is now a matter of when. By taking the time to prepare for that sort of emergency, businesses will better weather the storm.

Data Protection is the availability, confidentiality and integrity of information hence SMBs as well as larger organizations need to employ five essentials elements. Firstly, they have to understand the need of Data Protection. Obviously, they need to protect their intellectual property, and personal information of employees and customers. By doing that they avoid financial impact from regulatory authorities, bad reputation and of any loss of important information i.e. future strategic plans, secrets etc. The average cost of a data breach has risen 12% over the past five years to US$3.92 million, according to IBM's 2019 Cost of a Data Breach study, which drew on input from more than 500 companies around the world that suffered a breach over the past year.

By mapping data flows company realizes how data is entering and exiting the network, where digital assets are located and who has access to them. It is an interesting exercise and can be done by interviewing internal and external users. Process can be assisted by a data classification tool. Based on data mapping results a risk assessment should be carried to understand the threats, unaddressed vulnerabilities and possible impact. Upon finishing this process, we should prioritize the most severe weaknesses and vulnerabilities and develop a set of policies to address the risks.

Another essential element is People. They can define the success or failure of a data protection plan. Therefore, need to be trained and be aware of their role, responsibilities and consequences in case of a data breach. Monthly newsletters, boards, but also initiatives to motivate them are important. However, this shouldn't be limited on internal employees but also on 3rd parties that interact with our organization.

Finally, all these elements need be revisited, reviewed and have a response plan handy in case an incident occurs.

What is the role of technology?

Technology is one of the most important elements in developing a data protection strategy and enforce it. An easily managed and tested commercial solution for data encryption to protect data at rest or in motion, a Two-Factor Authentication solution to fortify user logins in the network but also in different applications can make a very good set of protection. Then we shall utilize a Data Loss Prevention to monitor user behavior and create the appropriate policies to address any employee misbehavior and enforce data protection policies. Endpoint Protection to protect for threats like ransomware, data wipers and hacking is really important however in the unlikely situation where systems are compromised a detection and response solution will minimize the impact. Network protection via firewalls or network traffic analysis for larger organizations can minimize the risks too. Last layer of protection but very important is the backup and recovery in case some other layer fails at least we can reassure the availability and integrity of our data.

How ESET is assisting on data protection?

At ESET apart from the technologies required to implement and enforce a data protection plan we are offering a useful e-book for IT Professionals working in small and medium sized companies, titled "Data Protection for Dummies" which is available for download via our website.

DOES LACK OF CONTROL, PRIVACY AND SECURITY OF YOUR DATA IN THE CLOUD CAUSE YOU ENDLESS WORRIES? WELL IT SHOULD.

REST EASY WITH

CLOUDASHUR®

The key to your data™

The iStorage cloudAshur Hardware Security Module is a PIN authenticated, hardware encrypted USB device that encrypts all data in transit and at rest with a FIPS certified randomly generated AES 256-bit encrypted encryption key which is stored within a dedicated iStorage secure microprocessor (CC 4+ Ready).

cloudAshur offers ultimate protection of your data, whether it's stored in the cloud, on your PC/MAC or transferred as an email attachment or file sharing software. cloudAshur eliminates data security vulnerabilities associated with cloud platforms, such as lack of control and unauthorised access to your confidential data.

ENCRYPT to ensure the ultimate protection of your data. **SHARE** your encrypted data securely with authorised users. **MANAGE** your cloudAshur devices centrally.

www.istorage-uk.com | info@istorage-uk.com | +44 (0) 20 8991 6260

iStorage®

BULWARK Distribution

Primed to spring your business forward

Jessy Jose, Director of Bulwark Technologies, reveals plans to unlock exponential value for channel partners through industry-leading solutions and comprehensive strategies for growth.

Bulwark, the cybersecurity specialized Value-Added Distributor, is continuously working on a robust and partner-centric strategy for the channel community to develop a win-win situation and flourish in the market. We understand and address the requirements of resellers and their pain areas and ensure that they are assisted at every stage of customer engagement. This approach results in enhanced customer satisfaction in addition to accelerating their business and revenue growth and opportunities.

To provide the right solutions to our customers, we are working with a wide array of system integrators and channel partners in the region. We focus on delivering value-added services and round-the-clock partner support, which include solutions pre-sales consulting, training, partner enablement programs, post-sales implementation and technical support, and adding value at every stage of product life cycle.

Partner development and growth in focused territories across the GCC and Middle East has been our constant endeavor. We execute comprehensive, action-oriented and established partner programs, which benefit our partners through deal registrations, better rebates, joint marketing activities, technical and sales enablement and promotes greater synergy among our vendors and partners and added value to end customers. Bulwark has made significant investments in certified professionals, demonstration equipment and value-added services infrastructure, which in turn, has significantly helped in the go-to-market approach to the channel community.

Moreover, our parent relationship management strategy is centered around key performance indicators reported regularly for partner and customer satisfaction. It is our continuous and ongoing effort to understand the partner challenges and assist them for their business growth.

Besides staying focused in specialized avenues in the cybersecurity domain, we encourage our partners on knowledge enhancement and continuous monitoring of current market scenarios to cater to the evolving customer requirements. Hence these strategies and vision support us in having a satisfied and thriving channel ecosystem.

In today's rapidly changing business landscape, it takes more than just a vision to succeed; building a sustained and robust brand requires a high-performing group of employees. I want to attribute our success to a team of product specialists who are constantly developing, directing and implementing various strategies across the region to promote their products and services through its channel ecosystem. Our product specialists are certified in both technical and business development, making them a jack of all trades. Our team is always on a constant learning curve, keeping themselves updated with the latest advancements in IT cybersecurity. They actively engage on social media platforms such as Twitter and LinkedIn and take up the occasional blog writing to keep customers updated with the latest trends on the solutions Bulwark has to offer.

We also have continuous in-house training programs for continuous and enhanced partner support. Bulwark has a team of specialized security sales and marketing experts who are continually developing, directing, and implementing various strategies across the region to promote their products and services through multiple channels. Our team of technical experts/ engineers attain various certification levels to provide round-the-clock technical support, product demos, Proof of Concept (POCs) for complete partner and customer satisfaction.

Taking this a step further, we provide education and training to our partner community so that they can design, implement and support the wide array of solutions in our portfolio. Bulwark is the authorized training provider for some of the key vendors we represent in the region.

As technologies are constantly evolving, it is our responsibility to ensure that our partners are trained adequately to support the changing dynamics of the industry.

"We execute comprehensive, action-oriented and established partner programs, which benefit our partners through deal registrations, better rebates, joint marketing activities, technical and sales enablement and promotes greater synergy among our vendors and partners and added value to end customers."

20 YEARS

Bulwark Celebrates 20 Successful Years in the Region

Bulwark, the regional cyber security-specialized value-added distributor has successfully entered twenty years of successful operations in the region.

Bulwark Technologies has established an excellent track record in the Middle East region, delivering world-class products with excellent customer service and value addition has been at the very core of Bulwark's operations since its inception in 1999, making the company grow multiple folds over the past years.

Recently, Bulwark has expanded its operations in the Indian sub-continent region. The expansion plans are in response to the company's growing business, robust partner network and strong demand for IT Security Solutions in India. Bulwark's India office will help the company to better serve the needs of a robust partner network and its growing customer base in India.

Bulwark, the cyber security specialized Value-Added Distributor showcases & provides an integrated range of innovative and specialized security solutions and services for the IT Security industry including PIM/PAM,Deception Technology,DDoS Protection, WAF, Cloud Email Security, HSM, Endpoint Security, Firewall,SOC Automation,SCADA Security and a wide array of cyber security solutions to customers across the region.

Bulwark has an established a network of over 500 enterprise resellers throughout UAE, Saudi Arabia, Qatar, Oman, Bahrain, Kuwait & other ME countries and India.

NEW VENDOR PARTNERSHIPS:

utimaco®

ENDPOINT PROTECTOR

TRAPX SECURITY

radware Every second counts

CYBERBIT PROTECTING A NEW DIMENSION

InterMapper Real-time Network Knowledge

Bulwark Announces Partnership with TrapX Security, The Global Leader in Deception Technology:

Bulwark Technologies, announced a new partnership with TrapX Security, the global leader in cyber deception technology. Now available to businesses across the Middle East & India. Bulwark's portfolio has been strengthened by the TrapX Deception Grid platform, taking the fight against cyber-attacks to the next level.

Protecting networks against a multitude of attacks including malicious insiders and sophisticated cybercriminals, DeceptionGrid, named the Best Deception Technology of 2018, lays decoys and lures attackers away from the network / cloud and into a contained environment.

"We're delighted to have cemented our partnership with TrapX Security," said Jose Thomas Menacherry, Managing Director at Bulwark Technologies. "TrapX, as the market leader in deception technology takes cyber security to the next level. Their intelligent approach to combatting advanced cyber-attacks leads way to the next generation of cyber defense strategies for businesses and we look forward to introducing this technology to our customers and delivering this solution to the Middle East & Indian markets." "It's our pleasure to announce that TrapX Security can now be delivered by Bulwark," said Ori Bach, GM & VP of Products at TrapX Security. "Known for their strength and longevity within the security industry, Bulwark brings to the table a wealth of technical expertise and a strong understanding of the challenges facing Middle Eastern & Indian businesses today. This coupled with our intuitive deception technology paves the way for a more secure future for our clients."

BULWARK AWARDS & ACCOLADES:

Reseller Hot 50 2018: Best Security Training Initiatives Award – Bulwark Technologies

Bulwark was awarded the 'Best Security Training Initiatives Award' at the prestigious Reseller Hot 50 Awards 2018 organized by CPI Media Group. The awards recognize and honors Bulwark for being an eminent player and making significant contributions in security specialized training to the channel community.

mimecast

Mimecast Partner Connect 2019 – Legend of the Year: Sincy Santosh

mimecast

Mimecast Partner Connect 2019 – Technical Legend of the Year: Deepu Thomas

CATALYSTS AWARDS 2019 RECOGNIZING EXCELLENCE

Marketing – Corporate Communications: Sonali Basu Roy

Bulwark-Your Valued Partner in Cyber Security

THE ENTITIES OF BULWARK:

- Bulwark Distribution
- Bulwark Technologies
- Bulwark Technologies India Pvt. Ltd

MEET OUR TEAM – COMMITTED TO YOUR VISION & SUCCESS:

- Sales & Business Development: Constant focus on business development & revenue generation.
- Pre-Sales Support: Offer consultancy through proof of concept (POC) & round-the-clock technical support.
- Technical Trainers: Focused on training to develop right technical skills, knowledge & know-how.
- Marketing: Continued focus on branding, visibility & demand generation through MARCOM activities undertaken through various channels.
- Renewals: Helps maintain existing customer relationships and renewals.
- Accounts & Logistics: Offering support for fulfillment & delivery of projects, with a time-specific & focused approach.

OUR EDGE:

- High end professional services in solution architecture, sales, marketing, implementation and support through team of certified security professionals.
- Very innovative and rewarding partner loyalty programs
- Training labs providing high end solution training and partner enablement
- Dedicated & active 500+ reseller network in the region
- Diverse Customer experience giving us an edge to understand different industry verticals & their requirements.

GEOGRAPHICAL REGIONS COVERED:

- Dedicated and active 500+ partner/reseller network in the region covering: -
- United Arab Emirates
- India
- Bahrain
- Kuwait
- Oman
- Qatar
- KSA
- Egypt
- Jordan
- Lebanon

For more information,please write to : info@bulwark.biz

What our partners have to say

Here's what some of them have to say about partnership with us.

"My interaction with Bulwark goes back more than a decade as a Security integrator and now Security Advisor; COMMENDABLE is the word, witnessing their anticipated progression around cybersecurity with futuristic vision, technologies and vendor portfolio. Today's enterprise could not ask for a partner better equipped than Bulwark which has the expertise to design and stitch customer requirements, best practices and security framework and making them seamlessly secured and industry certified."

Narendra Talreja | Country Leader: Middle East | SoftwareONE AG Trading LLC.

"Bulwark is professional & has a timely and quality focussed approach. It has been great pleasure working with the Bulwark team. They have been professional, conscientious, timely and strive to provide quality work. We consider bulwark to be a key strategic partner in our business's success and we intend continuing our relationship with them. We look forward to a long-term collaboration with Bulwark."

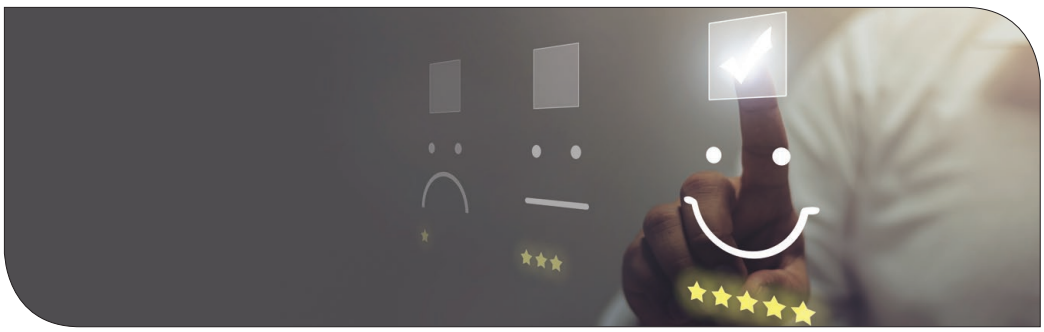
Robin Sinha | General Manager: UAE | Unicorp Technologies LLC.

"It was easy to work with Bulwark as they were always available for any kind of support. They were with us from the very beginning of our business. They helped us in closing successful POC's apart from getting the deals with their pre-sales expertise, advising us regularly in closing deals successfully."

J. Fiaz Uz Zama | Business Unit Head | Net Desire Technologies LLC.

What our customers say about us

Don't just take our word for it. Bulwark Technologies lets their customers do the talking.



"Bulwark has been an invaluable cyber security partner in project planning & implementation of the solution required for our organization. Working hand-in-hand with us, they delivered the project with a focused and value-driven approach."

Prashant Menon | Manager – IT Infrastructure & Support | Metito Overseas Limited

"Bulwark team is always very responsive and helpful when we reach out – all with a great attitude. First, they truly understand our challenges and vision before making any recommendation.

We decided to change from our existing Endpoint security due to the growing security threat observed in the year such as Ransomware, DDoS attacks and Personal Information Protection.

Bulwark was highly recommended, and we were impressed with the solution provided based on our requirement. We were able to swiftly migrate 6000+ user desktop and laptop endpoints with a stipulated time period with the support of Bulwark team. We are currently closely working with them on implementation of PAM solution.

The team possesses an excellent pool of talents who are well motivated to add value for the projects they deliver."

Suresh Nair | Associate Vice President | NMC Healthcare

Murali Vellat, Division Manager, Bulwark Technologies, talks about why security plays an important role in the success of digital transformation projects.

BRIDGING THE DIGITAL TRANSFORMATION SECURITY GAP

Digital transformation initiatives that don't consider core security functions can expose organizations to greater risks. In fact, according to Gartner, by 2020, 60 percent of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risks. With digital transformation becoming vital to the long-term survival of companies today, improving cybersecurity is no longer a choice but an imperative.

"Digital transformation is all about change, innovation, agility, and connectivity with the fundamental objective of providing always-

"With strong regulations in the industry such as GDPR, it is imperative to get the security strategy or transformation to match the digital transformation scope correctly. The punitive damages are enough to wipe out the gains made from digital transformation, not to mention the loss of reputation."

on available information in a seamless manner, regardless of where the resource is being requested from. It involves last mile digitalization, cloud computing, IoT, data analytics, robotic process automation, Artificial Intelligence, merging of OT and IT networks, etc. This, therefore, leads to a completely borderless way of transacting information with nothing binding or controllable. The very nature of digital transformation requires a completely new way of thinking for security. Organizations must look at security transformation to keep pace with the speed at which digital transformation is taking place. Security transformation involves building security into the fabric that involves people, processes, applications, and devices," says Murali Vellat, Division Manager at Bulwark Technologies.

He says that contrary to popular belief that security is a barrier, any digital transformation project not rooted in proper security governance and culture is a recipe for failure.

"Digital transformation projects and cybersecurity strategies need to walk hand-in-hand. Security is an enabler and not an impediment to digital transformation. It ensures to meet security's core triad – Confidentiality, Integrity, and Availability - without compromising user experience, performance, and agility. Security must not be treated as a cost centre or in archaic perspective, rather a critical part of the digital transformation strategy. With strong regulations in the industry such as GDPR, it is imperative to get the security strategy or transformation to match the digital transformation scope correctly. The punitive damages are enough to wipe out the gains made from digital transformation, not to mention the loss of reputation," he added.

With the arrival of new digital technologies, the need for rigorous security has never been more critical, and there are significant challenges organizations face when it comes to securing digital transformation projects. "It has expanded the attack surface with the advent of full-fledged cloud services platform that is more software driven and defined to IoT based devices that is increasing exponentially making it more difficult to secure and protect critical assets. With the explosive growth in technology and data, the barriers have blurred between the physical, virtual, and cloud platform that has made security now far more complex. It is becoming increasingly difficult to manage cybersecurity for such distributed and hybrid environments. Digital Identity is a key component and a challenge to cybersecurity, which involves authenticity of the information provided to the rightful user at the right time," says Vellat.

Another issue to contend with,is the general feeling amongst key executives that their digital transformation strategy would see impediments from the security team. This false notion leads the security teams being avoided in the planning stage to a later stage when it is too late to fit in the security part. This is a considerable risk to manage and should be avoided at all costs.

How do you get security right in digital transformation? There are some key best practices that organizations must follow to bolster their security postures while undergoing digital transformation. As a first step, says Vellat, security must be seen from a strategic top down approach and a safety-first principle, rather than an afterthought, that encompasses people, processes and systems, clearly identifying the risk class for the entire data lifecycle, data owners, business owners and accountability of information.

He explains: "Digital assets should be defined, classified and protected with the highest available standards of security. This should involve data governance in terms of the way it is being used and shared. There are several compliance standards specific to the industry that can be adopted to help define the path. Security awareness and training must be implemented for all employees as a continuous approach rather than one off. Companies should also consider building resilience into their cybersecurity practice to help rebound and recover from cyber-attacks. Assessments and gap analysis would help to address and mitigate such challenges."

With its deep expertise in cybersecurity, and partnerships with industry-leading players, Bulwark Technologies is at the forefront of the battle against cybercriminals. "Some the key digital security solutions we carry protect customers from breach exploits, strengthen public facing resources, cloud protection from threats flowing through web and email traffic, security awareness and training, controlling and managing privileged users, data security solutions, strong authentication systems, tools to help securely collaborate information with third parties, secure, hardened tamper proof devices to store critical assets such as keys, and information," adds Vellat.

Alliant Credit Union Enhances PCI DSS Compliance with GoAnywhere MFT Agents

As a member-owned **credit union** headquartered in Illinois, Alliant Credit Union processes and tracks over 500 file transfers a week. These file transfers must consistently meet the needs of their members and remain 100% PCI DSS compliant.

Growing Business Needs Sparked Search for a New Solution

Before GoAnywhere entered the picture, Alliant Credit Union used a mix of WS_FTP and MOVEit from Ipswitch and homemade manual scripts to process their file transfer needs. Based on the suggestion of a previous employee, Alliant Credit Union implemented GoAnywhere MFT for its robust capabilities and advanced set of features. Not only has GoAnywhere saved Alliant Credit Union hours of manual work since implementation, it's solved many in-house problems and improved the security of their data overall.

Computer Operations Supervisor Jay Wehner knew it was time to move to a new product when Alliant Credit Union started development on a new data warehouse. "With our current setup, we saw we needed a more robust system," Wehner explained. "We wanted better automation of the files and a process to import them."

Faced with increasing demands for PCI compliance, file transfer automation, and encryption, the team at Alliant Credit Union looked at GoAnywhere MFT as a possible replacement for their current setup. It had the features they wanted—database integration, clustered active-active failover, and secure email transfer—and the release of GoAnywhere MFT Agents only further expanded what they could accomplish.

GoAnywhere's Advanced Features Exceeded Expectations

Moving from their combination of file transfer solutions and manual scripts to GoAnywhere was painless. "No other product was evaluated. GoAnywhere is a true 'one product does it all.' It's not just file movement and SFTP."

After Wehner's team implemented GoAnywhere across the organization, they used it to create secure encrypted connections between their servers. This enabled them to promote the safety of their data and lock down common ports and protocols—which, for a company dealing with personal banking information, was absolutely critical. They also took advantage of GoAnywhere Secure Mail, an ad-hoc email module that can integrate with Microsoft Outlook. As they continued to explore the product beyond its basic capabilities, they found exciting features they've since integrated into their day-to-day tasks.

One such surprise was GoDrive, an Enterprise File Sync & Sharing module for GoAnywhere. Alliant Credit Union was also able to integrate GoAnywhere with their enterprise scheduler, a cross-platform, cross-application IT solution, to perform all their business procedures seamlessly.

Enhanced PCI DSS Compliance with GoAnywhere Agents

One main draw Alliant Credit Union had to GoAnywhere was the ability to enhance their PCI DSS compliance using GoAnywhere MFT Agents. "We needed a way to securely store and transmit PCI data. By utilizing GoAnywhere Agents, we were able to use a secure channel to transmit this data. We now no longer use standard protocols like SMB ... for file transfers, which protects our data from unwanted network scanning."

Other initiatives run by Wehner, like a workflow that archives and purges files across multiple projects after a set amount of days, help keep Alliant Credit Union organized and compliant with PCI DSS retention policies.

Saving Time and Money with GoAnywhere's File Transfer Capabilities

As an institution that deals with loan requests, automatic payments, and more, Alliant Credit Union processes a large amount of transfers a week. GoAnywhere cuts the transfer process down to around 15 minutes.

GoAnywhere also contributes to the company's bottom line. "I can't even begin to say how much time and money GoAnywhere has saved us each month. Automating your transfers, databases, and CSV files is an enormous cost saver."

When asked if he'd suggest GoAnywhere to others, Wehner didn't hesitate. "Buy it! The abilities are endless for file manipulation, transfer[s], database[s], encryption, and more!

www.arconnet.com

Some of the world's biggest enterprises trust ARCON to protect information assets

ARCON | **Privileged Access Management** is an enterprise class solution that provides seamless access, scalable architecture with real-time monitoring and analytics to **predict**, **protect**, and **prevent** insider & cyber threats.

Arcon
Predict | Protect | Prevent

BULWARK
Technologies

At the heart of fighting cyber threats

Nikhil Taneja, MD, India, SAARC & Middle East, Radware, writes about the need to create cyber awareness in the cyber arms race

Today we live in a cyber age amidst the cyber arms race between the good and the bad. While the bad ones are fighting for unethical gains and to cause disruption, the good ones are fighting to shield the good against the bad. Is there an end to this battle! Well, not really.

With each passing day, the cyber criminals are getting better and smarter in deceiving the best of the breed cyber security solutions and are innovating at a never seen pace. What was little known a decade ago, Ransomware is the buzzword today. We are well aware of the chaos caused by Wannacry and Notpetya in the recent past and it's just the beginning of what could be an Armageddon. With the advent of side channel attacks, file less malware and bots they have taken this battle to a new height.

While organizations fight this to protect their data, customers and intellectual assets, the nations on the other hand are fighting to protect its citizens and their interest. The latter is lot more difficult as the citizens of a nation are exposed to multitude of threats big and small by virtue of their connected lifestyle.

How do governments protect its citizens

Cybersecurity is not a destination, it's a journey. A journey that involves being aware of the cyber landscape, building a secure IT infrastructure, making necessary changes from time-to-time, investing in people and newer technologies and most importantly educating the citizens on the importance of cyber security and how they can contribute to the nations' safety by being aware and educated.

As cybersecurity evolves, so do the methods of attack. Hence cyber education should go beyond the software updates, regular antivirus scanning, and complicated passwords and include advanced social engineering issues through consistent and insightful trainings that make them aware of how serious leaked information can be for their company or nation.

With the North American headquarters in Mahwah, New Jersey, Radware is a leading provider of cyber security and application delivery solutions that constantly works towards helping organizations and nations in fighting this cyber arms race and keeping them ahead of the bad guys. Offering a broad spectrum of solutions including Application Delivery, Application Performance, Virtualization, Private/ Hybrid Cloud, Web Application Security, SSL Attack Protection, DDoS Protection and Attack Mitigation Solutions in addition to Cloud WAF Service, Cloud Web Acceleration Service, Cloud DDoS Protection Service and Cloud Malware Protection Service and Bot Management solutions, Radware defends and protects its customers from all known threats.

Radware's clear vision and strategy, leading attack mitigation technology and fast-growing subscription and cloud business coupled with continued innovation and comprehensive solutions are being used by more than 12,500 customers around the world across industries.

These customers include:

- 8 of the top 12 World's Stock Exchanges
- 11 of the top 20 World's Banks
- 10 of the 10 top Telecom companies
- 3 of the top 8 North American Software Companies

Radware's focus has always been on educating its customers and partners on the cyber threat landscape through various workshops, webinars, advisories, blog, social media and several other channels equipping them with the knowledge to take on the cyber challenges and come out victorious. In this regard, Radware has been working closely with several Governmental organizations of various countries in sharing the threat intelligence, exchange of critical information and consulting on cyber defense thereby assisting them in protecting nations' critical infrastructure and of course the citizens of the connected world.

Securing payment with the right Hardware Security Module

Ibrahim Abu Wishah – Regional Sales Manager: South Europe, Middle East & Africa, Utimaco, gives us the low-down on HSMs.

Hardware Security Modules (HSMs) are widely deployed by enterprises for the protection of the client's sensitive information and business transactions, especially in highly regulated and security sensitive markets like banking and financial services. But what does an HSM do?

An HSM is the security component that acts as the backbone of the cryptographic infrastructure of the organization and protects sensitive data from unauthorized access and malicious manipulation. It generates high-quality cryptographic keys, protects them against a wide range of logical and physical attacks, and utilizes these keys to perform cryptographic operations in a secure environment.

Many attacks on payment systems are able to exploit infrastructure vulnerabilities in their encryption key management. If the infrastructure is weak, the protection of payment transaction data can be undermined by an advanced attack using a fake or guessed key. To avoid this, sensitive card transactions can be protected by securing the encryption keys within the safe confinement of a Hardware Security Module.

The importance of HSMs in banking and payment is highlighted by the fact the Payment Card Industry Security Standards Council has mandated the inclusion of HSM as a part of its Data Security Standard (known as PCI-DSS) compliance. An HSM compliant with PCI-DSS standards provides unrivaled implementation of AES and other safeguards for payment transactions. For example, the HSM protects and manages encrypted keys required by key operations such as:

- PIN translations
- Card verification
- EFTPOS
- ATM
- Cash-card reloading
- EMV transactions processing
- Key generation and injection

PCI SSC mandates the following physical security requirements for HSMs:

a. Tamper Detection and Erasure

In the event of an attempt to tamper with the cryptographic keys, the HSM must implement security mechanisms (tamper switches, zeroization circuitries and firmware) which should readily/automatically erase and zeroize all clear-text secret information in a way that it is impossible to recover.

b. Multiple Security Mechanisms for One Threat

The HSM has to be designed in a way to prevent that the failure of a standalone security mechanism compromises the security of the whole HSM. There must be at least two security mechanisms for protection against a particular threat.

c. Physical Tamper Evidence

The HSM must include visible tamper detection controls, e.g. by placing especially designed tamper-resistant stickers that are impossible to remove on the HSM's opening screws and accessories, to prove any physical manipulation of the device. This protective measure is not only used to deter the attacker but also to prevent HSM users from intentionally or accidentally opening the device.

d. Impossible to Replicate / Fabricate

The HSM design must protect it against substitution and cloning attacks. Cloning of an HSM is understood as the successful extraction of the HSM key and backup partition from a compromised/stolen HSM with the aim of replicating it into a full-fledged separate HSM. There should be no practical way to duplicate or refabricate an HSM with accessories and components that are available commercially.

e. Separation of Cryptographic Boundary

HSM design strictly segregates between the normal HSM device boundaries and the cryptographic boundaries to ensure that there is no chance that the core crypto module holding the CSP (Critically Secure Parameters) is exposed during the maintenance or service of an HSM. Sensitive information must only be dealt within the protected areas of an HSM that are not prone to accidental or intentional modification or substitution.

f. Detailed Security Policy for HSM Management

HSM vendors must provide a detailed security policy describing the proper use of the HSM, its key management mechanisms, administrative functionalities, and environmental requirements. The security policy must include all roles supported by the HSM and detail the permissions of each designated role. All approved functions & operations performed by the HSM must be documented in the security policy, and the HSM should not include any hidden feature/functionality.

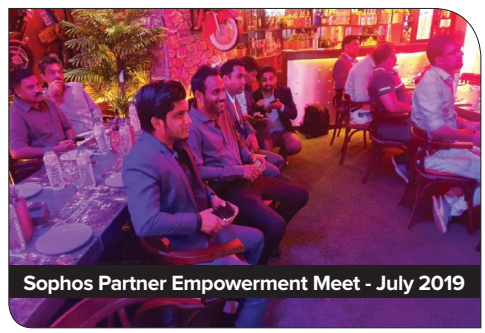
GITEX 2018 - October 2018

Sophos Partner Empowerment Meet - November 2018


Utimaco Technical Training - September 2019


Bulwark Christmas Meet - December 2018


Sophos XG Technical Training - February 2019


Sophos Partner Empowerment Meet - July 2019


GISEC 2019 - April 2019


Bulwark Corporate Iftar - May 2019


Sophos XG Technical Training - July 2019


Gear Up for 42Gears Partner Summit 2019 - May 2019

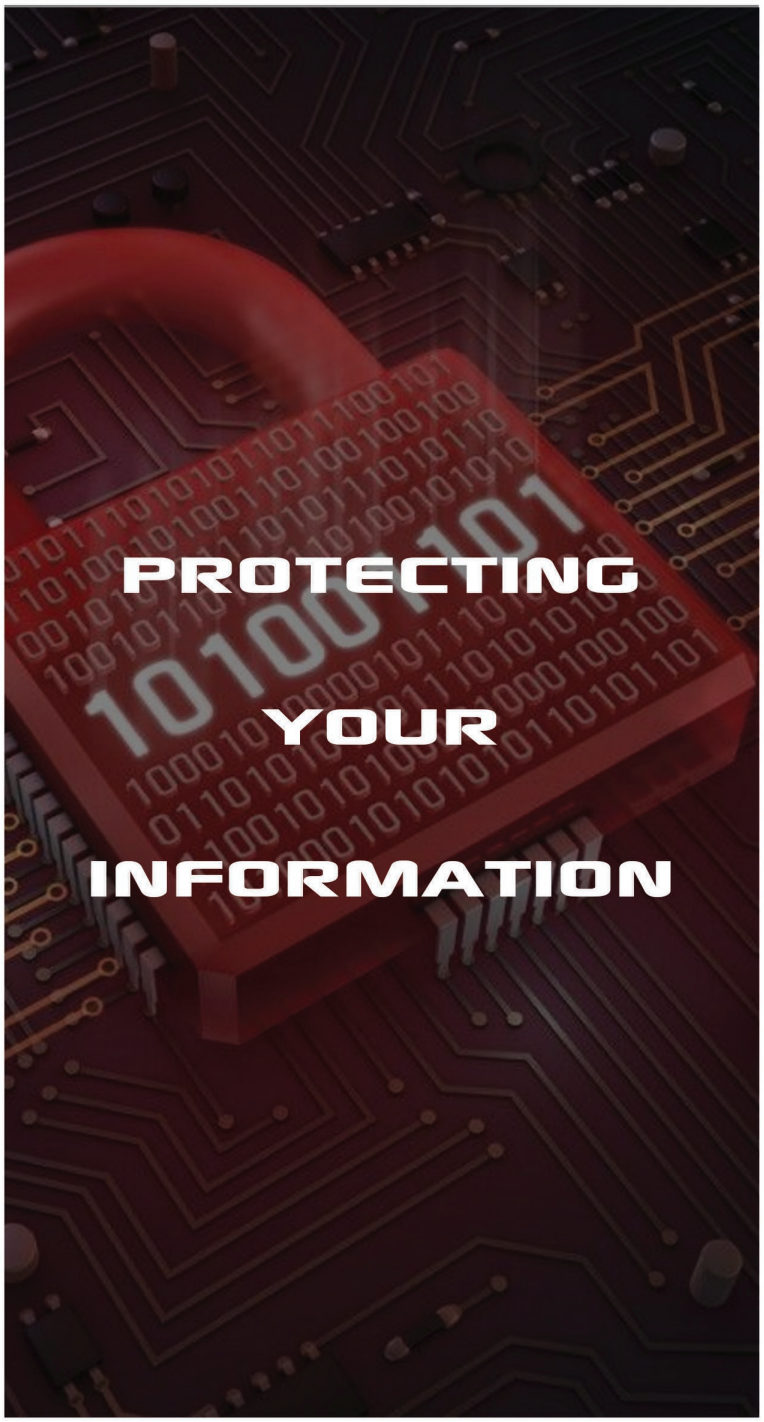

Sophos XG Technical Training - Oman - August 2019


HelpSystems Partner Enablement Meet - August 2019

BULWARK

39TH GITEX TECHNOLOGY WEEK | 06 - 10 OCT 2019
DUBAI WORLD TRADE CENTRE

Stand # SR-D20 | Sheikh Rashid Hall



SOPHOS Security made simple. | MAIL STORE | eset | iStorage®

42GEARS | EnGenius® | mimecast | Aarcon Predict | Protect | Prevent

NetSupport | lastline | radware | ENDPOINT PROTECTOR

TRAPX SECURITY | CYBERBIT PROTECTING A NEW DIMENSION | utimaco® | netwrix

GO ANYWHERE® A HelpSystems Solution | acunetix | Accellion

SecurEnvoy | sendQuick® | EKRAN.

BULWARK Technologies
www.bulwark.biz

For Further Details, Please contact us:
710, IT Plaza, Dubai Silicon Oasis,
Dubai - UAE | Phone: +971 4326 2722
E-mail: info@bulwark.biz

BULWARK Distribution
www.bulwarkme.com