www.businessconnectindia.in

RNI No. DELENG/2018/76695

BC MAGAZINE Business Connect

INSPIRING BUSINESS COMMUNITY

Vol-2 | Issue 6 | January 2020 | 299/-

WORK SMARTER NOT HARDER

TOP TRENDS FOR FOOD AND BEVERAGE INDUSTRY BUSINESSES

BEST WAYS TO STAY FIT WHEN YOU WORK IN AN OFFICE

Sudhakar Ramakrishna
Chief Executive Officer, Pulse Secure

Science Says Entrepreneurs Put Themselves at a Higher Risk for These Mental Health Problems

FOOD AND BEVERAGE PACKAGING TRENDS IN 2019

PULSE SECURE

DELIVERING SECURE ACCESS IN A ZERO TRUST WORLD

Follow us on

COVER STORY

PulseSecure

PULSE SECURE

DELIVERING SECURE ACCESS IN A ZERO TRUST WORLD

As workforce mobility and cloud computing continues to grow at a rapid pace, so too have cyberthreats, attacks and data breaches increased. This has resulted in the need to advance digital access protection. EnterPulse Secure.Under the leadership of their chief executive officer, Sudhakar Ramakrishna, Pulse Secure has transformed from being a remote access company to becoming the world market leader in Secure Access for hybrid IT.

Sudhakar Ramakrishna
Chief Executive Officer, Pulse Secure

ABOUT THE CEO

Brought up in Hyderabad, Sudhakar Ramakrishna studied Computer Science and Engineering. From there, he earnedhismaster's degree from Kansas State University in Computer Science and an MBA from Northwestern University.

About business, Sudhakar says, "I have had the good fortune of working with customers from the start in my career,whichhelped me to gaina deep empathy for 'customer success' and 'value-based solutions.' Over the years, he has held engineering, product and general management responsibilities in medium to very large companies serving customers across geographies, industries and segments."My customer-centered management focus evolved during my time at 3Com Corporation, and further while at Motorola, Polycom and Citrix."

His dedicated work in building networks, collaboration, mobile, and security and cloud solutions has provided him a unique vantage point of changing industry and customer trends. Sudhakar states, "I have had the good fortune to work with curious, collaborative and competitive teams that have put me on a path of learning, exploring – and enjoying – every single day. Ultimately, my role is to empower people to communicate better, work better together and be more productive."

How did I become part of the "Pulse Nation?" I have had a long-held belief that security should be about access and not just control. After all, security should not impede productivity. Being able to deliver security while preserving the simplicity of access offers unique value to customers - and a unique opportunity to innovate. Pulse offered me the opportunity to build a company from its core remote access heritage into a world-class provider of Secure Access solutions designed for the data center and cloud. Pulse also gave me the pleasure of serving, learning from, and growing with diverse and talented employees, as well as world class partners and customers."

DIGGING INTO THE DETAILS OF THE COMPANY

Chances are, if you have taken a flight, paid a bill, checked your bank account, logged in to get your email, streamed a movie or updated an online document – you've been protected by Pulse Secure. While only five years old, the secure access software company has amassed over 23,000 enterprise and service provider customers, has millions of devices under management, and engages business through its 700 employees and more than 2,500 partners in almost every part of the world.

Pulse Secure was established from the Siris Capital acquisition of the Junos Pulse- a business unit of Juniper Networks in 2014. From the start, their mission has been to enable secure access between people, devices, things and services that improve visibility, protection and productivity for their customers. Through the Junos Pulse acquisition, they obtained a solid foundation of products, patents, partners and customers. They've been busy ever since - acquiring mobile, authentication, application security technologies and advancing theirsecure access platform for hybrid IT.

While Pulse Secure is known for itspopular enterprise VPN solution (Pulse Connect Secure), they have realized even greater demand for their Suites that allows customers to take advantage ofthe company's integrated remote, mobile, web, network and application access security portfolio. They sell their solutions through channel partners and service providers to medium, large and global enterprises across industries, such as financial, healthcare, manufacturing, government, hi-tech, education and retail.

DIGITAL TRANSFORMATION RISKS

"We see digital transformation initiatives and new cyberthreats accelerating across multiple fronts. IT organizations are operating at breakneck speed to meet business needs which often introduces security exposures. This is further complicated by requirementsto support work style innovation – providing more employee work flexibility. These business risksare driving organizations re-think their secure access strategy," says Sudhakar.

Not only a trend in Asia, but throughout the world, businesses are empowering users to improveproductivity and work life balance by allowing employees to interact on their device of choice, when they want, and no matter where they are located. Organizations arealso pushing to move applications to the cloud, to benefit from utility computing, and to leverage the Internet of Things (IoT), if not the Internet of Everything. The diversity of users and devices, and the morphing of data center and cloud resources makes it more difficult for companies to ensure that necessary policies and defenses are active and effective. The most elemental policy is that of access security.

In the backdrop, cyber threat actors and attacks are increasing in velocity, sophistication and coordination. Globally, corporations are dealing with more than 40,000 incidents per day at an average cost of nearly $4M per breach. High profile data breaches at reputable companies like Equifax, Target, Sony and others have spurred significant privacy compliance mandates, which in turn have prompted executives to insist on more concerted governance. Lastly, IT organizationshave been working withtoo many security tools with fewer skilled personnel and budget to procure, deploy, manage and make good use of these tools. These trends have motivated organizations to assess their digital defense capabilities and have reinvigorated what is a $36B secure access market.

SECURE ACCESS ENABLES BUSINESS

Secure Access is a set of policies and technologies that ensure users, devices and things connect to applications, resources and services in an appropriate and protected manner. The objective is to enable productivity and business innovation while mitigating cyber threats and the risk of the data breach. Workforce and consumer mobility, cloud computing, big data and AI helpfuel digital transformation. “When you think about it, the use of these technologies has two things in common– connectivity and exposure. With connectivity comes potential exposure to threats, attacks and sensitive data leakage. In this way, Secure Access is crucial for digital transformation. Having a large and diverse customer base, we have the unique vantage point to see how our solutions are an enabler. The classic application would be that of ensuring remote users connect to network resources through a protected communication session – like checking your corporate email from home. But modern secure access solutions can handle a wide variety of business needs,” states Sudhakar.

How can you not only simplify and improve a user’s access experience, but also ensure the identity of the user, as well as assure that the device they use is sanctioned and secure – from PC to smartphone, from a personal device to shared kiosk?How do you ensure protected application access from users on the road, in stores, at a meeting, on a plane, at home, on vacation? Furthermore, how can you segregate personal from corporate apps and data across the vast assortment of personal devices? The applications and resources themselves no longer exist solely in corporate networks. While legacy, often complex applications will remain in the data center, many enterprises are moving to a private cloud or public cloud infrastructure. How can you enforce that secure connection for each application and regardless where it resides? Additionally, how do you gain Shadow IT oversight as divisions and teams procure cloud applications and equipment on their own.

Business not only relies on securinguser connectivity, but also on protecting transactions between things and services from ticketingmachinesand connected cars to medical dispensers and manufacturing equipment. This requires having visibility and control over endpoint and IoT devices across corporate networks, and by extension, private cloud. It also requires more automated means to identify and segregate devices to protect networks. As companies expand services and capacity through their partners and supply chain, and grow through mergers and acquisition, how canyou ensure data protection obligations are consistent an accounted for? Lastly, government entities contend with similar questions, albeit with greater requirements, like their commercial counterparts. These are the digital transformation challenges that Pulse Secure and its Secure Access solution address.

ZERO TRUST AND SECURE ACCESS

Many consumers have become desensitized to the fact that nearly 4,000 data breaches and leakage of billions of records were publicized in 2019. However, these security issues are part of the conversation at the board and executive level, especially given the potential financial and reputation impact on a business. This has renewed interest in a Zero Trust model even though it was created almost a decade ago. Its core principle is that of verifying everything before granting access.

The conventional security model trusted users and devices once they were on a corporatenetwork. Essentially, you, your laptop, phone, and IP camera are all presumed safe because they are within the enterprise perimeter. That perimeter security paradigm has come into serious question given numerous high-profile breaches. Now users work out of the office, browse the internet, infect their laptop, and that compromised device infects and further exposes the corporate network. It would also assume the resources and applications are all still on a corporate network. But we know that is no longer the case as most enterprisesoperatehybrid IT environments – data center and cloud. Therein lies the interest behind Zero Trust.

“The Zero Trust model requires authenticating users, devices, applications and infrastructure, and that conditions for access be assessed against a centralizedpolicy. That may seem obvious, but a lot of solutions do not do that. And if anything, they blindly provide access even if your device is at risk, or they try to verify something well after they provide you access,” adds Sudhakar. Access policies account for users, roles and applications, but with Zero Trust, they must also accommodate more granular conditions such as degrees of authentication, device and configuration compliance, location and access behavior. Not only should the conditional access be verified at the time of the request, but also during the session. This goes beyond just supplying a username and password before a secure session is established between the user’s device and the Microsoft Office 365 application hosted in a public cloud. Zero Trustraises the bar for access security and reduces an organization’s attack surface.

ZERO TRUST ACCESS CONSIDERTIONS

Zero Trust is not a panacea for cyberattacks and no product delivers Zero Trust. Organizations must orchestrate a variety of often disparate and complex access security technologies in order to strengthen their security posture and claim alignment with the Zero Trust model. Customers should look for access solutions that offer enhanced usability, deployment flexibility, automated provisioning and resource optimization, and solutions that work with their existing infrastructure.

“Simplifying this access control coordination, for both users and for network security administrators, is the top requirement for ourcustomers and paramount for enterprises that are large, multi-national and often heavily regulated. Today, over half of oursales are for ourZero Trust-based Access Suite. Beyond the sheer value and economics of consolidating tools into an integrated suite, their approach provides easy, compliant access for end users and single-pane-of-glass management for administrators. Organizations can centrally manage and enforce access to applications, data and services that are delivered on premise, in private cloud and public cloud,” states Sudhakar.

The company’sAccess Suite uniquely integrates VPN, Mobile Device Management (MDM), Single Sign-on (SS0), endpoint and IOT device visibility, Software Defined Perimeter (SDP), Network Access Control (NAC) and virtual Application Delivery Controller (ADC) capabilities.

PULSE SECURE EMPLOYEES QUALITIES

Sudhakar states, “At Pulse, great competence, exemplary commitment, and fantastic attitude are quintessential attributes for an employee. I am proud to say that our employees display these qualities abundantly and we have been distinguished as one of the best places to work on a routine basis.”Beyond hiring talented and smart people, the companyseeks diverse and active contributors who exhibit respect, integrity and humility. Additionally, theybelieve that behavior drives outcomes. To that end, they focus tremendously on reinforcing key behaviors of implicit trust, challenging and supporting, debating and aligning, and cross-functional collaboration.

LOOKING FORWARD

Sudhakar Ramakrishna, on the horizon with regard security concerns for 2020, says,”I anticipate a perfect storm in 2020 – an increase phishing and malware incidents, an increase in targeted cyberattacks and breaches, and an increase in global data privacy regulation and actual fines. We are experiencing new attack vectors and sophisticated malware. For example, recent OAuth application exposures show just how well hackers are going after all possible attack vectors, especially ones that imitate known, popular applications to trick users into accepting malware or providing credentials. In 2019, we saw thousands of publicized data breaches – I suspect that many more were not. The State of Louisiana in the U.S. has experienced service outages due to cyberattacks.As such, I expect we will also see similar targeted attacks exploiting IoT and IIoT vulnerabilities in industry’s that rely on these devices and that are merging IT/OT environments. Lastly, similar privacy compliance specifications to GDPR will be adopted more broadly in the U.S. and other countries and we will see a rise in awarded penalties. These trends certainly call for more vigilent assessment of security and secure access capabilities.”

In 2020, Pulse Secure’s priority is to extend its market leadership position by giving customers more value and capabilities across their Secure Access portfolio, as well as expand ways for their solutions to be consume theircustomers. The company will further enable its customers to support a broader set of use cases through enhanced interoperability with the popular network, security and cloud infrastructure, including new integrations to support Industrial Internet of Things (IIoT). In addition, Pulse Secure plans to introduce “Secure Access as a Service” for their customers and partners.