InvestBank bolsters security with F5

Sharjah-based bank invests F5 BIG-IP iSeries Application Delivery Controller

⬆ The new technology will be critical to shaping and safeguarding InvestBank's next phase of development, says Mukeri.

One of the leading commercial banks in the UAE, InvestBank has tapped F5 Networks to bolster its cyber security posture.

With this deployment, F5 Networks solutions will allow the Sharjah-based bank to pre-empt complex consumer demands and support compliance with global best practices, including the payment card industry data security standard (PCI DSS).
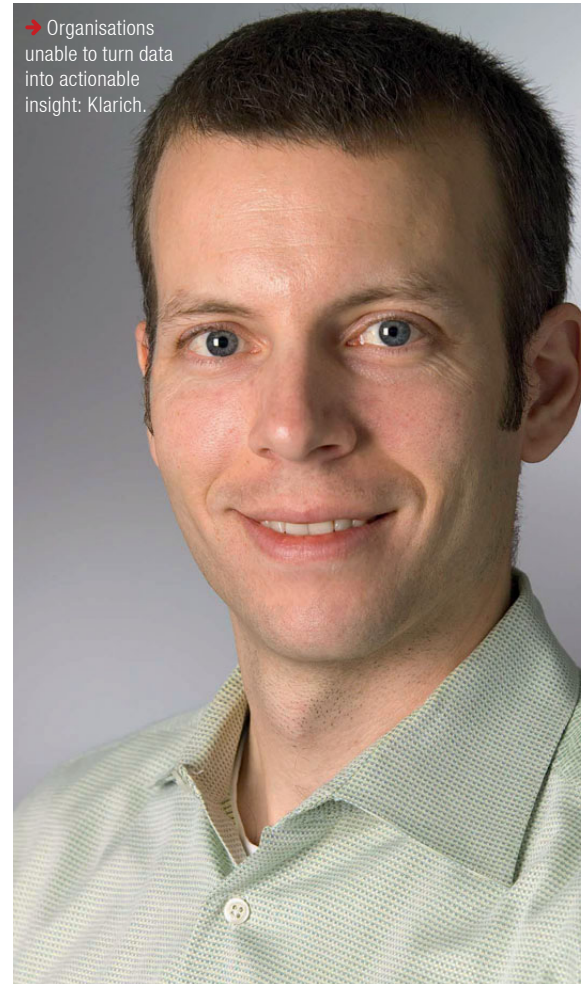
"InvestBank is committed to continually improving its ability to scale and innovate, as well as offering our customers the most user-friendly, secure services possible. The new technology we've introduced will be critical to shaping and safeguarding our next phase of development," said Kausar Mukeri, CISO and head of information security, InvestBank.

InvestBank is using the cloud-ready F5 BIG-IP iSeries Application Delivery Controller (ADC) platform, designed to deliver easier programmability, ecosystem-friendly orchestration, and better software-defined hardware performance. It also helps accelerate private clouds and secure critical data at scale.

The project also encompasses the F5 Silverline cloud-based services delivery platform to protect against application attacks.

THE NUMBER OF NEW MALWARE VARIANTS IN DECEMBER REMAINED ROUGHLY THE SAME AS NOVEMBER: SYMANTEC MONTHLY THREAT REPORT, DEC 2017

Source: Symantec

➜ Organisations unable to turn data into actionable insight: Klarich.
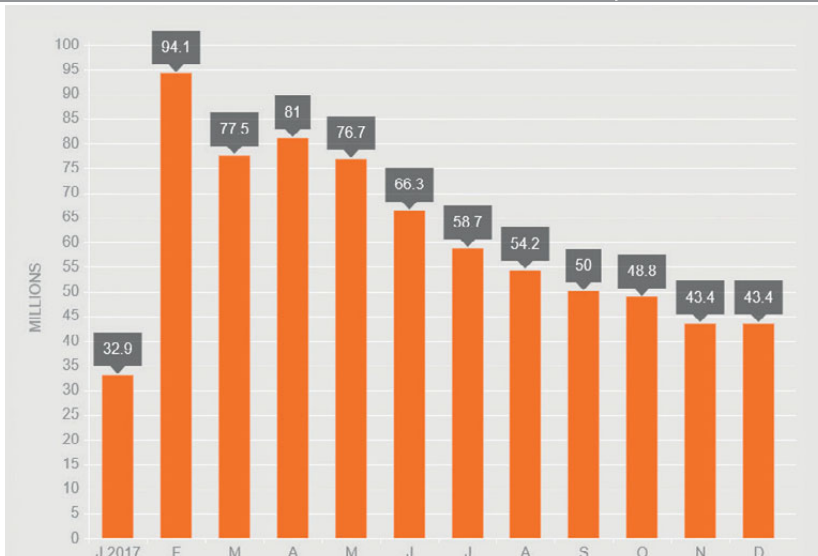
Palo Alto seeks to ease GDPR blues

Cloud-based logging service ensures data stays local

Palo Alto customers can now collect their own security data from the Palo Alto Networks Next-Generation Security Platform, after the cyber security vendor launched a cloud-based logging service in Europe.

The service will make large scale log collection affordable while addressing data privacy and location needs for many European organisations, and those with access to EU citizens' data. All data sent to the Logging Service in Europe will be stored within a data centre located in the EU, as GDPR looms.

According to Lee Klarich, chief product officer at Palo Alto Networks, organisations are often challenged by an inability to collect large volumes of data and turn it into actionable insights to optimise their security posture. "The Logging Service allows our customers to do this and to meet changing business needs, simplify operations and increase automation. Having our Logging Service in Europe ensures that our customers can benefit from these data collection capabilities while ensuring that their data remains within Europe to meet their privacy needs."

Cybersecurity products generate massive amounts of valuable data in the form of logs that can be used to counter sophisticated threats. Today's organisations require the ability to store, process and analyse as much log data as possible. However, traditional hardware-based log collection comes with administrative overhead and scale limitations.

45%

Of data centre operators saw their internet bandwidth saturated due to DDoS attacks

13th annual Arbor WISR report

"Despite a steady stream of cybercrimes in the media, too many people feel invincible and skip taking even basic precautions."

Tamim Taufiq, Head of Norton Middle East
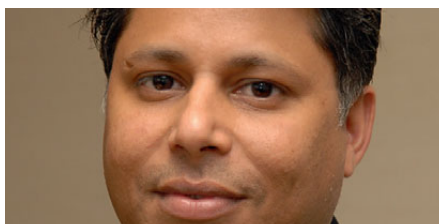
"The (cyber) attacks and their orchestrators are evolving faster than the security technologies that can combat them."

Sachin Bhardwaj, director, eHosting DataFort

Veritas 2018 Predictions: how data management will rock IT in 2018

IT will be forced to take responsibility for cloud data management and cut costs: IT will find out they are responsible for management in the cloud – possibly through a breach – and the CFO will demand cuts infrastructure costs.

Data will grow exponentially, but data storage will slow for the first time: In 2018, we'll see successful companies shift their storage strategies from a "save-it-all" mentality to one that identifies and stores data that provides valuable insights or mission critical information.

One of the first companies to be fined under the GDPR will be outside of Europe: Despite the impending deadline, only a third of companies surveyed by Veritas worldwide believe they are GDPR compliant.

Data management will get a major IQ boost from analytics. We'll begin to see advancements in analytics that move the traditional archiving, backup and storage conversation far beyond "add more capacity."

The severity of data breaches will increase. According to the Identity Theft Resource Centre, 2016 saw 1,093 data breaches last year, a 40% increase from 2015; 2017 almost hit that mark by July.

Source: Johnny Karam, VP, emerging markets, Veritas