ASK Technologies, Inc.

FALL 2018

Volume 18 Issue 1

ASK NEWS

In this edition of ***ASK News***, we are proud to share two important accomplishments. First, ASK is 25 years old this month, and second, ASK is once again the receipt of the Philadelphia Business Journal's Top 25 Technical firms in the Philadelphia and Metro Area. Also in this edition, we discuss two of our key partners, Datto and Tegile and some of features and benefits of their show stopping product lines. Enjoy the read.

Stephen Pirolli, ASK Technologies, Inc.

Inside this issue:

WELCOME NEW CLIENTS

BACHARACH

R&S CONCRETE, PAVING & SITEWORK

MOD WORLD WIDE
THE MODERN AGENCY

Feasterville
Family Dentistry

Microsemi
a Microchip company

ASK Technologies Partners with Tegile

From our Sales Team

ASK Technologies is proud to announce its newly established partnership with Tegile, a Western Digital brand having a comprehensive storage product portfolio ranging from hybrid storage to all-flash solutions. Tegile Intelligent Flash Arrays are powered by IntelliFlash™ operating system. This intelligent software architecture includes several patented technologies designed to deliver consistently high performance and low latency while maximizing uptime, streamlining data protection, and curbing storage costs.

Flexible Architecture

IntelliFlash gives you the flexibility to use all flash, a mixture of flash and disk, or a mixture of high-performance flash and high-density flash — all within a single storage system. The software architecture intelligently manages different storage media to deliver optimal performance and capacity.

Intelligent Caching

Intelligent caching algorithms place the most frequently accessed application data on DRAM and flash.

continued on pg. 2

ASK Celebrates 25th Anniversary

This month marks a major milestone year for ASK Technologies, Inc. – it's our 25th anniversary! To put that into perspective, Microsoft had just released Windows NT when ASK was founded.

As we reflect on how far our company has come, we must give a huge thank you to our incredible clients – your loyalty and trust in us throughout the years allows us to push our boundaries and challenges us to strive for excellence in all that we do. Our clients are more than just clients, they are family. The relationships our company has built – and will continue to build – with each of our clients will always be our number one motivator for success.

Being in business for 25 years would not have been possible without the amazing people within our organization. We are incredibly thankful for the hard work and dedication from our employees, and are so appreciative to be able to work with each of them every day. This milestone would not be possible without them.

We are proud of the progress we have made and are thrilled to see what the next 25 years holds for our company.

ASK Receives "Top Tech Employers" Award

ASK TECHNOLOGIES, INC. is once again a proud recipient of the Philadelphia Business Journal prestigious award for "Top Tech Employers". This marks the fifteenth consecutive year that ***ASK TECHNOLOGIES, INC.*** has been recognized as an industry leader in the Philadelphia and Metropolitan Area.

ASK provides our clients the ability to transform current information technology into productivity. Whether utilizing technology to bridge the gap between employees, business workflow and computers, or using technology to supply access to data, regardless of connection, location and time, ***ASK*** offers the solutions you need to survive in a very competitive world.

* * *

ASK Technologies Partners with Tegile

continued from pg. 2

These caching algorithms are optimized for various I/O patterns and seamlessly adapt to differing media latencies across multiple levels of cache.

Inline Compression & Deduplication

Data is compressed and redundant blocks are removed before they are written to disk.

These techniques not only reduce the storage footprint, they also help to improve performance by freeing up cache space in DRAM and flash for faster reads and writes.

Unified Storage

Tegile arrays natively support both block (SAN) and file-sharing (NAS) protocols, enabling you to run applications and manage files on a single array. Supported protocols include iSCSI, Fibre Channel, NFS, CIFS and SMB 3.0*.

Point-in-Time Snapshots & Replication

Take an instantaneous snapshot of your data. Snapshots are VM-aware and application consistent. They are also space-efficient and incur no performance overhead. Replicate snapshots for DR, and restore data instantaneously from the local or remote array.

Encryption

Data security is provided using 256-bit AES encryption of data at rest. IntelliFlash delivers inline encryption of data on SSDs and HDDs with unnoticeable impact on performance.

Key management required for encryption is performed natively in the system without needing any user intervention.

Non-Disruptive Operations

All hardware components, including SSDs and HDDs, can be replaced online with zero downtime. Software upgrades to the array can also be performed with no downtime or loss of access to data.

Why Tegile

Clients such as VMware, Tesla, Ferrari, Chipotle, CVS, and thousands of others trust Tegile Storage because Tegile flash storage solutions offer greater flexibility, multi-protocol support, and affordable disaster recovery.

We invite you to find the best fit for your business by taking this one-minute storage survey from Tegile, and you will be eligible to receive a $25 Amazon gift card, just for completing it.

For more information about Tegile's Intelligent Flash Arrays, please contact your local ***ASK Sales Rep*** at (610) 617-300.

tegile
a Western Digital brand

"We invite you to find the best fit for your business by taking this - minute storage survey from Tegile, and you will be eligible to receive a $25 Amazon gift card, just for completing it."

SIRIS: What Does Business Continuity Mean for Your Business?

From our Sales Team

Imagine you are a medical practice that can't book appointments because your server is down. How long could this business be down before it starts to "hurt" patients? Imagine you are a law firm that needs specific case files, but whose files were recently "locked up" by the Cryptolocker virus. Imagine you are a retail business that needs to process hundreds of transactions a day, but your point of sale system was damaged in an electrical storm, and you can't process and record transactions. How will you stay in business? What will you do?

Now imagine getting it all back in a matter of seconds. Your business is running, and you're back to making business decisions.

It's no longer a matter of "if," but "when" a real world threat will compromise your business data. Between natural disasters, viruses, user error, and ransomware like "cryptolocker," these threats are becoming ever-present.

• *Business continuity made for your business*
No matter how complex your IT environment may be, business continuity should be simple, fast, and fail-safe. It should work when you need it to – in an instant's notice – locally in your office or from an off-site location. It should prove itself day in and day out on your schedule.

Datto SIRIS is a robust business continuity solution that brings together state of the art hardware with a secure cloud storage capability.

The result is a comprehensive backup, recovery, and business continuity solution that gets your business up and running instantly in the event you can't access your data or systems.

• *With a SIRIS you get Total Data Protection*
SIRIS combines the most important elements of data protection into a single fully integrated package: backup capture and verification, backup restore, and a complete virtual host for business continuity.

• *Leverage award winning core technologies*
Easily protect your IT infrastructure without the need for multiple tools. Backup your data, including your operating systems and applications from Windows or Linux, and files and folders from your Mac automatically to a local device with copies in our secure cloud storage environment.

• *Recover critical data quickly*
Should you experience a server failure, the SIRIS can have your Windows or Linux environment and data recreated in minutes from the local device or the Datto Cloud, and have your Mac files and folders recovered just as quickly.

• *Proof that your backup was successful*
Visual proof in the form of a screenshot and service verification gives you peace of mind that your data has been successfully backed up.

• *Compare backup points*
Now you never need to guess when data was deleted, added, or modified. You can know what changed and when – in a matter of minutes. What do you get with Datto?

• *Data Protection on Premises and in the Datto Cloud*
Every image-based snapshot of your system is stored both locally and in secure, purpose-built data centers using Datto technology. This means no third-party cloud providers are involved in the safety of your data.

• *Built for Quality*
All Datto business continuity products are designed and assembled in Datto's build facilities in Monroe, CT by a highly trained

Continued on pg. 4

PROTECT ANYTHING
Mac, Windows, Linux, and Virtual

RESTORE ANYTIME
Diskless Restore, Hybrid Virtualization, Cloud Virtualization & Local Virtualization

INFINITE CLOUD PROTECTION
Daily after 7 Days
Weekly after 2 Weeks
Monthly after 6 Weeks
Delete Never

RUN ANYWHERE
Physical, Imaged, Virtual on Multi Devices

Proofpoint: Advanced Email Security

from our Tech Staff

More than 90% of advanced threats come through email. Organizations like yours are struggling to address the speed, volume, and complexity of today's fast-evolving cyber threats, which hurt your brand-and your bottom line.

Today's attacks are no longer just about malware. Many of today's biggest threats-including credential phishing and email fraud-don't involve malware at all. As a result, organizations with defenses focused only on detecting and blocking malware have had to rethink their email security strategy. Today's security teams must manage the whole spectrum of email threats. And that includes hard-to-detect, targeted email fraud.

Only Proofpoint Advanced Email Security solves the entire email threat problem. Our unified solution helps you prevent, defend, and more easily respond to today's most advanced attacks.

While other email tools may help with some aspects of email security or stop some attacks, our multilayered approach covers every threat that matters-most of them before they reach the inbox.

Advanced Email Security is built on a complete, extensible platform. It offers clear visibility into all of your email and any threats they contain. With this insight, you can understand the threats you face and respond more quickly and effectively.

We stop threats that seek to compromise your users through social engineering, not just technical exploits.

Here's how each element of the Advanced Email Security platform works together for complete protection, response, and continuity.

Email Analysis and Classification-Email Protection

Proofpoint Email Protection stops email threats and other unwanted messages in every major language. Using multilingual analysis powered by machine learning, our email classifiers divide incoming email into separate quarantines by type. This feature gives you granular control over a wide range of email. This includes spam, phishing, impostor email, malware, bulk and adult content.

Email Protection also detects threats that don't involve malware, such as credential phishing and email fraud. Email Protection assesses the reputation of the sender by

continued on pg. 5

proofpoint.

"Today's attacks are no longer just about malware. Many of today's biggest threats-including credential phishing and email fraud-don't involve malware at all."

SIRIS What Does Business Continuity Mean for Your Business?

continued from pg. 3

team using the best components on the market. Each device is assembled to our exacting standards with extreme attention to detail.

• *An Award-Winning Industry Leader*
Award-winning technology and innovative new solutions from a team that prides itself on building a better business continuity solution day in and day out. Datto has been recognized for its ingenuity by The Atlantic, Forbes, Fast Company, Bloomberg Business, and The New York Times.

For more information about Datto and their product offerings, please contact your local ***ASK Sales Rep*** at (610) 617-0300.

datto
PARTNER PLUS

Premier
PARTNER

Client Quote

"Congratulations on A. S. K. Technologies' 25th anniversary!

It is not surprising that a company with such a well-deserved reputation for excellence and client-oriented service should reach this milestone.

Your staff, with their dependable expertise, have been a valuable asset to Musco Food Corporation in our efforts to keep pace with an ever-evolving market.

We wish you continued success."

Musco Food Corporation, Maspeth, NY

Proofpoint: Advanced Email Security

continued from pg. 4

analyzing hundreds of thousands of email attributes.

These include the sender/recipient relationship, headers, and content.

Protecting Against Advanced Threats-Targeted Attack Protection

Proofpoint Targeted Attack Protection (TAP) helps detect and block advanced threats, including ransomware, that target people through email. We detect known threats and new, never-before-seen attacks that use malicious attachments and UR Ls with dynamic and static analysis techniques. TAP is unmatched at stopping attack techniques such as polymorphic malware, weaponized documents, and sandbox evasion.

Through the TAP dashboard, you get unsurpassed visibility into the threats that are hurting your business. TAP gives you the insight you need to understand attack campaigns and the threat actors behind them. At the same time, industry and geographical threat analysis give you a complete picture of the individual threat landscape for your business.

Preventing Email Fraud-Email Fraud Defense

Building on the email analysis offered by Email Protection, Proofpoint Email Fraud Defense protects against today's advanced email threats, including email fraud and consumer phishing. Visibility into who is sending email across your enterprise enables you to authorize all legitimate senders and block fraudulent emails before they reach your employees, business partners and customers.

Email Fraud Defense is the only email authentication solution that helps you fully deploy DMARC (Domain-Based Message Authentication, Reporting & Conformance) faster with less risk. Integration with Email Protection offers visibility into the security posture of your supply chain.

Prevent Attacks Using Lookalike Domains-Domain Discover

Attackers often register domains confusingly similar to those owned by trusted brands. These lookalike domains can trick victims into trusting unsafe email.

Proofpoint Domain Discover searches for domains that could be mistaken for yours. It categorizes them according the threat they pose. And it helps you block email from any suspicious or unsafe domain before attackers can use them. You can integrate this proactive intelligence with policies defined in Email Protection to automate the process.

continued on pg. 6

"Attackers often register domains confusingly similar to those owned by trusted brands. These lookalike domains can trick victims into trusting unsafe email."

Proofpoint: Advanced Email Security

from our Tech Staff

Control Data Loss-Information Protection

Proofpoint Information Protection provides far-reaching visibility out of the box. Though a flexible, cloud-based platform, you get advanced data loss protection without the complexity and costs of legacy tools. Easily manage sensitive content sent through email. Automatically classify information according to your security policies and industry standards. And transparently encrypt and quarantine your data.

Respond to Malicious Email—Threat Response Auto Pull

Proofpoint Threat Response Auto Pull (TRAP) takes the manual labor and guesswork out of incident response to help you resolve threats faster and more efficiently. Automatically remove already-delivered email from users' inbox and get an actionable view of threats. Our threat-management platform enriches alerts and automatically collects and compares forensic data. You can quarantine and contain users, hosts, and malicious email attachments—automatically or at the push of a button.

Maintain Email during a Server Outage—Email Continuity

Email Continuity ensures that users' email, calendar, and contacts are always available to them, even when your regular email service is down. Your users stay productive, sending and receiving email—no IT intervention needed. The service is always hands on, hands-off, and works automatically to ensure that an email outage doesn't disrupt your business

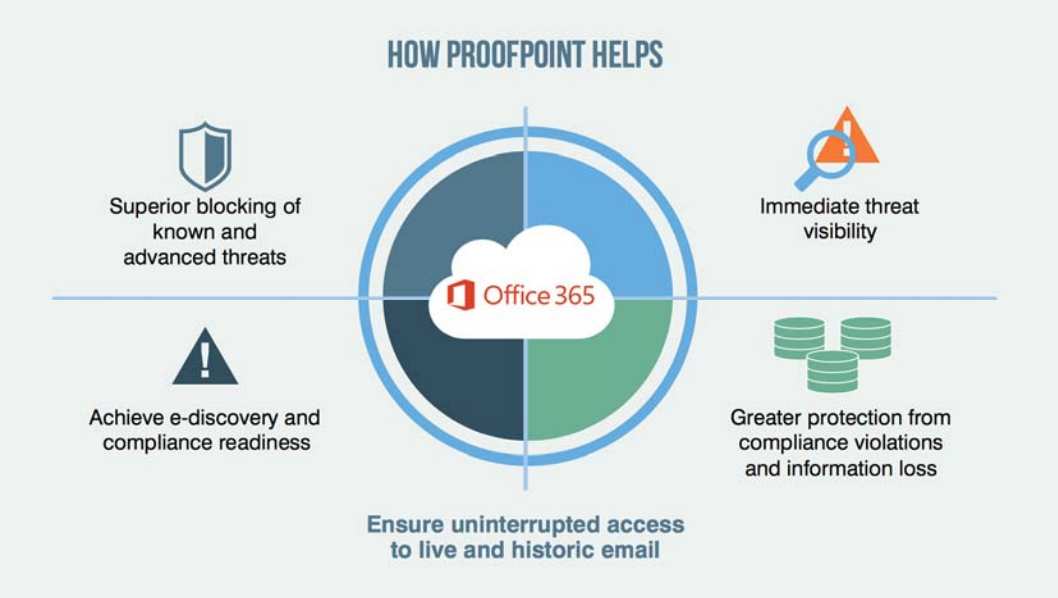
Test and Train Users—Wombat Anti-Phishing Suite

Wombat Anti-Phishing Suite carries out simulated attacks on your users to help gauge how prone they are to falling for today's threats. It depicts a wide range of real-world attack techniques including attachments, embedded links and requests for personal data. Users that fail the simulation can be auto-enrolled into relevant security training.

For more information about Proofpoint Advanced Email Security, please contact your local ***ASK Sales Rep*** at (610) 617-0300.

wombat security
a division of proofpoint

"Wombat Anti-Phishing Suite carries out simulated attacks on your users to help gauge how prone they are to falling for today's threats. It depicts a wide range of real-world attack techniques including attachments, embedded links and requests for personal data. Users that fail the simulation can be auto-enrolled into relevant security training."



proofpoint.

ASK Technologies, Inc.

7 Bala Avenue
Suite 201

Bala Cynwyd, PA 19004

610-617-0300 Office
610-617-0307 Fax
info@asktech.com

*For operational excellence at predictable costs, turn to **ASK**.*

SHORT CUTS
for Windows 10

Windows key + D
Display and hide the desktop.

Windows key + L
Lock your PC or switch accounts.

Windows key + M
Minimize all windows.

Windows key + R
Open Run dialog box.

Windows key + S
Open Search.

Windows key + U
Open Ease of Access

ASK TECHNOLOGIES, INC.

Creating new standards in multi-service network integration.

Homeland Security National Cyber Awareness System: Ongoing Threat of Ransomware

From our Tech Team

National Cybersecurity and Communications Integration Center (NCCIC) has observed an increase in ransomware attacks across the world.

Ransomware is a type of malicious software or malware, designed to deny access to a computer system or data until a ransom is paid.

Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

Ransomware can be devastating to an individual or an organization. Anyone with important data stored on their computer or network is at risk, including government or law enforcement agencies and healthcare systems or other critical infrastructure entities.

Throughout different ransomware events, NCCIC's best practices and guidance remain the same:

- Create system backups
- Be wary of opening emails and attachments from unknown or unverified senders
- Ensure that systems are updated with the latest patches

NCCIC encourages users and administrators to review its Ransomware page and the U.S. Government Interagency Joint Guidance for further information.

Contact your local ***ASK Sales Rep*** for more information about protecting your business from the ongoing threat of ransomware, by calling (610) 617-0300.

Protect Your Workplace: Cybersecurity Guidance

as featured on us-cert.gov

For Employees:

• Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
• Change your passwords regularly (every 45 to 90 days).
• Do NOT give any of your usernames, passwords, or other computer/ website access codes to anyone.
• Do NOT open emails, links, or attachments from strangers.
• Do NOT install or connect any personal software or hardware to your organization's network without permission from your IT department.
• Report all suspicious or unusual problems with your computer to your IT department.

For Leadership & IT Professionals:

• Implement Defense-in-Depth: a layered defense strategy includes technical, organizational, and operational controls.
• Establish clear policies and procedures for employee use of your organization's information technologies.
• Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
• Update your system's anti-virus software daily.
• Regularly download vendor security "patches" for all of your software.
• Change the manufacturer's default passwords on all of your software.
• Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.