



# STASH®

THE BREACH STOPS HERE

---

NO RANSOM RANSOMWARE PROTECTION  
Mitigates the attack and the attacker

---

ZERO TRUST & DLP  
Secure data governance & access platform

---

DATA & SYSTEM RESTORATION  
in real-time

---





## GRANULAR CONTROL, PROTECTION, RESILIENCY & RESTORATION OF DATA INSIDE & OUTSIDE OF THE ORGANIZATION & THE SYSTEM THAT RUNS IT

- Proactive Offensive Protection
- Agnostic
- Persistent
- Autonomous
- Automatic
- Controlled Access
- Zero Trust
- No Ransom
- Quantum-resistant
- Data Security
- Data Privacy
- Data Resilience
- Data Residency
- Data Governance
- Real-Time Data Restoration with a Click
- System Restoration in 2 Hours

02

# TABLE OF CONTENTS

---

<b>INTRODUCTION</b>	<b>4</b>
• Digital Revolution Security Impact	7
• Security Drivers 2023 and beyond	8
• What Business & Government Want	9
• Why STASH® Delivers	10
<b>ORGANIZATIONAL RISKS &amp; CHALLENGES</b>	<b>11</b>
• Solution	12
• Key Components	13
• Technology	14
• User Experience	15
<b>DESIGN</b>	<b>16 - 17</b>
<b>FEATURES   BENEFITS   VALUE</b>	<b>18 - 20</b>
<b>USE CASES</b>	<b>21 - 27</b>
<b>STASH® SOLUTIONS SUITE</b>	<b>28</b>
<b>RETURN ON INVESTMENT</b>	<b>29</b>
<b>APPLICATIONS</b>	<b>30 - 31</b>
<b>CONTACT DETAILS</b>	<b>32</b>

# INTRODUCTION

---

The **STASH**<sup>®</sup> Data & Image Protection & Restoration with No Ransom Ransomware Solution is a unique data protection and resilience platform for commercial and government use designed for deployment in environments where granular data control and eradication of data compromise are highly sought-after outcomes. An all-in-one, quantum-resistant, agnostic, automatic and autonomous solution in a sea of tools, it provides proactive datacentric data protection directly to data bytes at creation, during transit, when sharing inside and outside of an organization, and at rest in any cloud configuration or off-cloud storage environments.



**UNSECURED,  
UNPROTECTED DATA**



**SECURED, PROTECTED,  
RESILIENT DATA**

# IMPACT

---

The **STASH**<sup>®</sup> Data & Image Protection & Restoration with No Ransom Ransomware Solution is a deliberate departure from low-value defensive modes of data management. Distinctly effective when high performance proactive Secured Data Governance and Ransomware Protection recovery is required, supporting data regulatory compliance, sovereignty, and residency demands. Delivered via modular, low friction, no integration required activation, it brings complete, real-time/all the time data protection, as well as visibility to where data is. Suitable for the largest through smallest organizations, it is the ubiquitous antidote to the pervasive problem of data breach, loss, manipulation, and ransomware that defensive tools cannot solve. The **STASH**<sup>®</sup> Data & Image Protection & Restoration with No Ransom Ransomware Solution was developed to deliver a previously unavailable and unobtainable level of Secure and Resilient Data Governance, reducing immediate and future financial, and also human losses from data compromise to the lowest possibility ever.

The **STASH**<sup>®</sup> Data & Image Protection & Restoration with No Ransom Ransomware Solution blankets any platform, network, infrastructure, and every format of unstructured data with omnipresent protection, ensuring always available and ever resilient data. It is an organic fit to all legacy and later technology tools, built to flexibly augment or replace low value tactics. How to use the solution is solely in the hands of the organization, orchestrated by an administrator dashboard. 100% maintained and supported by **STASH**<sup>®</sup>, but 100% controlled by the organization, it works in the background with minimal friction, invisible latency, with no actions other than 'business-as-usual' required of users.

**STASH**<sup>®</sup> has no access to data other than its own; patented multi-component quantum-resistant keys are activated at use and destroyed after. The Solution allows cloud providers, systems integrators, and other technology business partners (TBP) to quickly, seamlessly, and efficiently add the solution as an OEM component that completely seals the holes inherent in long-time defensive solution postures. Critically, The Solution allows service providers (SP) to deploy a broadly adaptable, highly scalable, easy to implement, cost-efficient solution with excellent ROI, streamlining the sales and delivery process to support more customers with less effort and exceptional problem resolution vs the status quo.

# COMPETITION

---

Due to the very competitive nature of today's cybersecurity environment, cost of ownership, time to market, and proven effectiveness have become critical criteria in commercial and government environments, and to service providers and their customers, when selecting data protection protocols and the tools that support them. Traditional defensive security options, while showcasing the appearance of positive results, have proven to be ineffective, very expensive, time consuming to deploy, and questionably cooperative with existing tools. They are rarely nimble, and often require additional human and capital requirements that stifle flexibility and adoption. Often, the user experience is onerous, prompting an often-lamented scenario of non-compliance at the weakest security link: the user. They are often not a cost-effective alternative for smaller organizations and service providers. While large organizations can afford to choose any defensive option, the cost to value ratio of ineffective data protection tools extrapolates with the increasing size of the organization and data volume, quickly creating a chasm of low value, high-cost failure to protect data, and greater probability of data compromise.

The **STASH**<sup>®</sup> Data & Image Protection & Restoration with No Ransom Ransomware Solution is a radically effective departure from security postures comprised of application stacks cobbled together from disparate sources. In and of themselves, these create the requirement of a 'business within a business', that of deploying, integrating, and perpetually managing data management and security applications, at the expense of working with data to generate ROI. The Integrated Secure Data Governance Solution is an innately viable alternative that offers a refreshingly complete, flexible, non-proprietary, set it and forget it answer to secure and resilient data governance requirements anywhere in the world.

This document describes how **STASH**<sup>®</sup> approaches data security and resilience, and how the solution protects data while it is in use, in transit, and while stored or archived.

# DIGITAL REVOLUTION SECURITY IMPACT

---



## **SECURITY IS ERODING AS AN INHIBITOR OF CLOUD DEPLOYMENT.**

- Cloud currently supports 80% of enterprise workloads.
- More enterprises are using cloud services for complex, mission-critical, and high-risk applications.



## **ENTERPRISE & CLOUD PROVIDERS MUST MANAGE SECURITY TOGETHER.**

- Cloud providers are responsible for physical hosts, networks, and data centers - not what resides in the Cloud.
- Enterprises retain responsibility for user identity and access management rules, data security and handling policies, and application security practices.



## **HYPERSCALERS INCREASINGLY ADD FUNCTIONALITY AND EYE ON-PREM INCURSION.**

- Most enterprises look outside of hyperscalers for their security options, but hyper-scalers (AWS, Google, Microsoft, et al.) are looking to penetrate and capture on-prem environments with 'cloud to ground' initiatives.

**80% OF ENTERPRISE WORKLOADS ARE IN THE CLOUD**



# STASH<sup>®</sup> SOLVES

## THE MOST CRITICAL SECURITY DRIVERS 2023>

---

**1 • INCREASING ENTERPRISE VULNERABILITY DUE TO GROWTH OF CLOUD MIGRATION, MOBILE ENDPOINTS, AND IOT DEVICES.**  
forcing evolution of entire security stack, deployment, and purchasing models.

**2 • ATTACK SURFACE EXPANSION ACCELERATES WITH IOT/OT PROLIFERATION, DEVOPS ADOPTION, AND THIRD-PARTY RELATIONSHIPS.**  
Porous perimeters, poor IT hygiene, failure to accept cloud responsibility, and security awareness deficits enable exploits.

**3 • RESURGENT PRIVACY AND OTHER REGULATIONS FUELED BY THE SURVEILLANCE ECONOMY BACKLASH, THIRD PARTY RISK AWARENESS, AND UNRELENTING HACKS.**  
GDPR, CCPA, and CMMC are harbingers of more to come.

**4 • TALENT DEFICIT IN BOTH CLOUD AND SECURITY FUELS PRODUCT-FOR-PEOPLE SUBSTITUTIONS.**

- 69% of enterprise executives believe artificial intelligence will be necessary to respond to cyber attacks.
- Pro-Serv, Managed Services, and AI/ML automation critical to augment or stretch available resources.



# THE PRESENT & FUTURE IS STASH® DATACENTRIC

---

## WHAT BUSINESS & GOVERNMENT WANT...

- Consolidated All-in-One Solution.
- One-Click No Ransom Ransomware, Protection, & Restoration.
- Buy and Use - No Stack Building.
- Data Focused Security.
- No Integration Required.
- Agnostic.
- Autonomous.
- Bolsters or Replaces Legacy Tools.
- Minimal Latency.
- Cost-Effective.
- Low Friction Deployment.
- Previously unobtainable efficacy
- Business as Usual UX.
- On-Cloud or On Local, Private Servers.

## ...THAT STASH® DELIVERS

# WHY?

---

Organizations are facing increasing external cyber-attacks as well as insider threats. Criminals, nation state actors, and even interested commercial parties are attracted to the crown-jewel types of data with which enterprises are often entrusted.

As **Microsoft, Okta, Roku, Boeing, U.S. Government, Infosys, IBM, Sony, Duolingo, Giant Tiger, Bank of America, Trello, Norton Healthcare, 23andMe, LastPass, U.S. Marshalls Service, Royal Mail, Dish Networks, JBS, Colonial Pipeline, Kaseya** and many other breaches in the last few years have shown, even sophisticated firms can be hacked with devastating impact on their reputations, customers, partners, and value. RaaS (Ransomware as a Service) has become a one stop shop for nefarious actors, easy to purchase and deploy with very lucrative outcomes. The consequences of breach can deeply compromise large organizations and destroy smaller ones with massive financial and even political consequences.


Organizations that hold intellectual property, merger and acquisition, commodity investment, contract negotiations, proprietary trade secrets, market deals, and other sensitive data are phenomenally attractive.

# THE RISK IS AS REAL FOR SMALL COMPANIES AS THE LARGEST ORGANIZATIONS.

A UBIQUITOUS PROBLEM REQUIRING THE **STASH**<sup>®</sup> UNIVERSAL SOLUTION.


ORGANIZATIONS ARE CHALLENGED WITH THE NEED TO EXERT GRANULAR CONTROL OVER ORGANIZATIONALLY AND CLIENT SENSITIVE DATA.

THEY FACE THREE PRIMARY CHALLENGES:

1.  The lack of technical controls associated with data entrusted to an employee or business partner.

2. The risk posed by negligent handling & deliberate misuse of data by employees, business partners, or criminals.



3.  The need to store and access sensitive data for long periods of time.

# WHAT IS THE **STASH**<sup>®</sup> DATACENTRIC SOLUTION?

---

## IN THE LAST 5 YEARS:

6,000 SECURITY  
TOOLS LAUNCHED  
YET THERE WERE  
185M+ REPORTED  
DATA BREACHES.

## THE FBI SAYS:

THIS REPRESENTS  
10-12% OF THE  
ACTUAL NUMBER  
OCCURRING.

**STASH**<sup>®</sup> is an OEM solution based on existing commercially viable technologies. Not simply another tool, **STASH**<sup>®</sup> provides proactive, comprehensive protection of data at creation, rest, and in transit. The solution was designed to:

1. Enable the secure creation, amendment, and sharing of unstructured data without the need of user or administrator management.
2. Provide access notification and classification controls.
3. Deliver secured data that is stored in multiples for resilience, in environments chosen by the customer including on-premise, private cloud, public cloud, and hybrid cloud.
4. Bolster the effectiveness of existing technology stacks and/or replace legacy tools.
5. Enable control of data in the background, inside and outside of the organization without changes in workflows or user dependencies.

# KEY STASH<sup>®</sup> COMPONENTS

---

## DIGITAL CONFETTI<sup>®</sup> .....

Any format of unstructured data is encrypted with 256-bit encryption, the strongest and most robust encryption standard that is commercially available today. It is then parsed into an arbitrary number of small pieces, before the data is multiplied at a minimum of 3 copies (more/fewer upon client request) and stored, archived, and preserved at multiple locales, on-cloud or off, of an organization's choosing. The data synchronizes with the end-user system and is stored in virtual folders, protected from creation through destruction, in-transit, in-use, and at-rest, in the hands of legitimate users and when it gets into the hands of malicious actors.

## ..... KEYS-ON-THE-FLY<sup>®</sup>

The **STASH<sup>®</sup>** patented quantum-resistant symmetric encryption keys encrypt and decrypt files. They are built from a number or separate components from **STASH<sup>®</sup>** and from the organization that must come together in order to 'unlock' the encryption function.

Much like a nuclear launch pad, the components activate to form a complete key. The key or keys are destroyed after each use, only to be activated when an organization does so. The keys are not stored anywhere in between. No one else has access to your data, including **STASH<sup>®</sup>**. It's a part of our 'your data is yours, period' promise.

## NO RANSOM RANSOMWARE SOLUTION .....

- Mitigation by circumvention of attack and attacker.
- Files restored in real-time from admin dashboard.
- Frozen file content not accessible by the attacker.
- Release or destruction of files don't matter.
- No ransom to pay.

## ..... DIGITAL RIGHTS MANAGEMENT

Digital Rights Management (DRM) consists of two main logical components:

1) Data Protection, and 2) Data Governance. **STASH<sup>®</sup>** encryption technologies are used to provide data (content) protection, while DRM trust management and policy management technologies are used to allow protected information to be distributed and used by authorized entities only. The user, the most vulnerable weak point in any security protocol, is removed from the decision-making process regarding data access inside and outside of the organization. Intentional or inadvertent release of data to those without access is eradicated.

## STASHIMAGE<sup>™</sup> and STASHSECURE<sup>™</sup> .....

**STASH Image<sup>™</sup>** and **STASHSecure<sup>™</sup>** is a revolutionary data and system protection service. Working in the background, **STASHImage<sup>™</sup>** creates a secure snapshot of your system (operating system, application, configuration, and data) while **STASHSecure<sup>™</sup>** encrypts, shards, makes copies, and distributes the shards of company documents to multiple locations. When your system is compromised (or just fails), you can restore the System Snapshot quickly and easily – all the hard work is done for you. With our new Priority Restoral feature – even large organizations can recover quickly. Data is also restored with the click of a button from a dashboard. No onerous support task, no internal denials of service, it just works, getting you back to work.

# HOW STASH<sup>®</sup> WORKS: TECHNOLOGY

---

## ZERO TRUST

PROACTIVE NOT DEFENSIVE. THE BREACH STOPS HERE.



Quantum Keys-on-the-Fly<sup>®</sup> Secures Data Worldwide  
24/7/365



Multiple Copies  
DigitalConfetti<sup>®</sup> Multiple Places for Resilience



Prevents Data Leakage & Exfiltration with Access Control (DRM)



Touchless Synchronization In/Out of Organization



Protects Content from Creation through Deletion



Security Stays with Data Everywhere

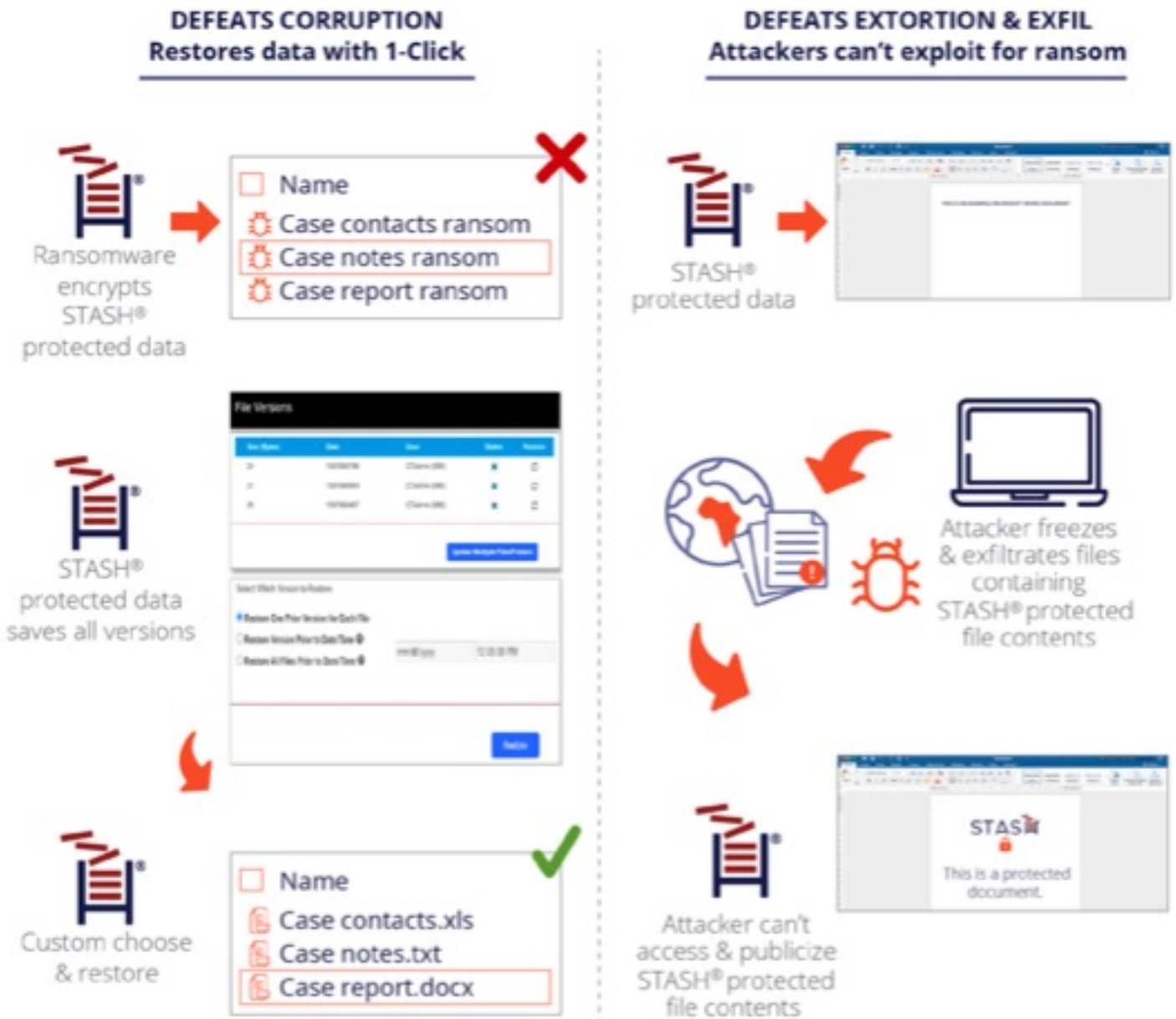
## PLUS



## PLUS 1-CLICK NO RANSOM RANSOMWARE PROTECTION & RESILIENCE

Data, infrastructure, network, and platform agnostic, designed for a seamless "business as usual" user experience, **STASH<sup>®</sup>** provides granular control to administrators without the need for integration. It is turn-key, activated, and supported by **STASH<sup>®</sup>**.

# HOW THE STASH® NO RANSOM RANSOMWARE SOLUTION WORKS



**STASH®** operates behind the scenes, making it possible for users in the organization to go about their business without changing anything about the way they do business. Persistent automatic data protection at the byte level wrapped in digital rights management (DRM) performs seamlessly with minimal latency in person-to-person or machine-to-machine (M2M) data exchange environments.



# STASH<sup>®</sup> DESIGN

---



MODULAR



SNAP-ON



NO INTEGRATION



MINIMAL  
FRICTION



OEM

The **STASH<sup>®</sup>** architecture was deliberately developed to mitigate the risk, complexity, time, and expense typical of the deployments and integrations that have plagued defensive security postures of the past. This ensures that organizations have the flexibility to use **STASH<sup>®</sup>** to amplify and bolster existing applications and architecture choices or to replace legacy or redundant tools with **STASH<sup>®</sup>**. An illustration of some of the aspects of this modular freedom of choice is outlined in the following table.

# AUGMENT OR REPLACE

## Select Specific Modules

Organizations may be using proprietary and/or legacy tools. In this case, **STASH**<sup>®</sup> datacentric modules assimilate to bolster the existing platform, OR replace select tools for optimum performance and value. For example: An organization can choose to use its own single-sign-on, digital rights management, or data classification/tagging solutions and **STASH**<sup>®</sup> datacentric security modules will seamlessly fold in.

	ENTERPRISE APPROACH	STASH <sup>®</sup> OPTIONS
DISCOVERY & CLASSIFICATION	Integrate with solutions such as Boldon James, Tutus, others.	Integrate policy definition and management; utilize DRM features.
AUTHENTICATION	SSO (single sign-on), 3 <sup>rd</sup> party identity provider, token-based MFA (multi-factor authentication).	
QUANTUM RESISTANT ENCRYPTION	HSMs; proprietary key management and cryptographic systems.	Cloud or local storage locations; all pieces in one location, round robin use of each file location, or random distribution across locations.
SHARDING	Use of secret sharing-based algorithms; random size slices	Quantum resistant 2-key system; keys generated as needed, not stored, AES-256 standard algorithms to encrypt files.
STORAGE	Proprietary storage backend; use of distributed file systems; local tape or optical storage destinations	STASH <sup>®</sup> is its own identity provider; MFA, endpoint thumbprinting, & geolocation analytics.
DIGITAL RIGHTS MANAGEMENT	Integrate with Vera, Intralinks, Adobe Experience Manager, Fasoo, Nest Labs, SealPath Covertix, Digify, File Open Systems, Microsoft Azure Rights Management (ARM) and Active Directory Rights Management (ADRM), Vitrium Systems, CapLinked, Galaxkey, Forcepoint, Box, Sharepoint.	Integrated UI, automated classification engine, reporting micro service & Attribute Base Access Controls.

# STASH<sup>®</sup> FEATURES

---

The average enterprise is using 156 defensive security tools, at a cost of millions per year. An outcome of the use of these tools without a proactive datacentric security component has been pervasive data compromise.

## STASH<sup>®</sup> was built for this Presumed Failure.

- Administrative and user interfaces that control the data protection and management process (authorize/deauthorize users, remove data).
- A technology solution that can function across hybrid environments and perform required visibility and control functions (geolocation, authorization, alerting, revocation).
- Visibility and control capability that functions harmoniously with existing security and data governance policies (firewall rules, data retention/handling requirements, network/user access controls).
- Reporting on sensitive data accessed by authorized employees.
- Reporting on sensitive data accessed/attempted to be accessed by unauthorized employees/persons or nation states outside the organization.
- Enforcement of employee data access policy for data stored outside of the regular controls of the enterprise.
- One-click Ransomware recovery.
- Access data via SaaS, agent-based sync client, or through a flexible API.

# STASH<sup>®</sup> BENEFITS

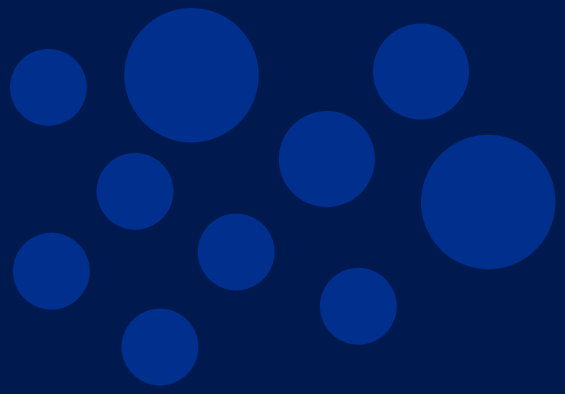
---



- Minimize low-value tactics & their cost.
- Proactive: mitigates need for resource intensive detection/remediation.
- Reduces loss expectancy from data compromise to statistical anomaly.
- Automatic persistent protection to sensitive data inside & outside of the organization.
- Smart access, control, and monitoring.
- Create secure/private workflows for seamless sharing of protected data.
- Exposes personnel and actors who attempt to leak, steal, and proliferate stolen data.
- Comply with existing/emerging national, Int'l & NATO data security standards.
- Supports privacy laws and protocols worldwide.
- Data breach no longer means data compromise.

**Cloud providers are only responsible for defensive security "of" the cloud. Organizations are responsible for the security and resilience of what's "in" the cloud - their data. Defense can't do that. STASH<sup>®</sup> does.**

# VALUE



The **STASH**® Solution protects unstructured data shared with partners inside and outside of the organization; the security stays with the data wherever it is or goes. **STASH**® takes a "belt and braces" approach to data security and resilience, delivering data privacy & security, plus granular control of data access.

**THE DATA IS NOW THE PERIMETER.  
STASH® DOESN'T PREVENT BREACHES;  
NO TECHNOLOGY CAN DO THAT.  
INSTEAD, IT PROACTIVELY PROTECTS THE MOST VALUABLE COMMON DENOMINATOR: THE DATA ITSELF.**

**THEY ARE AFTER THE DATA.**

**SO, STASH® MAKES THE DATA IMMUTABLE TO THEFT, LOSS, RANSOMWARE, AND HARM.**

You have 48 hours from a Ransomware attack to when your data is gone forever.  
- Federal Bureau of Investigation -

There is fatal flaw in the main assumption underpinning perimeter-based security - the assumption that there is a 'trusted' internal network where data is safe and an 'untrusted' external network where data is unsafe. This implicit trust assumption is both incredibly naïve and untenable. - Forrester -



# USE CASES

---

## FINANCE

Financial services firms are three times more likely to be targeted in a cyberattack than any other organization and are targets of 25% of **all** malware attacks. There is always a new way to lose data. The more 'all about the customer' your company becomes, the harder it is to control and secure your most valuable data resources.

Firms need to inventory their technology, decide what is necessary to keep, remove unnecessary technology debt, and identify the remaining risks. Many risks cannot be remediated by applying a patch.

By activating **STASH**<sup>®</sup>, financial firms have an opportunity to control and protect unstructured data anywhere they operate in the world, ensure privacy laws compliance, preserve current customers, and attract new ones.





# USE CASES

---

## GOVERNMENT

It's different for the Government. These aren't traditional ransomware attacks, or email phishing scams. Government hacks are calculated. They're resourceful. People that target the government's data, networks, and systems are often politically motivated and looking to steal specific information. In the most extreme cases, these hackers are state-funded, giving them the time and money they need to ensure their efforts are successful. Hacking is a full-time job for them.

Their data is also scattered in so many places that the only logical way to protect it is by protecting the data itself, where it lives, and where it travels to. This is where **STASH**<sup>®</sup> shines. Our no integration technology is capable of adjusting to the trove of disparate legacy tools and technologies the government uses to operate. Because we protect at the data byte level, networks, infrastructures, platforms are by-passed while the valuable data is secured & controlled.





# USE CASES

---

## HEALTH/LIFE SCIENCES

Cyber security breaches really do begin to edge into literal life and death territory when there is the potential for product manufacture compromise or manipulation, medication to be mixed up, or for patients to miss out on vital treatment.

Life Science organizations are reliant on a large number of third parties, including IT providers, data collection, external advisors, and analytic firms as well as Contract Manufacturing Organizations (CMOs) and Clinical Research Organizations (CROS). The use of third parties means that businesses rely on systems and data over which they don't have complete control, making them even more susceptible to a cyber event. Hackers fraudulently gain access to prescriptions, medical treatment, or Government benefits.

When **STASH**<sup>®</sup> is deployed, low value data security and control tactics can be jettisoned, granular control of data access and security is in the hands of the organization. Even **STASH**<sup>®</sup> doesn't have access.



# USE CASES

---

# TECHNOLOGY

In many ways, all organizations are technology companies these days. For the ones that are building, developing, and manufacturing the communications, networks, infrastructures, and platforms of tomorrow, the technologies our world will run on, data breach and particularly ransomware strikes real panic.

Cyber risks are omnipresent for these organizations. Hacktivism is another significant threat in this sector. The amount of valuable, confidential, and sensitive data these companies hold is often many times larger than those in other industries. When breached, the loss, manipulation, or theft of this data often means real disaster. Compromised competitive advantage, negative brand equity, and for public technology companies, a diminished stock price, one that historically doesn't recover at least 30% of its pre-breach value.

**STASH®** defeats data loss, compromise, manipulation, theft and ransomware with granular control of persistent, autonomous, data access and protection.



# USE CASES

---

## MANUFACTURING

Manufacturing sits at the constellation of a host of other Critical Infrastructure (CI) sectors including energy, health, the Defense Industrial Base (DIB), transportation, autonomous vehicles (cars, trucks, drones, planes), water/wastewater, satellites, communications, chemical and food/agriculture. Each is essential to the economic and national security of nations around the world - and can impact the health, safety and security of individuals.

Manufacturing is one of 55 national critical functions at highest risk for a cyberattack. Prime attack vectors include data integrity issues/modification of customer specifications prior to manufacturing, cyber-physical damage to manufacturing facilities and end products, and Intellectual Property (IP) theft.

With so much at stake on a worldwide basis, the security, resilience, and granular control of critical data in the manufacturing sector is of critical import. There is no more effective solution to these demands than **STASH®**.



# USE CASES

---

## SUPPLY CHAIN

Every organization of any kind has a supply chain comprised of internal and external partners, vendors, materials, transport, manufacturing, quality control, data exchange, equipment, information flow, and dozens of other functions.

Your company may have a cyber security risk strategy but what about your key suppliers that have access to your systems? Or a niche company supplying vital goods or services that has access to important information and an immature approach to data security? The next problem is your suppliers' suppliers. Poor information security practices by lower-tier suppliers can sink companies. It is estimated that over 1/3 of corporate IT breaches are via third-party suppliers.

Cyber resilience in supply chains is still to be achieved in the process of mitigating risks. Uncertainty by senior management is compounded by the increasing complexity of global supply chains. **STASH**® provides the means to insulate critical data and withstand the attempts of attackers from less prepared business partners to steal or harm your data.





# USE CASES

---

## LAW ENFORCEMENT

Local governments are under "near-constant attack." The unauthorized access or loss of law enforcement data due to a cyberattack has serious operational and privacy implications. The importance of cyber security needs to be considered from multiple perspectives-those of employees, community members, crime victims, witnesses, informants, and prosecutors. A cyber attack could compromise an agency's ability to protect life and maintain order, thus eroding trust and credibility.

One of the critical issues facing all law enforcement organizations is the exponential increase of various types of digital evidence the agencies need to collect and store, including reports, pictures, videos, and other electronic records. Police Departments must secure digital evidence to ensure the integrity of the information's authenticity, while still providing access that offers verifiable accountability.

**STASH**<sup>®</sup> is particularly well suited to solve the challenge of ensuring digital evidence is private, resilient, available to select viewers, and unassailable by rogue actors and nefarious employees alike.

# STASH®

## SOLUTIONS SUITE

ZERO TRUST, AUTONOMIC, HOLISTIC & SELF-HEALING

### KEYS-ON-THE-FLY®

- \*Quantum Resistant
- \*Privacy

### DIGITALCONFETTI®

- \*SA & Cloud Deployments

### ENCRYPTION

- \*AES-256

- \*\*Existing Customer Algorithm Support

### SERVICE-BASED & MODULAR

- \*API, PaaS, SaaS
- \*Extensible

### INTELLIGENT CONTROL

- \*Granular Access
- \*Autonomous
- \*Admin-Only

### DRM & DLP

- \*User Trust
- \*Privacy
- \*Access Tracking & Alerts

### DASH

- \*View only timed sharing
- \*File stays in vault

### EDGE, VAULT, & REDUNDANT STORAGE

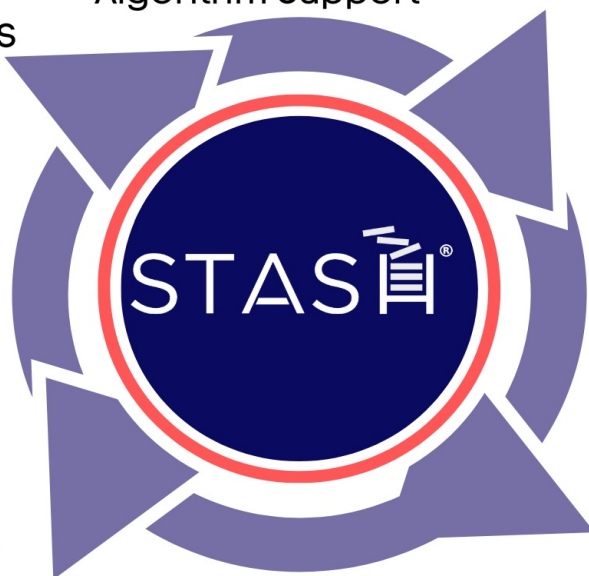
- \*Data-byte level protection
- \*Multiple Logistical Resilience

### STASHImage™ STASHSecure™

- \*System and Data Protection
- \*Real-time Restoration of Both

### NO RANSOM RANSOMWARE SOLUTION

- \*No Extortion
- \*No Ransom
- \*No Data Access
- \*Data Byte Protection
- \*Data Resilience



BUSINESS AND TRUST MODELS

28

# ROI

---

For the first time, organizations have automatic, autonomous, persistent, quantum-resistant, granular security and control of data on-premises, off-premises, in hybrid environments, in public or private clouds, and when stored locally anywhere in the world.

## **STASH® MITIGATES MILLIONS OF DOLLARS IN:**

- Ransom.
- Losses from business downtime.
- Fines and remediation.
- Negative brand equity.
- Diminished stock price (public companies).
- Lost customers.
- Employee turnover.
- Long term performance malaise.
- M&A abandonment/purchase price adjustment.
- Future attacks: if ransom paid, they'll be back.





# WHERE STASH<sup>®</sup> FITS

---

## **LARGE, COMPLEX NETWORKS WHICH:**

- Are highly segmented.
- Deliver a wide variety of services to both internal and external users.
- Exist in physical, virtual and hybrid environments.
- Are tightly regulated.
- Are geographically diverse.
- Are heterogeneous.
- Internationally distributed.

Solutions can be deployed on enterprise-class networks that operate both domestically and internationally.

STASH<sup>®</sup> was developed specifically to support data and IT resources that exist on customer premises, in a dedicated environment, at a co-location facility, exist in cloud and hybrid deployments.

## **OPERATING SYSTEMS:**

- Microsoft Windows Server 2016 or later.
- Microsoft Windows 7 or later.
- Mac OS X.
- Linux distributions including Ubuntu and Centos.

## **WITH TYPICAL ENTERPRISE SOFTWARE PACKAGES:**

- Microsoft Office Suite (including Word, Excel, PowerPoint), Open Office.
- Libre Office.
- E-Mail Archives (PST).
- Adobe Acrobat, or PDF creation clients.
- Adobe Acrobat Reader, or PDF viewing clients.
- Images, Audio, Video, and Media files.
- Database exports (.sql, json).
- Comma Separated Values (.csv).
- Source Code (.java, .php, .cs, html).
- STASH® protects any unstructured data files.
- SharePoint

## **THE ENTERPRISE'S ALREADY DEPLOYED SUITE OF SECURITY TOOLS INCLUDING:**

- Data classification and categorization.
- Data loss prevention.
- Firewalls.
- Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems (IPS).
- Authentication services.
- Identity services.
- Security Incident Event Manager (SIEM).
- Security Information Collectors (SYSLOG).
- Endpoint protection (anti-virus, anti-malware).

# **WHERE STASH® FITS**

---

31

## Contact Us



[chris@stash.global](mailto:chris@stash.global)

[janine@stash.global](mailto:janine@stash.global)

[john.dundas@stash.global](mailto:john.dundas@stash.global)



<https://www.linkedin.com/company/stash-global-inc/>



<https://www.facebook.com/stashglobal/>



<https://twitter.com/stashglobal>

**STASH**  [www.stash.global](http://www.stash.global)

## Find Us

