



Janusz Mierzejewski
Commvault/Metallic

Metallic® Solution Overview Customer Presentation

Helping customers face today's challenges

Digital transformation accelerates as risks are rising...

Rising cybercrime

Cybercrime increased **400%** during the pandemic²



Constrained resources

45% of businesses say they lack the funds to prepare for ransomware; **61%** believe they lack expertise³



Hybrid cloud data sprawl

80% of enterprises have a hybrid cloud strategy¹



1. State of the Cloud Report, Flexera, 2022
2. <https://www.Entrepreneur.Com/article/349509>
3. Cybersecurity in the Remote Work Era, Ponemon Institute, 2020

Safeguarding your data requires breadth, flexibility, and unmatched security

Mitigate your risk with a simple, SaaS-delivered solution



Comfortably meet SLA, retention and recovery requirements



Protect against ransomware and cyberthreats with layered security and early warning



Dynamically scale coverage, without egress charges



Deploy quickly and manage remotely



Remove capital, hardware, and infrastructure expenditures



Keep compliant with regulatory and eDiscovery controls



IDC projects DPaaS will surpass traditional DRP in 2021 or 2022¹



**Ransomware
Protection**



**Hybrid Cloud
Transformation**



**Data
Compliance**



Industry-leading DMaaS from the minds of Commvault



* customers remain responsible for complying with applicable laws

Metallic® SaaS Solutions

Data Protection as a Service (DPaaS) for your entire data estate

Hybrid Cloud Protection

Storage + Archive optional



Metallic® VM & Kubernetes Backup*

For VMware, Hyper-V, VMC, Azure VM, AWS, Oracle Container Engine for Kubernetes (OKE), Amazon EC2, OCI VM



Metallic® Database Backup*

For Microsoft SQL Server, Azure SQL Server, Azure MySQL, Azure MariaDB, Azure PostgreSQL, Azure Cosmos DB, Oracle, Oracle RAC, Oracle Database Cloud Service (DBCS), Oracle ExaData Database Service on OCI / on premises, SAP HANA, Amazon RDS, Amazon DynamoDB, Amazon DocumentDB, Amazon Redshift



Metallic® File & Object Backup*

For Windows Server, Linux/UNIX, Azure Blob & Files, OCI Object Storage, Amazon S3

Secure Cloud Storage



Metallic® Recovery Reserve™*

For air-gapped, long and short-term retention



Metallic® File & Object Archive

For cost efficiency and compliance of unstructured data

Archive & Compliance

SaaS App Protection

Storage included



Metallic® Backup for Microsoft 365^{†*}

For Exchange, Teams, SharePoint, OneDrive, Project



Metallic® Backup for Microsoft Dynamics 365*

For CE applications



Metallic® Salesforce Backup*

For production and sandbox environments

Endpoint Protection

Storage included



Metallic® Endpoint Backup^{†*}

For laptops and desktops

Threat Detection + Response



Metallic® ThreatWise™

For early warning into threats



Security IQ*

FREE WITH ANY SUBSCRIPTION
For actionable threat insights

Active Directory Protection



Metallic® Active Directory Backup

FREE WITH ANY SUBSCRIPTION
For Azure & Microsoft AD

[†] eDiscovery available

^{*} Metallic Government Cloud available
(FedRAMP High, hosted on Azure Government)

FROM INDUSTRY-LEADER

COMMVAULT 

Metallic® SaaS Solutions

Data Protection as a Service (DPaaS) for your entire data estate

Hybrid Cloud Protection

Storage + Archive optional



Metallic® VM & Kubernetes Backup*

For Microsoft Hyper-V, VMware, Azure VM, Kubernetes, Microsoft Azure, AWS, AVS, VMware Cloud



Metallic® Database Backup*

For Microsoft SQL, Azure PaaS, Oracle, Amazon AWS, SAP HANA



Metallic® File & Object Backup*

For Windows Server, Azure Blob & Files, OCI Object Storage, Amazon S3, Linux/UNIX

Secure Cloud Storage



Metallic® Recovery Reserve™*

For air-gapped, long and short-term retention



Metallic® File & Object Archive

For cost efficiency and compliance of unstructured data

SaaS App Protection

Storage included



Metallic® Backup for Microsoft 365^{†*}

For Exchange, Teams, SharePoint, OneDrive, Project



Metallic® Backup for Microsoft Dynamics 365*

For CE applications



Metallic® Salesforce Backup*

For production and sandbox environments

Endpoint Protection

Storage included



Metallic® Endpoint Backup^{†*}

For laptops and desktops

Threat Detection + Response



Metallic® ThreatWise™

For early warning into threats



Security IQ*

FREE WITH ANY SUBSCRIPTION
For actionable threat insights

Active Directory Protection



Metallic® Active Directory Backup

FREE WITH ANY SUBSCRIPTION
For Azure & Microsoft AD

[†] eDiscovery available

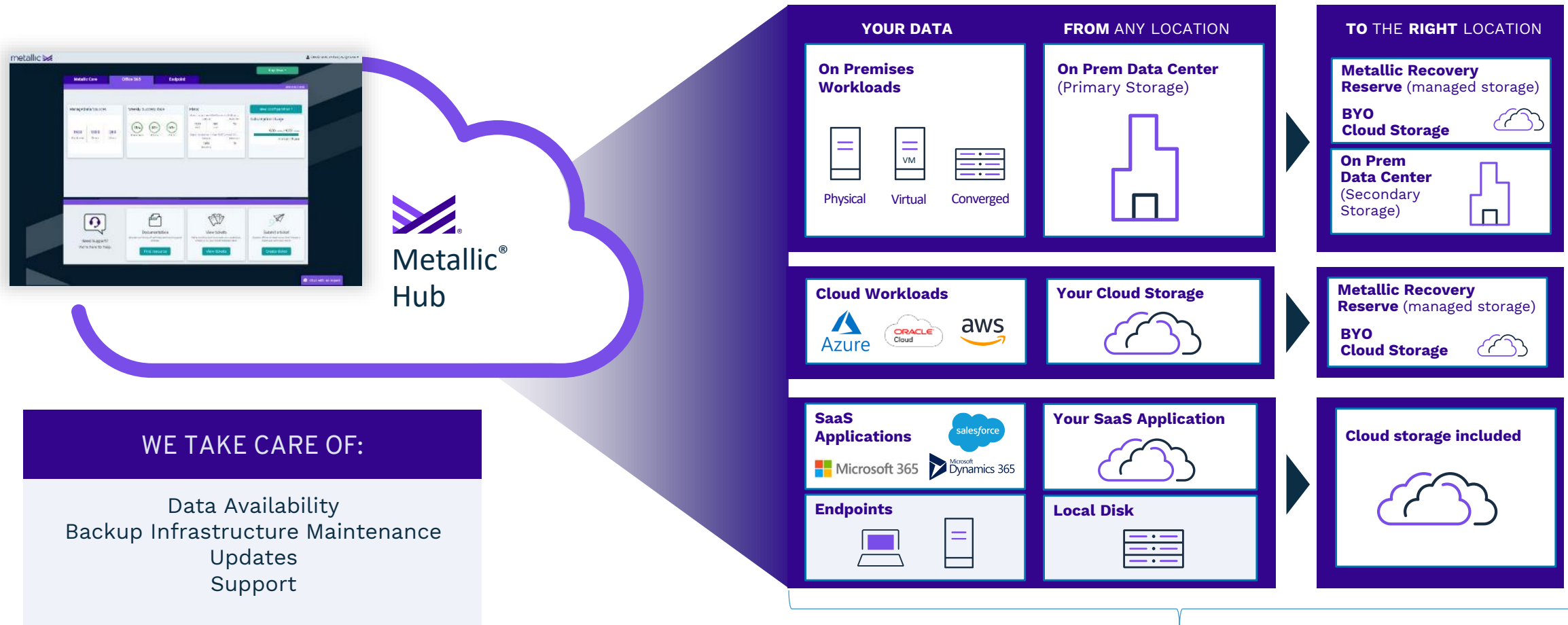
^{*} Metallic Government Cloud available
(FedRAMP High, hosted on Azure Government)

FROM INDUSTRY-LEADER

COMMVAULT 

Metallic: How It Works

The end user logs into Metallic for fast deployment and guided setup



Our Multi-Layered Security Approach

A new and differentiated approach to Data Protection

YOUR DATA

On Premises Workloads



Physical Virtual Converged

Cloud Workloads



Endpoints



SaaS Applications



Threat Sensors &
Ransomware
Alerts

Data encryption
in-flight/at-rest

Isolated
virtual
air gap

Separate
security domain

Security IQ Insights -

- Anomaly detection
- Trends & monitoring
- User behaviors

**Metallic
Control Plane**

Built-on
Microsoft Azure

Multi-factor Authentication
Zero-trust access controls

Immutable
data backups



The Metallic® Difference

Cloud-based data backup from industry-leader Commvault

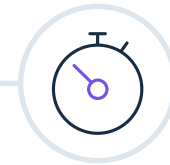
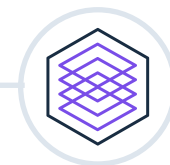
Safeguard your data and comfortably meet SLAs

No compromise SaaS
enterprise-grade coverage with
reduced management overhead

Up in minutes
pre-configured plans & best
practices built-in

Unique SaaS Plus
storage flexibility for
performance and value

Isolated, immutable backups
air-gapped coverage from
deletion or attack



Layered security

ransomware protection, advanced
encryption, and comprehensive
access controls

Ultimate performance

flexible, granular search with
rapid restore options

Data compliance

GDPR, ISO 27001, & SOC2 Type II
compliant*

Why Metallic SaaS?

A Fit for Changing Times

Smart Security:

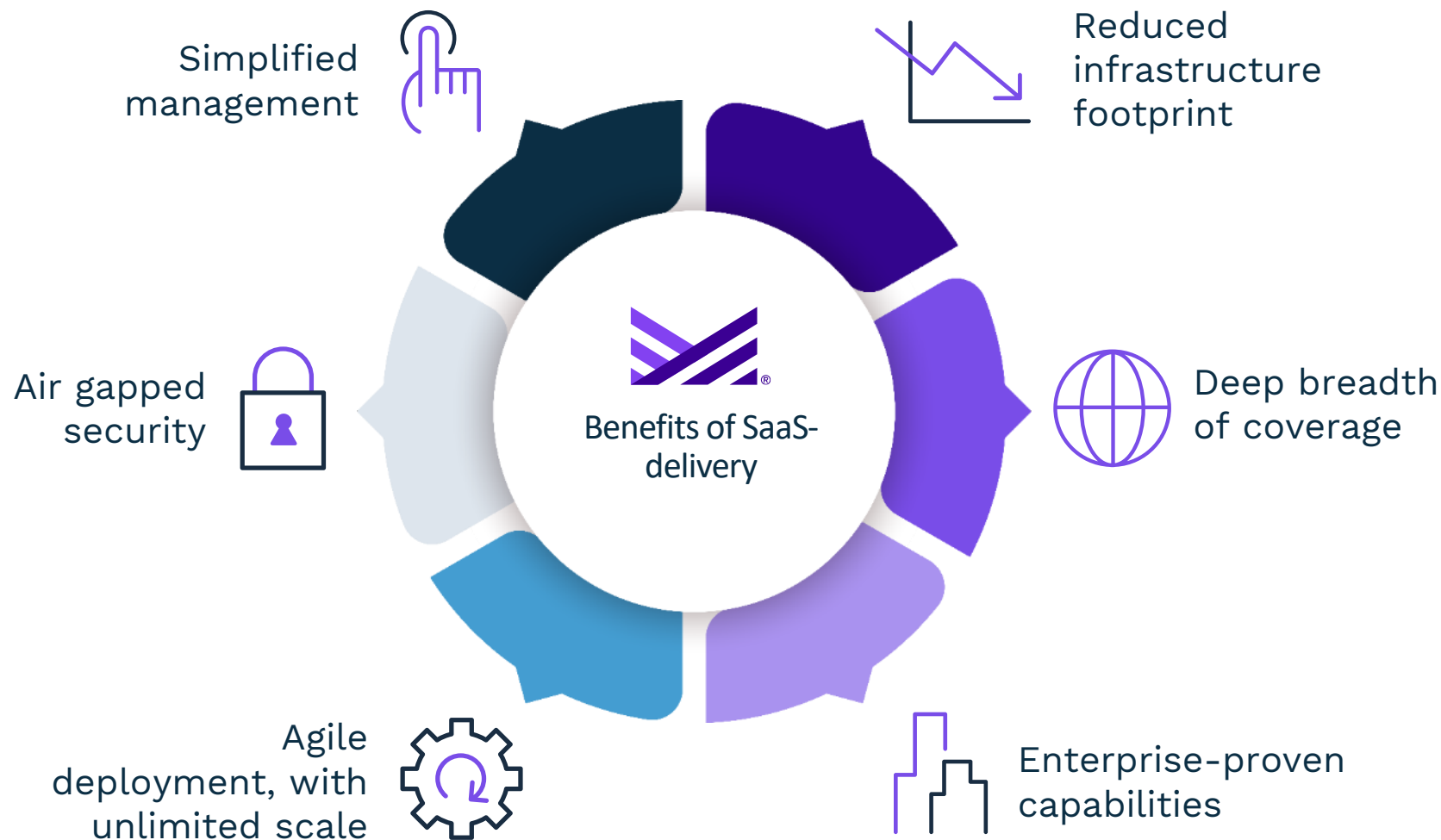
Improve ransomware protection

Smart savings:

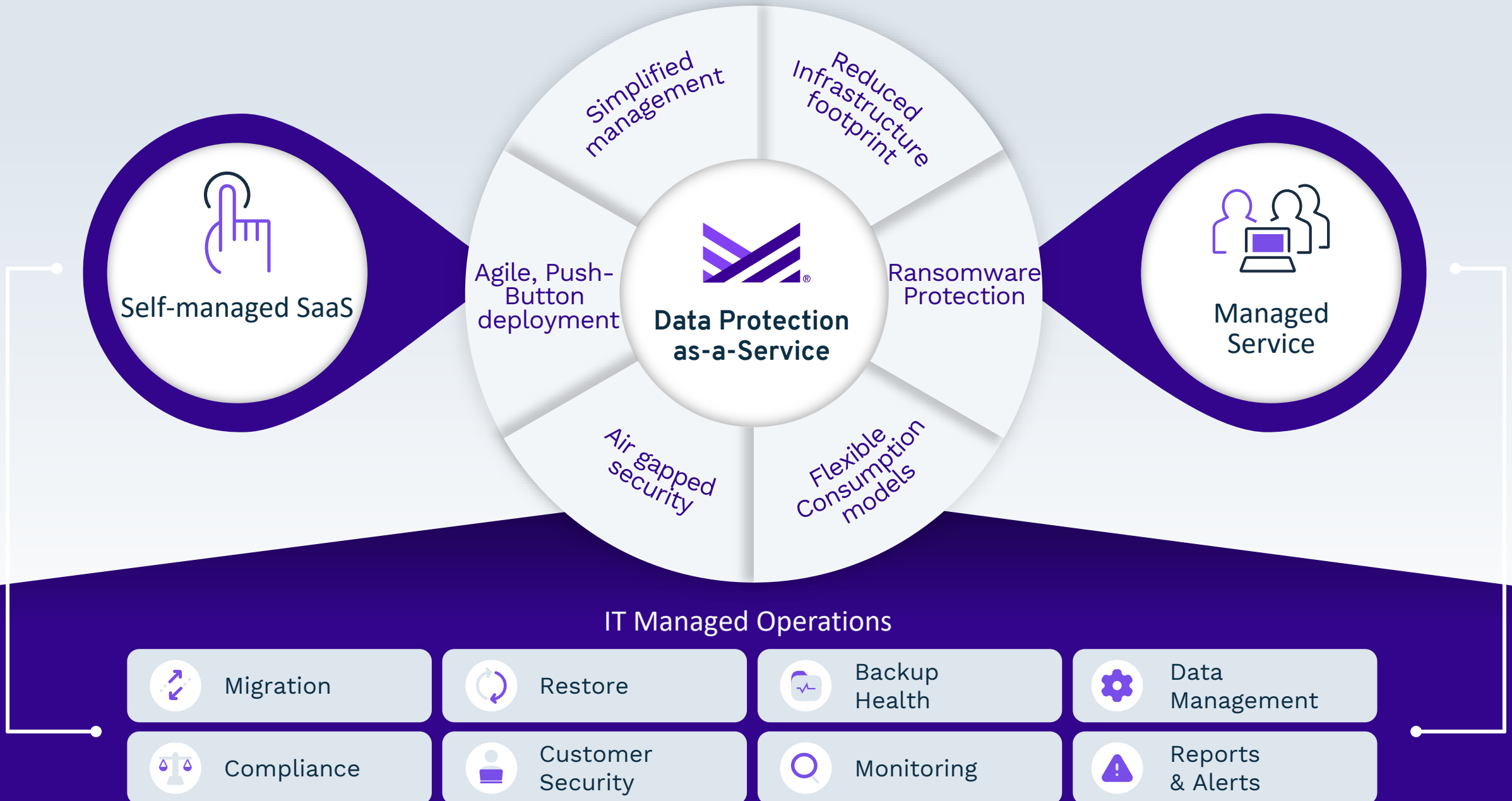
Create resource efficiencies

Smart modernization:

for hybrid cloud transformation



Protect your data, your way...



Recent Innovations: A Year in Review



New Offerings for SaaS App Protection

Comprehensive offerings including [Salesforce Backup](#), [Dynamics 365 Backup](#), and [Active Directory Backup](#).



New Enterprise and Multi-cloud Support

Continued addition of [multi-cloud support](#) across Microsoft, OCI and AWS - from databases to VMs and storage.



Expanded Storage Offerings

Flexible tiers for [Metallic Recovery Reserve](#) on Azure or OCI, plus [Commvault HyperScale X](#) for managing data at the edge



Geo expansion

[APJ and EMEA expansion](#) - now available in more than 30 countries and growing.



FedRAMP High Ready

for protection of [GCC High environments](#) – the only vendor in our space to achieve this status



Security Innovations

[ThreatWise early detection and warning](#) through cyber deception technology
[SecurityIQ](#) for simple [security insights](#)



Enhanced Experience and Support

Support portal with [Knowledge Hub](#)
[24x7 hotline](#) and [chat](#) support
Customer Community



And More!

Continued product innovations, features and enhancements

Supported Platforms and Applications

File System Backup

- Linux/UNIX
- Windows Server

Hypervisors

- VMware
- Hyper-V

Application Databases

- Microsoft SQL Server
- Azure SQL Server
- Azure MySQL
- Azure MariaDB
- Azure PostgreSQL
- Azure Cosmos DB
- Oracle
- Oracle RAC
- Oracle Database Cloud Service (DBCS)
- Oracle Exadata Database Service on OCI / on premises
- SAP HANA
- Amazon RDS
- Amazon DynamoDB
- Amazon DocumentDB
- Amazon Redshift

Active Database

- Microsoft AD
- Azure AD

Cloud Environments

- Microsoft Azure
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Block Store (EBS)
- Azure VMs
- Azure VMware Solution
- VMC
- OCI VMs

Containers

- Azure Kubernetes Service (AKS)
- Amazon Elastic Kubernetes Service (EKS)
- Oracle Container Engine for Kubernetes (OKE)
- Commvault Distributed Storage
- Any CNCF-certified Kubernetes Distribution, e.g.: RedHat OpenShift, VMware Tanzu, Rancher

Microsoft Dynamics 365

- Field Service
- Marketing
- Sales
- Customer Service

Microsoft 365

- Exchange Online
- SharePoint Online
- OneDrive
- Microsoft Teams
- Groups
- Project Online

eDiscovery

- Exchange Online
- SharePoint Online
- OneDrive
- Endpoints

Endpoints

- Linux
- MacOS
- Windows clients

- Amazon S3
- Microsoft Azure Blob
- Microsoft Azure Files

Cloud Storage

- Metallic Cloud Storage
- Microsoft Azure Storage
- Amazon S3
- HPE Cloud Volumes Backup

On-Premises Storage

- Commvault HyperScale X
- Commvault Distributed Storage
- NetApp E-Series
- Dell EMC > Isilon, DataDomain
- Pure Storage > FlashArray, Flashblade
- HPE > Primera, Nimble, 3PAR, StoreOnce Catalyst
- Hitachi > HNAS, VSP, HCP

Salesforce

- Sales Cloud
- Service Cloud
- Financial Cloud
- Health Cloud

What the Industry Is Saying About Metallic®...

SaaS Awards Finalist



IT World Awards Winner



Best of VMWorld 2020



CRN



Gold Stevie's Winner



DCIG



IT World Awards



TechTarget Infrastructure



"Cloud-based backup done right for a change..."

@TechTarget Infrastructure

Dutch IT-Channel Awards



Customers Are Living the Benefits

Across use cases and industries

Endpoints



“

It runs in the background and it's something that you install and then forget about ... For me, it works great and it does exactly what it says it does.



Benjamin Roper
Enterprise Backup & Recovery
Specialist
Parsons

Microsoft 365



“

We're more efficient in all of our backups for Microsoft 365 because it's in a single pane of glass.



Kristian Smith
Technical Services and Support
Manager
Linamar

Datacenter workloads



“

We are able to have all of our backups in the cloud now, and were even able to leverage our existing Azure storage. With Metallic, we no longer manage and maintain physical hardware which makes us financially and even technically more efficient.

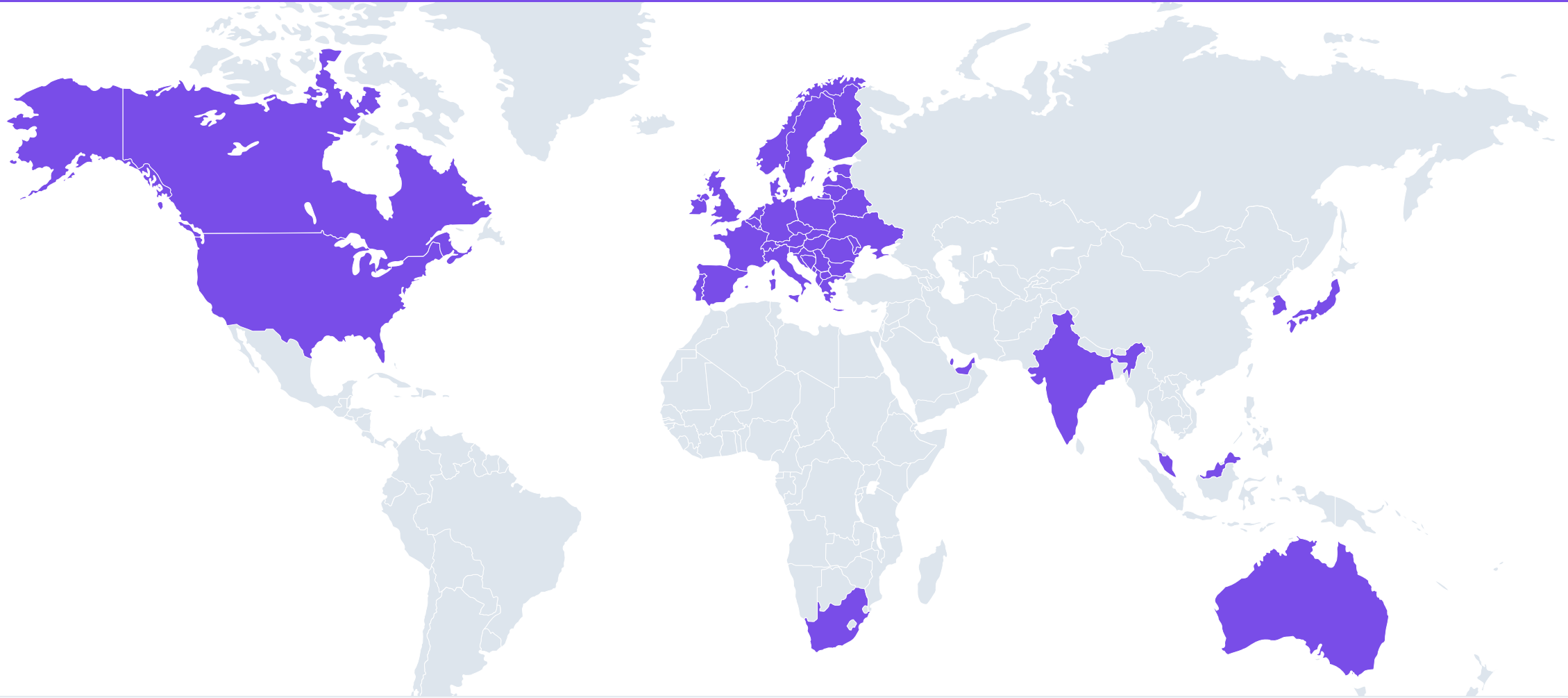


Jeff Day Smith
Systems Technical Supervisor
State of Nevada DoT

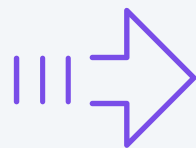
“

We originally purchased Metallic Backup for Microsoft 365 and have since expanded that deployment [...] for File & Object and VM & Kubernetes Backup. **The radical simplicity and unmatched scalability of Metallic is allowing us to completely rethink how we protect our data.**

Peter Gregorowicz, Network Services Manager, Vancouver Community College



Metallic regional
availability...

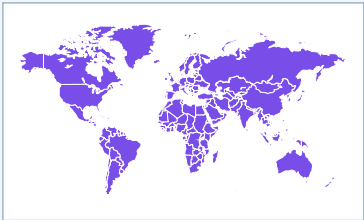


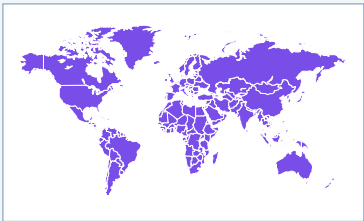
Metallic DMaaS is now available for purchase
in **over 30 countries and growing**



Azure Supported Regions

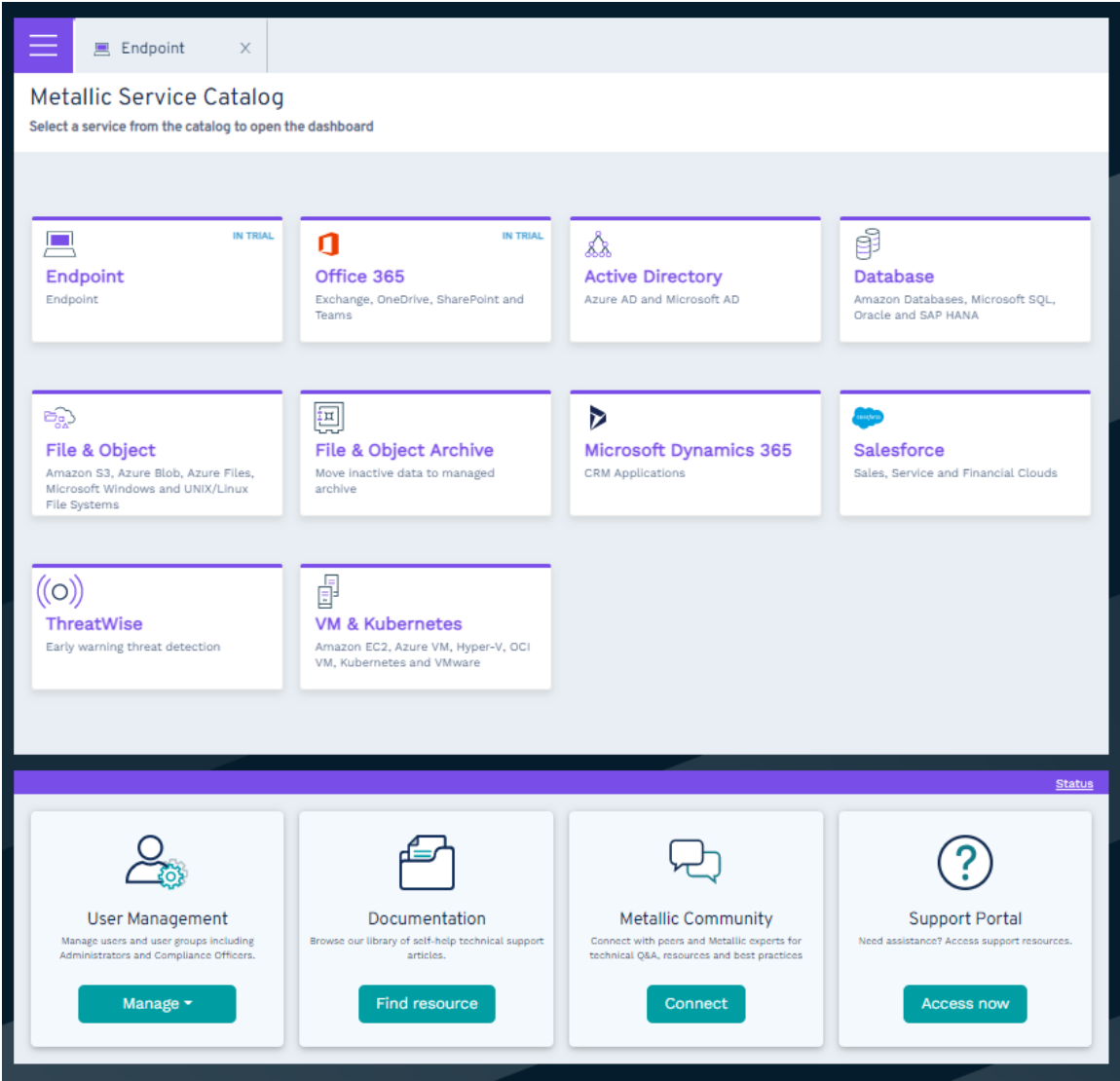
- Metallic & Recovery Reserve™ for Metallic SaaS
- Metallic Recovery Reserve™ for Metallic SaaS, & Recovery Reserve™ for Commvault Software





Metallic Hub

Designed to customers needs



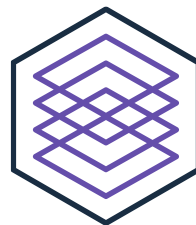
Metallic® Partnership Slides (MSFT)



Extending our joint capabilities to customers in three ways:



Metallic provides a **simple SaaS-delivered solution** for world-class data protection of on-prem, cloud-native, and SaaS workloads like Microsoft 365.



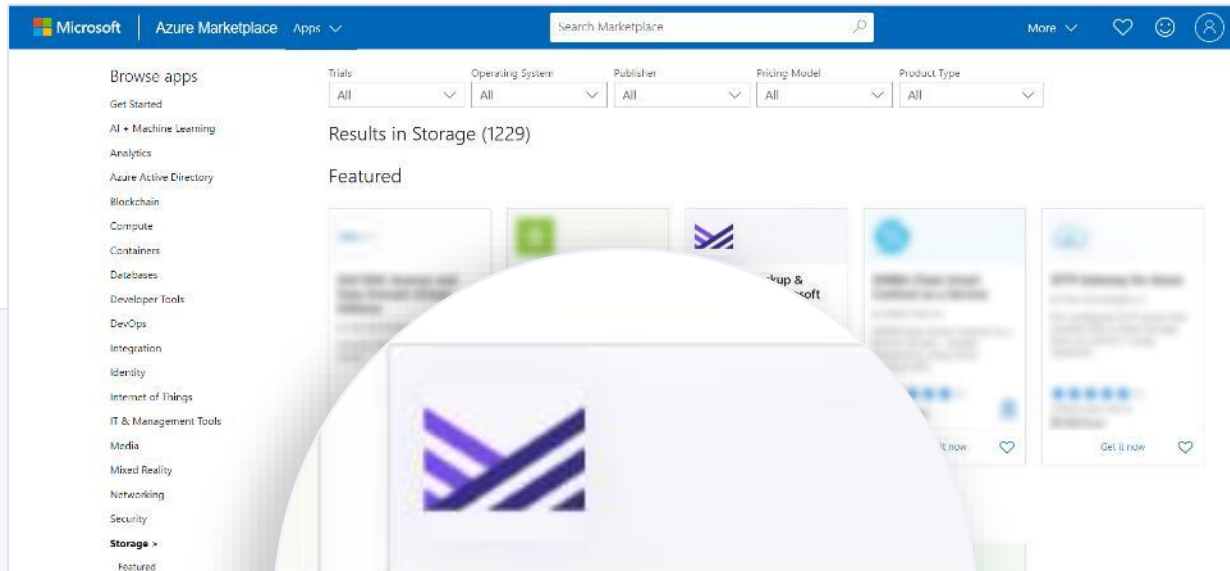
Metallic is built leveraging the best of Azure PaaS and native services for secure, **high performance and infinite scale** for companies of all sizes.



Metallic seamlessly leverages the **durability, security, and scalability** of Azure Blob Storage – for cloud data protection customers can trust.

For more information on the partnership, you can also visit: www.microsoft.com/metallic

Metallic[®] Is Featured on the Azure Marketplace!



Compatible with your existing
Microsoft Enterprise Agreements

Both Available NOW!



Metallic[®] Backup for
Microsoft 365



Metallic[®] Endpoint
Backup

Ransomware/Security Slides

Agenda



Why dedicated
ransomware protection



The importance of a
multi-layered approach
for your data



How Metallic
DMaaS helps

The Growing Sophistication of Cybercrime

Understanding the financial impact of cybercrime



A new ransomware attack will occur every **11 seconds** in 2021¹



Yet, half of cybersecurity pros believe their business is not prepared to combat a ransomware attack²



Average payout costs **\$4.44 million**³



Average downtime is **19 days**⁴



Average cost of downtime is **\$300,000/hour**⁵

Simplifying the 3-2-1 Rule

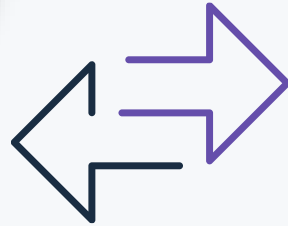
The cloud's role in data protection

3



Create three
copies of your
data

2



Keep two copies
in separate
storage media

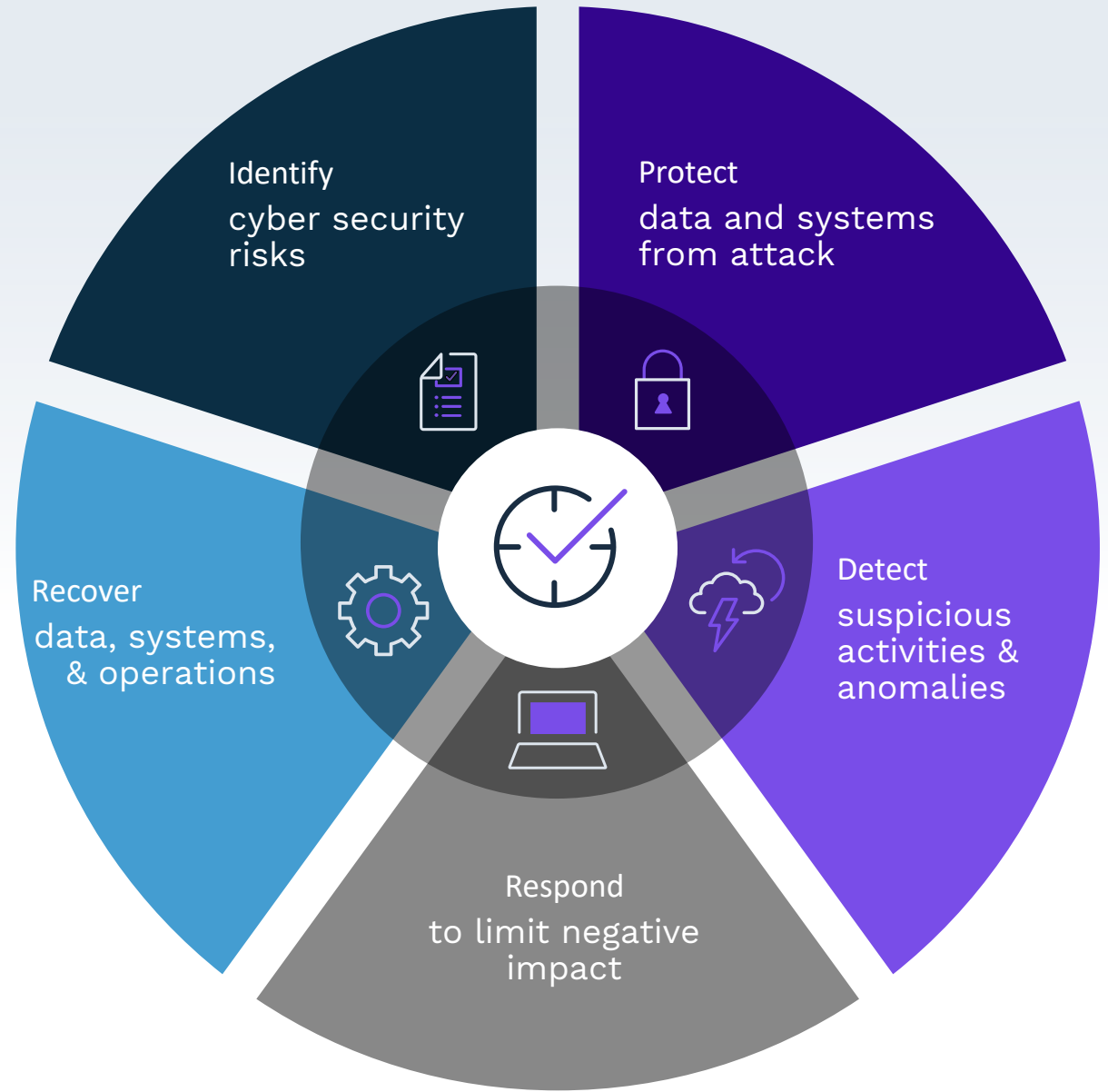
1



Store at least
one of those
copies offsite

A Ransomware Recovery Framework

A proactive strategy for your data



Three Keys for Comprehensive Ransomware Protection

A multi-layered approach to data protection



Protect

Insulate data from
successful breaches



Detect

Spot and identify
attacks



Recover

Fast and reliable
data restoration

Protect

Preserve data with virtually air-gapped services



Your Data

Immutable, separated data copies prevent tampering, altering, or deletion in the event of a breach



Your Service

Isolated service architectures ensure backup and recovery utilities are available if production environments are penetrated



Zero-trust access controls
with multi-authorization

FIPS 140-2 &
AES-256 encryption

ISO 27001, SOC 2,
& FedRAMP

Detect

Detect threats and vulnerabilities early



Advanced insights to pinpoint active and latent risks



**Monitor
unauthorized changes**

Spot unwanted configuration, restore, login, and user behaviors



**Detect
anomalies**

Uncover at-risk data set and unusual access patterns as they happen



**Track abnormal
conditions**

Surfaces real-time insights into suspicious changes, events, and data-types

Recover

Recover fast and eliminate downtime



Guidance

Intuitive recommendations on pre-ransomware recovery points



Speed

Optimized services for less redundancies and a higher availability of backup data



Precision

Granular search and flexible recovery options to restore data to the right place, at the right time

Our Multi-Layered Security Approach

A new and differentiated approach to Data Protection

YOUR DATA

On Premises Workloads



Physical Virtual Converged

Cloud Workloads



Endpoints



SaaS Applications



Threat Sensors &
Ransomware
Alerts

Data encryption
in-flight/at-rest

Isolated
virtual
air gap

Separate
security domain

Security IQ Insights -

- Anomaly detection
- Trends & monitoring
- User behaviors

**Metallic
Control Plane**

Built-on

Microsoft Azure

Multi-factor Authentication
Zero-trust access controls

Immutable
data backups



Security IQ Dashboard

Advanced security tools and insights



Outcomes

Evaluate and continuously improve backup security stature



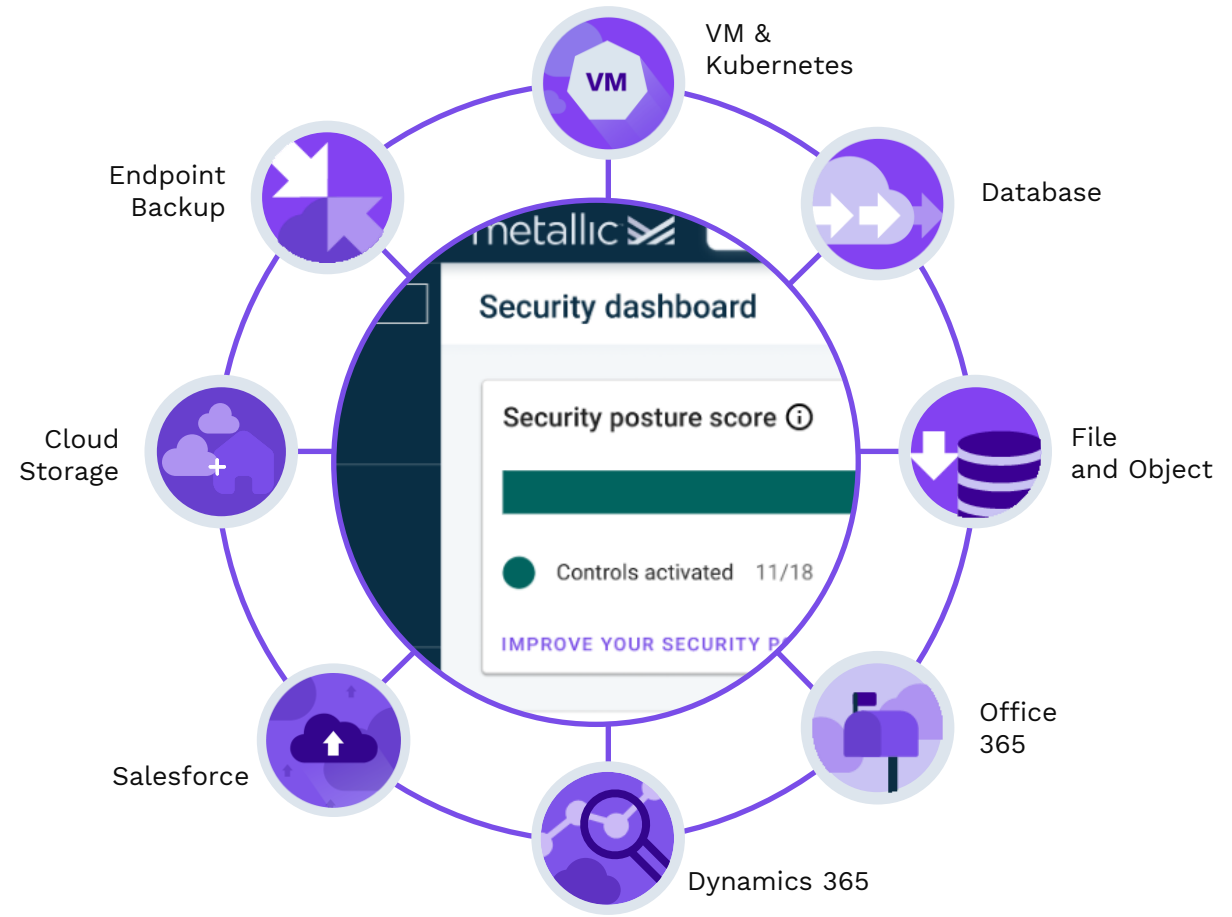
Insights

Gain real-time visibility into critical events, anomalous activities, and vulnerabilities

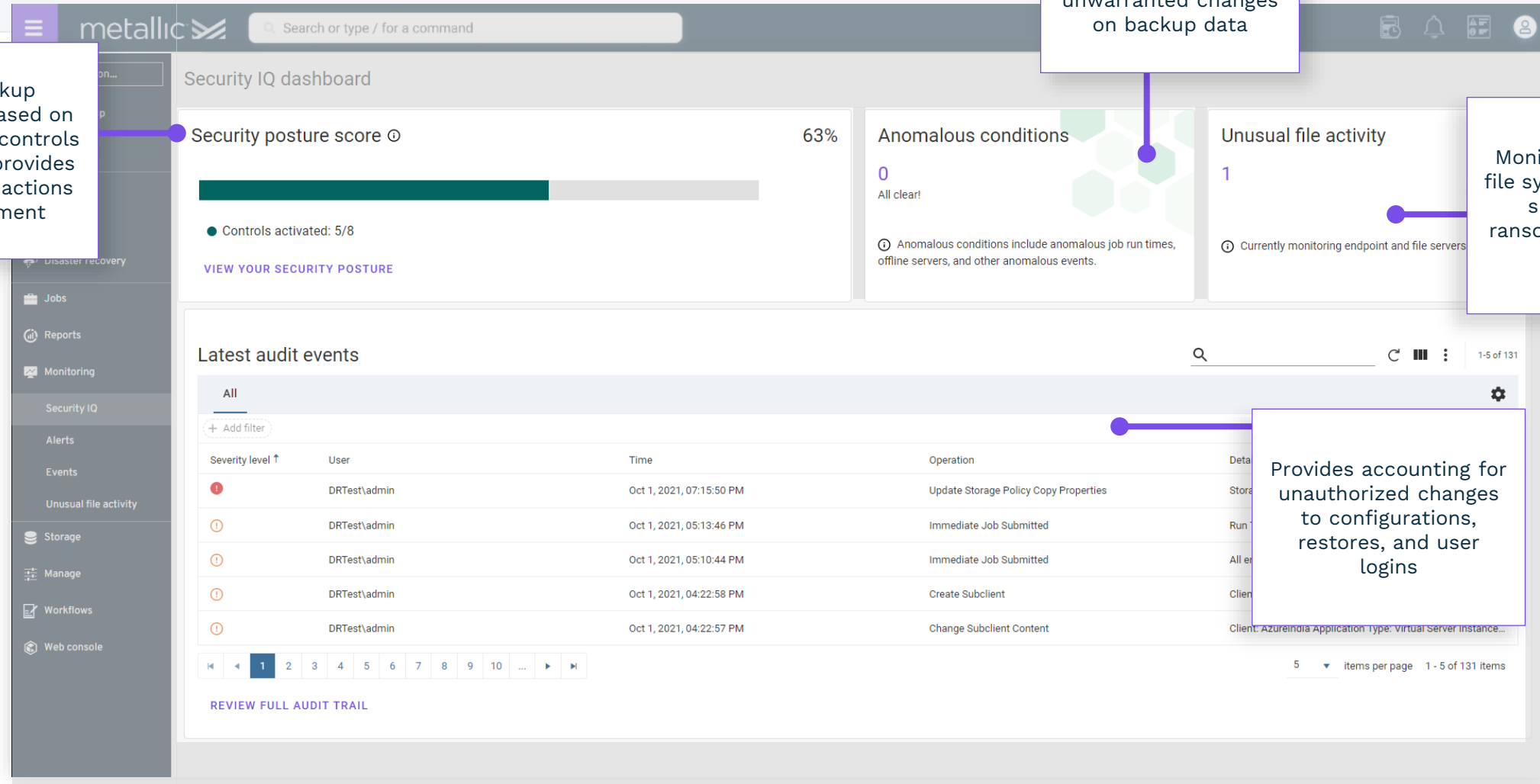


Recovery Points

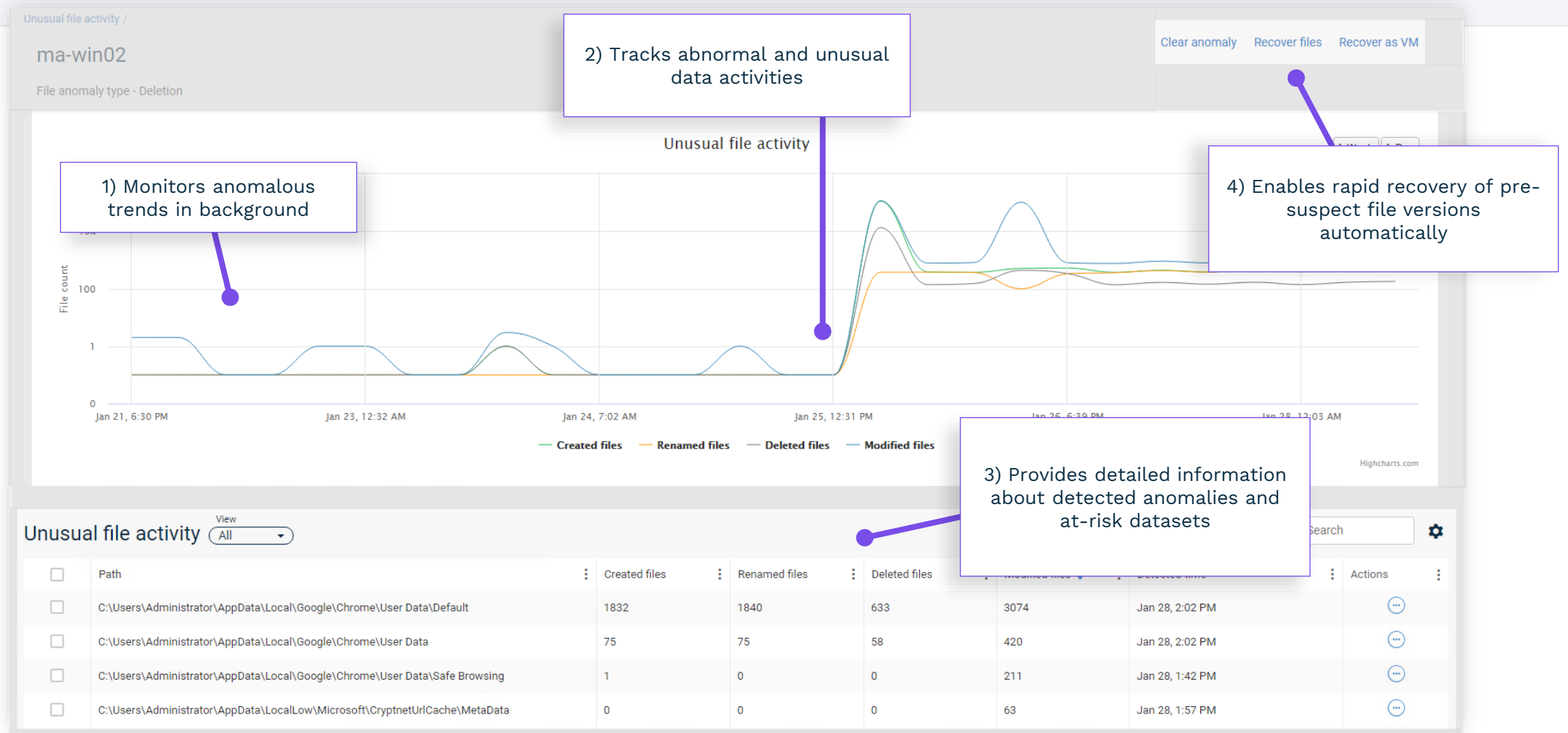
Make informed recovery decisions to exceed SLA objectives



Security IQ



Intelligent Ransomware Recovery





Security Stories

Metallic Security IQ Dashboard surfaces information on security controls, data anomalies, and security audit information within the Metallic environment, bringing awareness to unusual events, suspicious behaviors, and potential threats which could impact data and backups.

The following are five practical examples of how Security IQ helps businesses identify risks, improve their security posture, and recover fast.



Security Posture

Customer Scenario

Company XYZ recently implemented a new MFA provider and did not proactively update their Metallic environment to reflect this change.

How Security IQ Helps

Secure Posture Score: Metallic intuitively detected this change and provided the user with recommended actions to configure their new MFA. Metallic also surfaced other native controls (such as key management, storage encryption, & more) which were disabled, but could be configured to further bolster their security stature within their backup environments.





Malicious Insiders

Customer Scenario

Company XYZ terminated a former contractor but failed to revoke system access. The former contractor used their active credentials to re-enter their environment and attempt to delete sensitive data in mass.

How Security IQ Helps

Multi-authorization: Metallic multi-authorization prevented this deletion, as all deletion and restore attempts require additional authorization (from another administrator) to execute. This helps prevent both accidental and destructive tasks. As a result, the rogue user was not able to execute this action, and the organization was made aware of the attempt.

Audit Trails: Metallic audit trails captures all user actions within the environment, including logins, configuration changes, backup, and restore attempts. This provided Company XYZ with clear line of sight into the former contractor's activities and malicious attempts.





External Attack

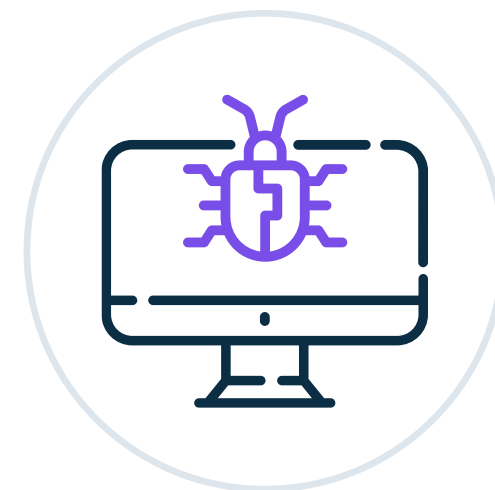
Customer Scenario

A zero-day threat had successfully penetrated Company XYZ's environment, without them knowing. The bad actor began embedded itself across systems to preparing to encrypt Company XYZ's data.

How Security IQ Helps

Anomalous Condition: Metallic identified offline servers, elevated resource loads, and slower than usual backups caused by data change, flagging this for Company XYZ. As a result, they were able to proactively cut-off infected systems and begin sanitization efforts – avoiding a successful ransomware payout.

Unusual File Activity (file systems & endpoints): Built-in anomaly detection was triggered, providing Company XYZ with visibility into an unusual number of files being created, changed, and renamed. Company XYZ was able to monitor these patterns and quickly execute an automated pre-anomalous recovery, rolling back data to a pre-suspect state.





Threat Response

Customer Scenario

Customer XYZ's security team has identified malicious applications within their environment, and fear that these malicious applications were also backed up.

How Security IQ Helps

Unusual File Activity (file systems & endpoints): With file anomaly detection, Metallic provides great insight into data changes, and allow pre-anomalous recoveries of data. Data can also be recovered out of place for forensic or investigative purposes of infected systems and datasets.

Data Sanitization: Metallic helps locate threat applications within backup content and quarantine the malicious applications in backups. This allows organizations to isolate datasets, to safely recover data without reinfection. You can also choose to restore the quarantined items out of place for forensic purposes.





Security Audit

Customer Scenario

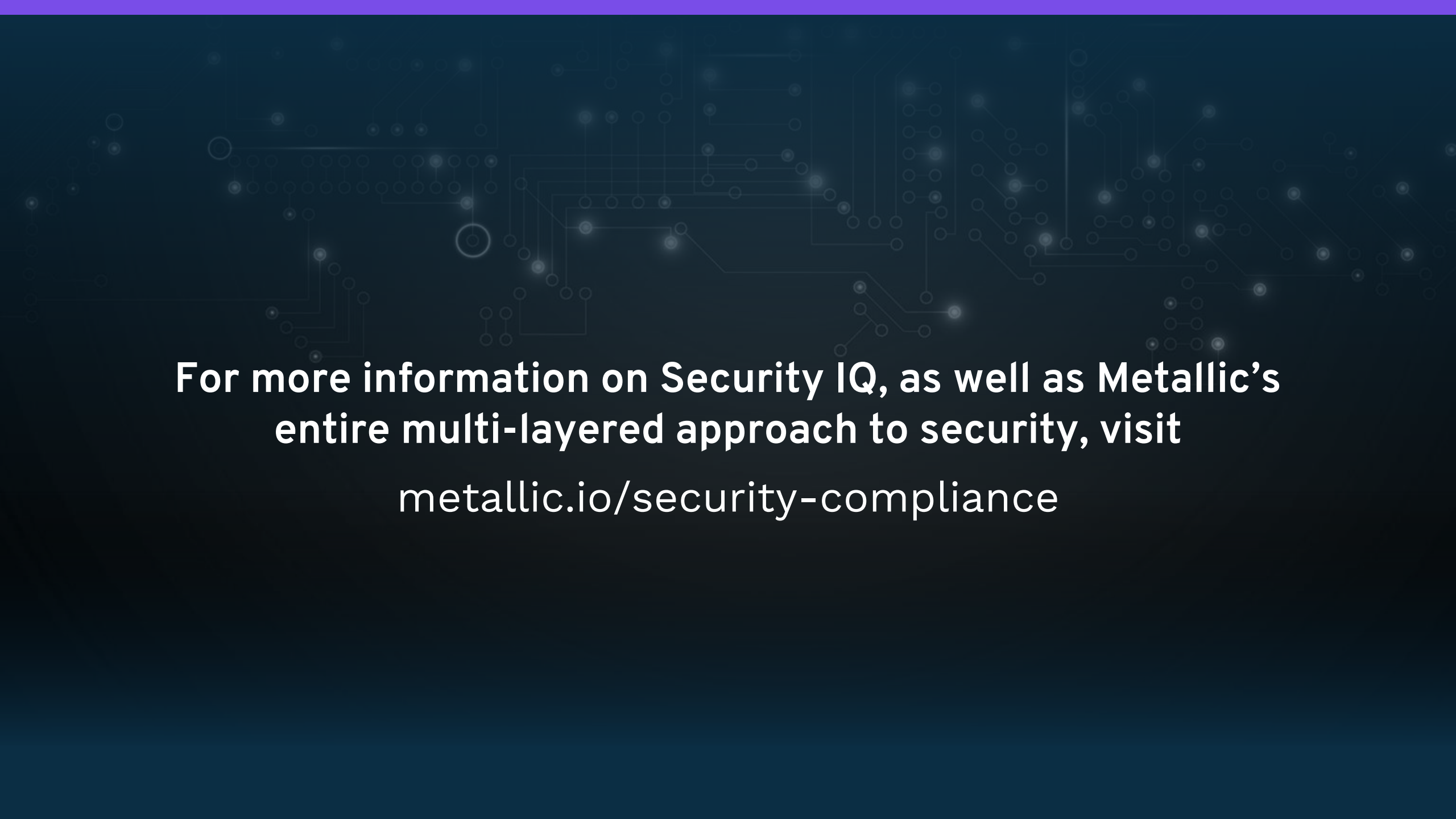
Customer XYZ is required to provide detailed information to Security Auditors pertaining to what security controls are applied protecting Metallic backups, such as MFA, Dual Auth, and Encryption.

How Security IQ Helps

Security Posture Score: With Metallic, you can easily gauge security levels and quickly enable missing parameters to bolster security posture of your environment. Users can also view a comprehensive list of leveraged security controls, and export details for offline access and review.

Audit Trail: With easily exportable audit trails, Metallic enables users to send information via email, on schedule, or with the use of APIs for offline preservation into another monitoring system.



An abstract background image featuring a dark blue gradient. Overlaid on this is a faint, glowing circuit board pattern. The pattern consists of numerous small, light-blue circular nodes connected by thin, white lines, creating a complex network that resembles a printed circuit board or a data flow diagram. The nodes and lines are more prominent in the upper half of the image and fade slightly towards the bottom.

**For more information on Security IQ, as well as Metallic's
entire multi-layered approach to security, visit
metallic.io/security-compliance**

ThreatWise™

Strengthening customer security with Metallic

Innovative data security services in the cloud



Isolation is needed for additional ransomware protection



Active Directory plays a role in 90% of attacks



Government agencies & contractors require more stringent protection



Data protection and recovery is a critical part of end-to-end security



Admins and IT pros need smarter data security and recovery insights



Data protection starts, before you're compromised...

Metallic Recovery Reserve

air gapped, scalable cloud storage target

Active Directory

FREE Azure & Microsoft AD Backup

Metallic Government Cloud

the ONLY FedRAMP High DMaaS portfolio

First MSSP Partner

inclusion in first Managed Security Service offering with new partner

Security IQ

advanced insights and security tools

Metallic ThreatWise

market-leading cyber deception technology

Lines Between Data Protection & Security are blurring

As ransomware surges, new data protection imperatives emerge

What keeps IT up at night?

88%

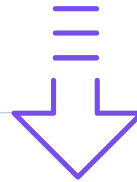
Preventing
data damage

86%

Avoiding
data loss

72%

Recovering
post attack¹



Yet only 12% have ransomware detection tools that are adequate and equally secure on-prem and cloud environments²

Lines Between Data Protection & Security have blurred

As ransomware surges, new data protection imperatives emerge

What keeps IT up at night?

88%

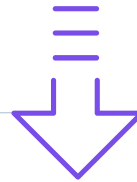
Preventing
data damage

86%

Avoiding
data loss

72%

Recovering
post attack¹

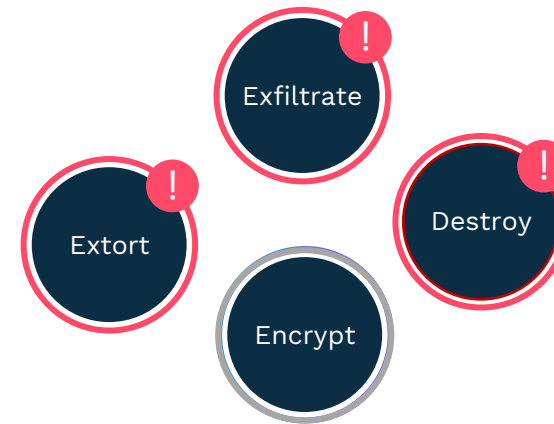


Yet only 12% have ransomware detection tools that are adequate and equally secure on-prem and cloud environments²

Confronting New Wave of Cyber Threats

Double and Triple Extortion Tactics

- ! Ransomware featuring, **exfiltration, extortion, or damage** has increased **83%.**²



Introducing Metallic® ThreatWise™

Industry Leading DMaaS meets Cyber Deception

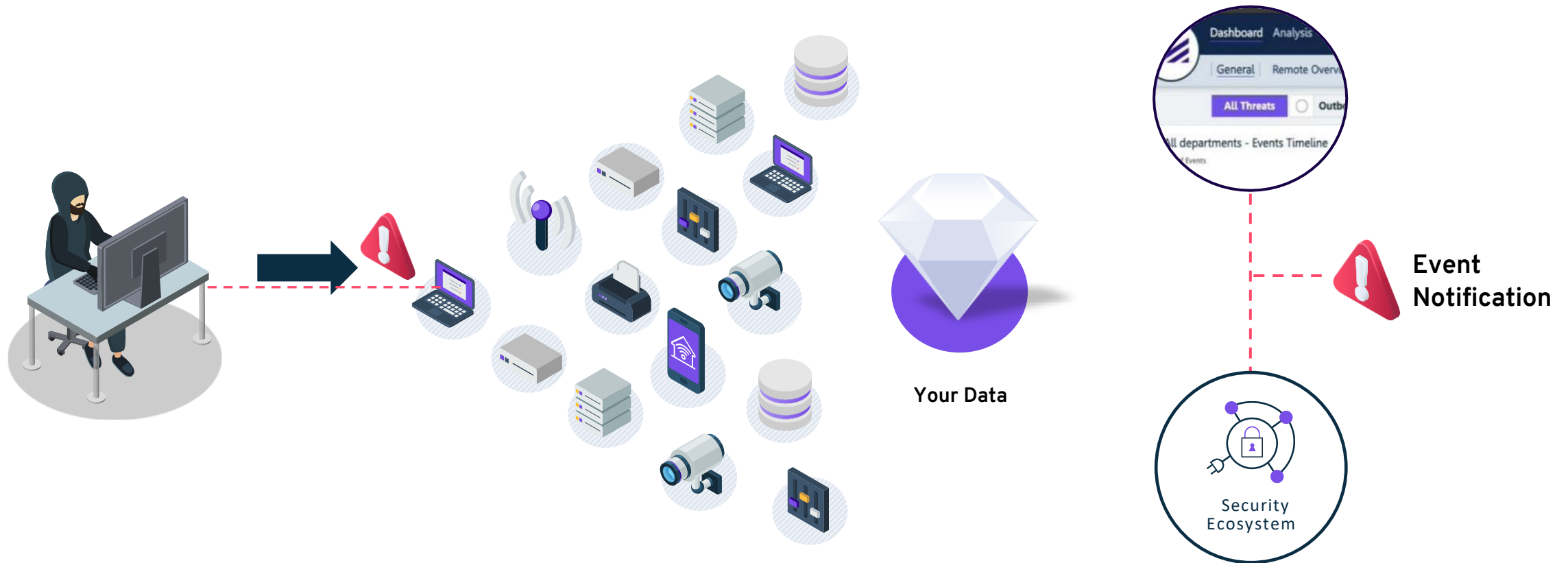
Data Protection starts
before your data is
compromised.



Metallic®
ThreatWise™

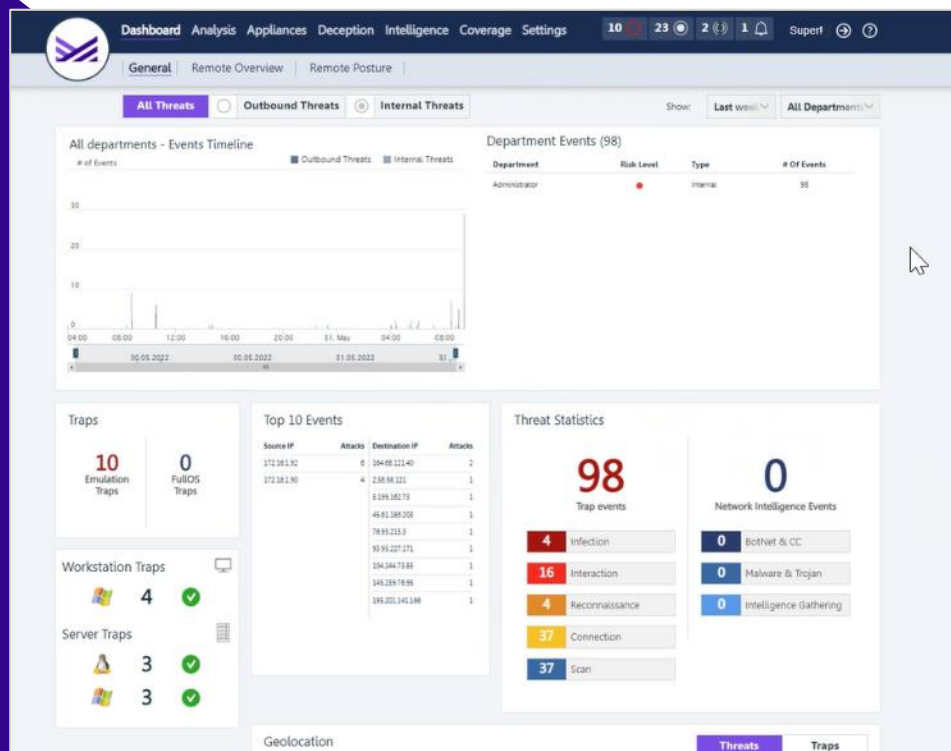
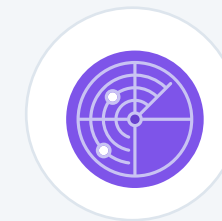
- ✓ Mimic real assets
- ✓ Trick bad actors
- ✓ Expose threats early
- ✓ Contain attacks before impact

Lightweight, Highly-Accurate Threat Signals



Metallic® ThreatWise™

Integrated Cyber Deception



Early Warning Ransomware Detection



Intelligent decoys that mimic and behave-like legitimate assets



Precise alerts to pinpoint threats without false-positives or alert-fatigue



Rapid scalability to protect entire environments and applications in seconds



Simple SaaS delivery with flexible, lightweight architecture

Data protection starts *before* you're compromised.

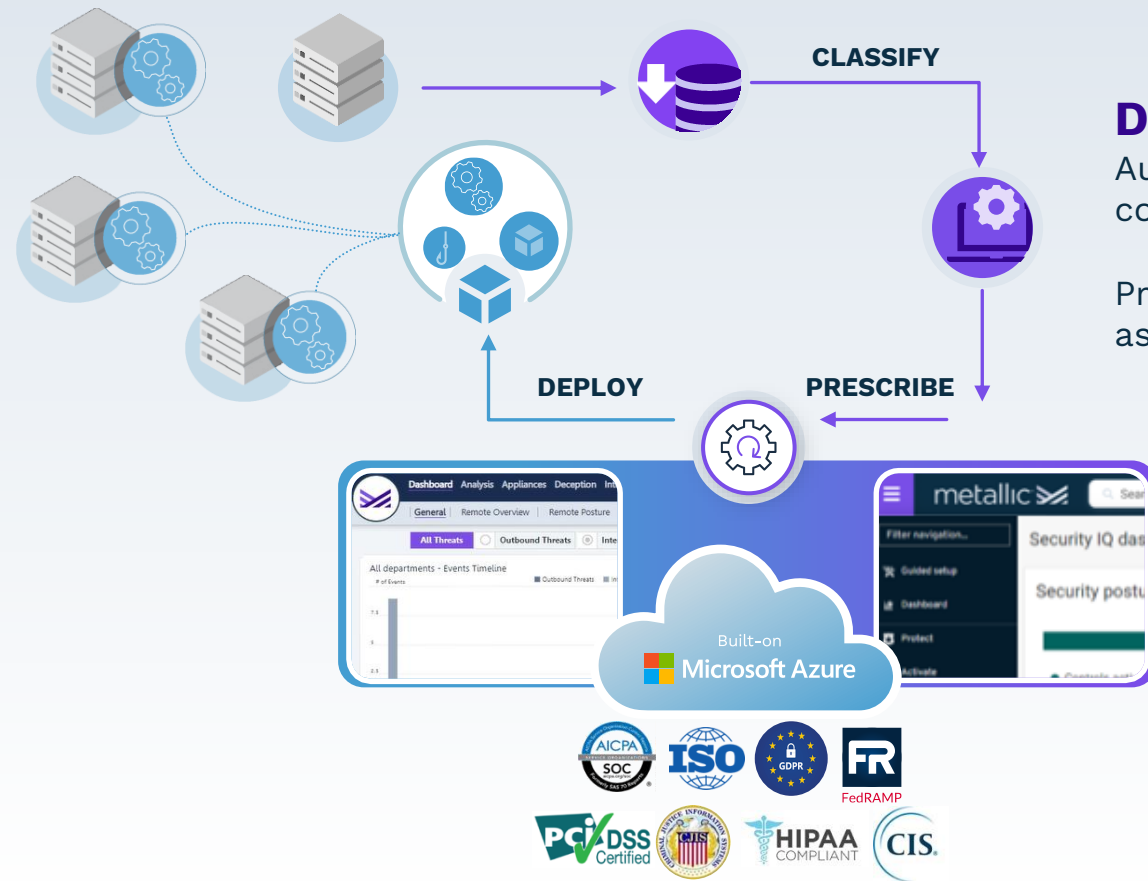
Data Centric Advantage

Vision for upcoming Releases

Alerting Benefits

Attacks on sensors are related to real assets and their data value

Alerts trigger both SIEM incidents and backup and recover playbooks



Deployment Benefits

Automation for easy configuration

Prescribed density based on asset value

The Need for Modern Cyber Deception

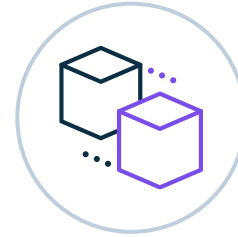
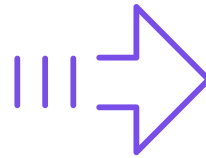
Evolution of next-generation deception



Conventional Honeypot Technology

Full system decoys designed to learn from bad actors and their techniques

- Tedious to set up and manage
- Consumes IT resources (licenses, compute, etc..)
- Difficult to deploy and scale
- Limited in their deceptive capabilities



Modern Cyber Deception

Asset emulation designed to actively engage bad actors for early warning

- Easily configurable
- Lightweight and passive architecture
- Rapidly scalable, designed for surface area coverage
- Can mimic virtually any resource

Metallic® SaaS Solutions

Data Protection as a Service (DPaaS) for your entire data estate

Hybrid Cloud Protection

Storage + Archive optional



Metallic® VM & Kubernetes Backup*

For VMware, Hyper-V, VMC, Azure VM, AWS, Oracle Container Engine for Kubernetes (OKE), Amazon EC2, OCI VM



Metallic® Database Backup*

For Microsoft SQL Server, Azure SQL Server, Azure MySQL, Azure MariaDB, Azure PostgreSQL, Azure Cosmos DB, Oracle, Oracle RAC, Oracle Database Cloud Service (DBCS), Oracle ExaData Database Service on OCI / on premises, SAP HANA, Amazon RDS, Amazon DynamoDB, Amazon DocumentDB, Amazon Redshift



Metallic® File & Object Backup*

For Windows Server, Linux/UNIX, Azure Blob & Files, OCI Object Storage, Amazon S3

Secure Cloud Storage



Metallic® Recovery Reserve™*

For air-gapped, long and short-term retention



Metallic® File & Object Archive

For cost efficiency and compliance of unstructured data

Archive & Compliance

SaaS App Protection

Storage included



Metallic® Backup for Microsoft 365^{†*}

For Exchange, Teams, SharePoint, OneDrive, Project



Metallic® Backup for Microsoft Dynamics 365*

For CE applications



Metallic® Salesforce Backup*

For production and sandbox environments

Endpoint Protection

Storage included



Metallic® Endpoint Backup^{†*}

For laptops and desktops

Threat Detection + Response



Metallic® ThreatWise™

For early warning into threats



Security IQ*

FREE WITH ANY SUBSCRIPTION
For actionable threat insights

Active Directory Protection



Metallic® Active Directory Backup

FREE WITH ANY SUBSCRIPTION
For Azure & Microsoft AD

[†] eDiscovery available

^{*} Metallic Government Cloud available
(FedRAMP High, hosted on Azure Government)

FROM INDUSTRY-LEADER

COMMVAULT 

Our Multi-Layered Security Approach

A new and differentiated approach to Data Protection

YOUR DATA

On Premises Workloads



Physical Virtual Converged

Cloud Workloads



Endpoints



SaaS Applications



Threat Sensors &
Ransomware
Alerts

Data encryption
in-flight/at-rest

Isolated
virtual
air gap

Separate
security domain

Security IQ Insights -

- Anomaly detection
- Trends & monitoring
- User behaviors

**Metallic
Control Plane**

Built-on
Microsoft Azure

Multi-factor Authentication
Zero-trust access controls

Immutable
data backups





With built-in zero-trust security protocols, Metallic meets the most stringent confidentiality, integrity, and availability standards for government agencies and business, alike

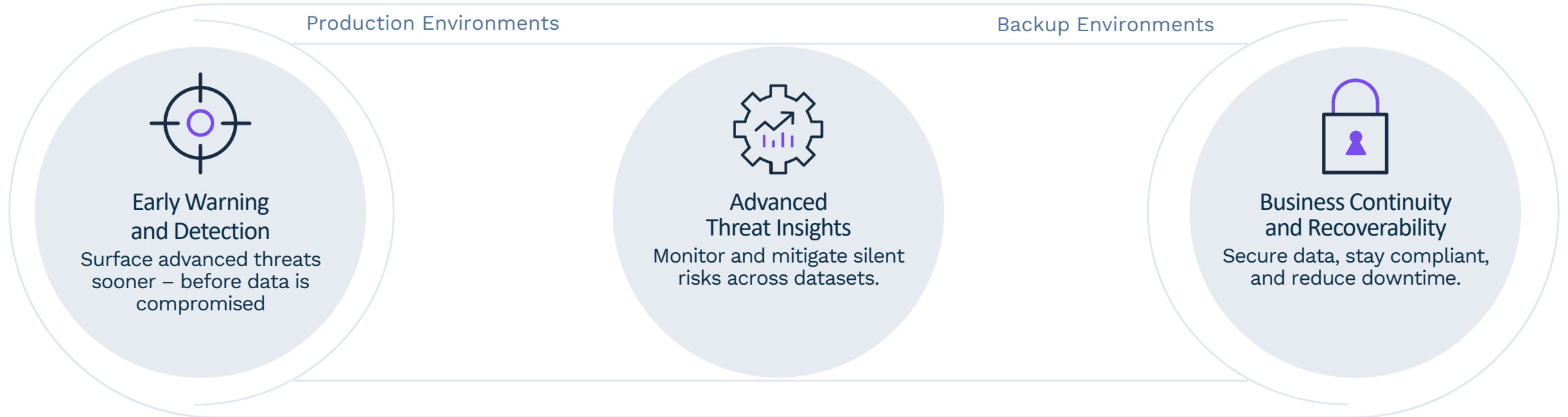


- **Customer Environment:**
Advanced cyber deception for early warning into ransomware and malicious intent.
- **Security DPR:**
Foundational detection, protection, and response services across the entire Metallic surface – from the Edge to the Data.
- **Zero-Trust Authentication:**
Stringent user authentication protocols built on FIPS 140-2 framework.
- **Zero-Trust Authorization and Access:**
Hardened controls with privileged identity management to prevent unwarranted access.
- **Virtual Air-gap:**
Cloud-based architecture, isolated and separate from source environments via security domains.
- **Immutability:**
Robust, multi-layered controls for tamper and deletion prevention.
- **Deception & Detection:**
Intelligent monitoring and risk identification to deceive and flag threats early in the attack life-cycle.



Bridging the Gap: Extending DATA Protection Beyond Backup

End-to-End Protection from Metallic



Metallic® ThreatWise™

Cyber Deception & Active Defense

Spot ransomware threats before data impact.

- Identification of zero day & unknown threats
- Rapid discovery, recon, & lateral movement detection
- Patented baiting, decoy, and threat sensor technology
- High-fidelity notification system

Security IQ

Actionable Threat Insights

Deep insights into suspicious data and behaviors.

- Security posture validation
- Anomalous and unusual file monitoring
- Pre-ransomware recovery suggestions
- Dataset isolation and reinfection prevention
- Commvault honey-pots

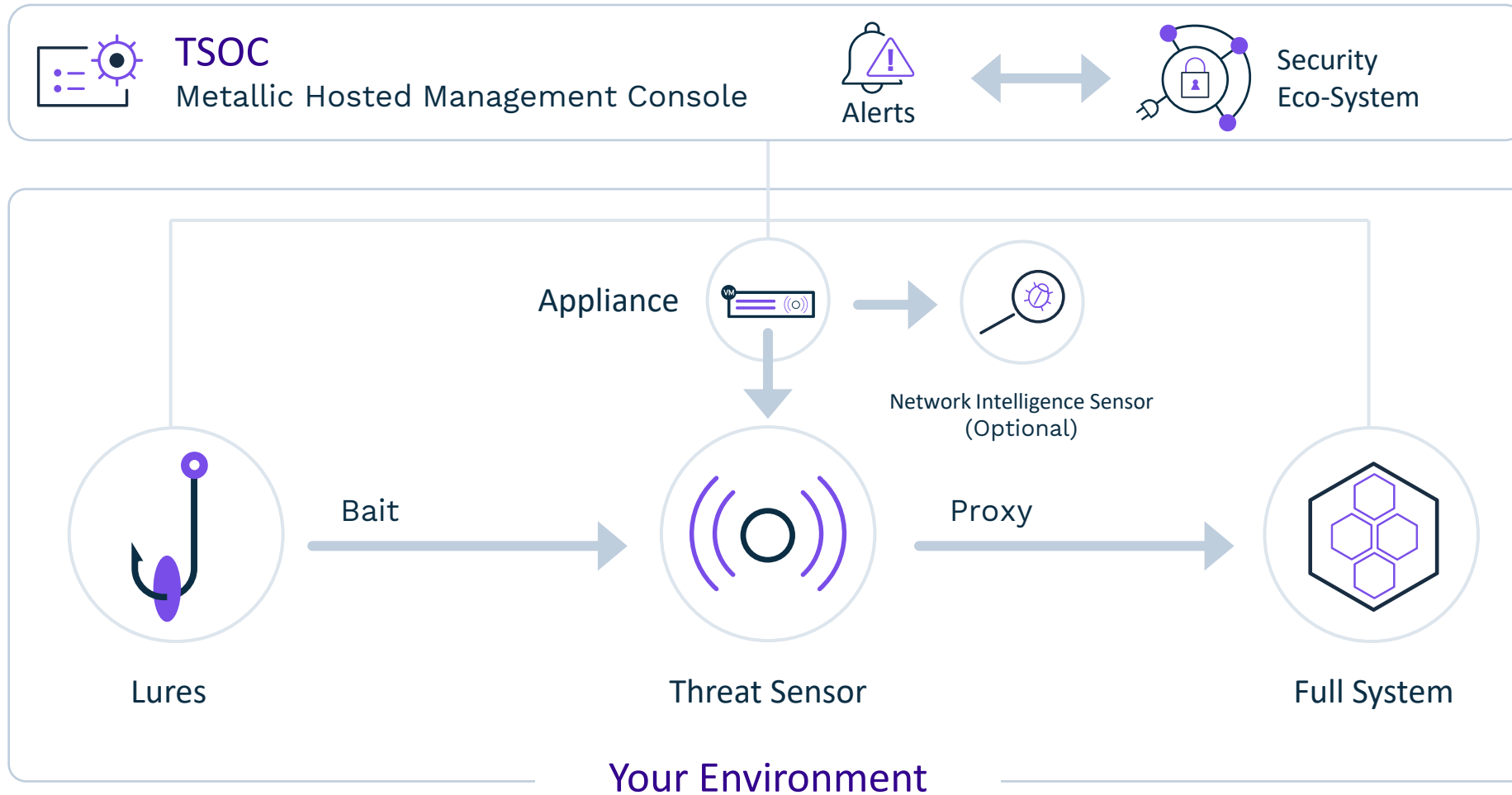
Metallic® Backup

Data Backup & Recovery

Proven and reliable recoverability.

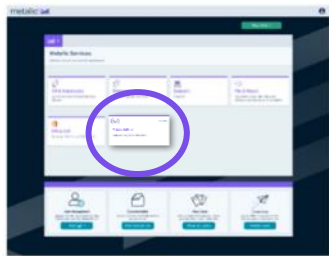
- Virtually air-gapped architecture
- Post-attack, rapid recovery controls
- Hardened-security controls baked-in
- eDiscovery & SLA compliance

High Level Architecture

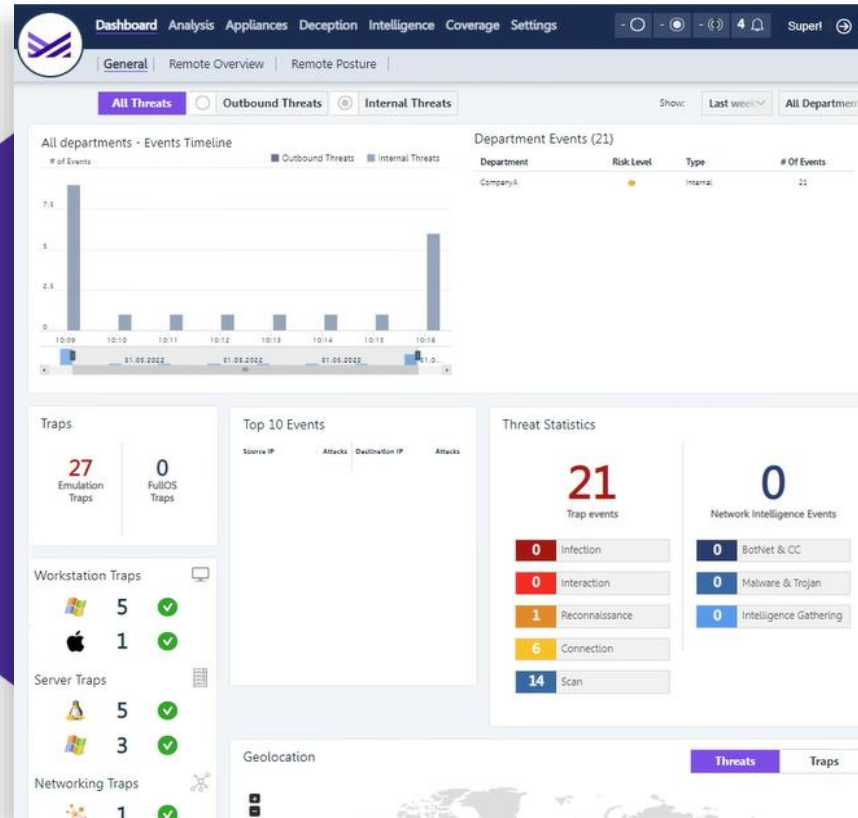


TSOC

ThreatWise™ Security Operations Console




Metallic®
Control Plane



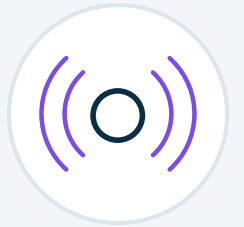
Manage ThreatWise™
appliances, deploy threat
sensors and view events

Point of Integration
to Security Eco-System
such as SIEM, Firewall,
NAC and Sandboxes

Accessed via Metallic
Hub/Control Plane

Threat Sensors

Infrastructure Components



Medium interaction decoys
that replicate network assets

- Quick deployment via Wizard
- Easy scalable via Mass Deployment
- Seamlessly customizable and blend-in
- Up to 512 sensors per appliance



Databases



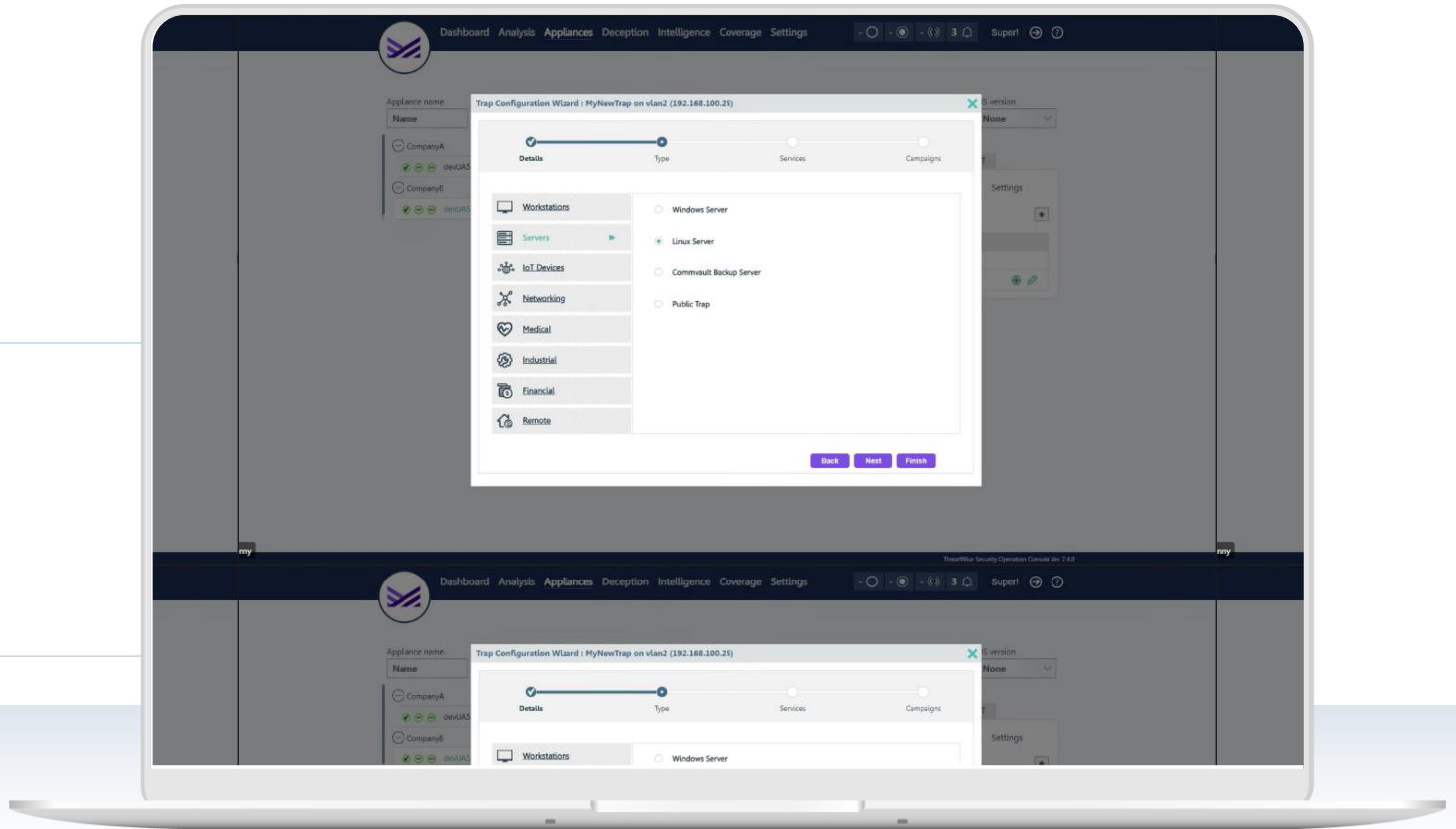
Servers



VMs

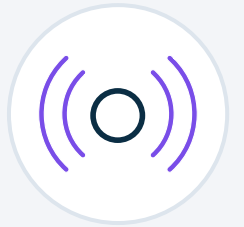


and much
more



Threat Sensor Deployment








Out of the box



Threat Sensor

Replicated Network Assets

- ✓ Highly scalable due to mass and bulk deployment
- ✓ Seamless blend in due to configurable services
- ✓ Deployed in Seconds

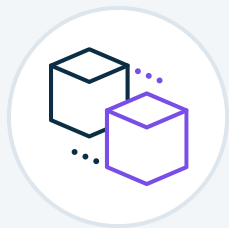
Category		Used Cases	
 Workstation		• Windows, Linux or Mac Endpoints	
 Servers		• Databases • Backup Servers	• Virtual Machines
 IoT Devices		• Printer • Security Cameras	• Point of Sale • Smart Lights
 Networking		• Switches (incl. PBX)	• VPN
 Medical		• MRI • CT	• PACS Systems
 Industrial		• SAP • PLC	• SCADA
 Financial		• SWIFT	• ATM

Indistinguishable Threat Sensor

To blend-in each Sensor type has various ways to enhance the configuration

**Replicate a
Backup Server**

Threat Sensor
Type:
Windows
Server 2019

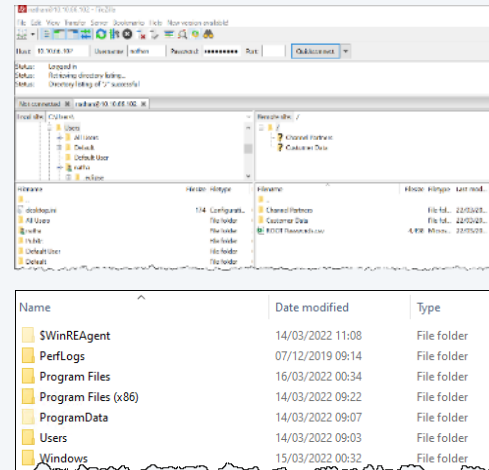


Deploy

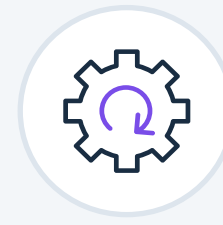
Enhance the interface
upload html/css files



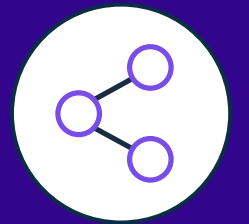
Individualize Sensor Template



Fake SMB & FTP enabled
content are uploaded to
a (default) "Data" folder



Deceive



re-use
templates in
multiple
deployments

Where Deception Helps

Last mile defense for ransomware attacks

Protection and
countermeasures against active
and successful attacks

SIEM – Better with Deception



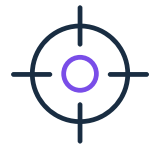
- Insight where SIEM can't reach
- Detects stealth techniques
- Reduces meantime to response

Vulnerability Management – Better with Deception



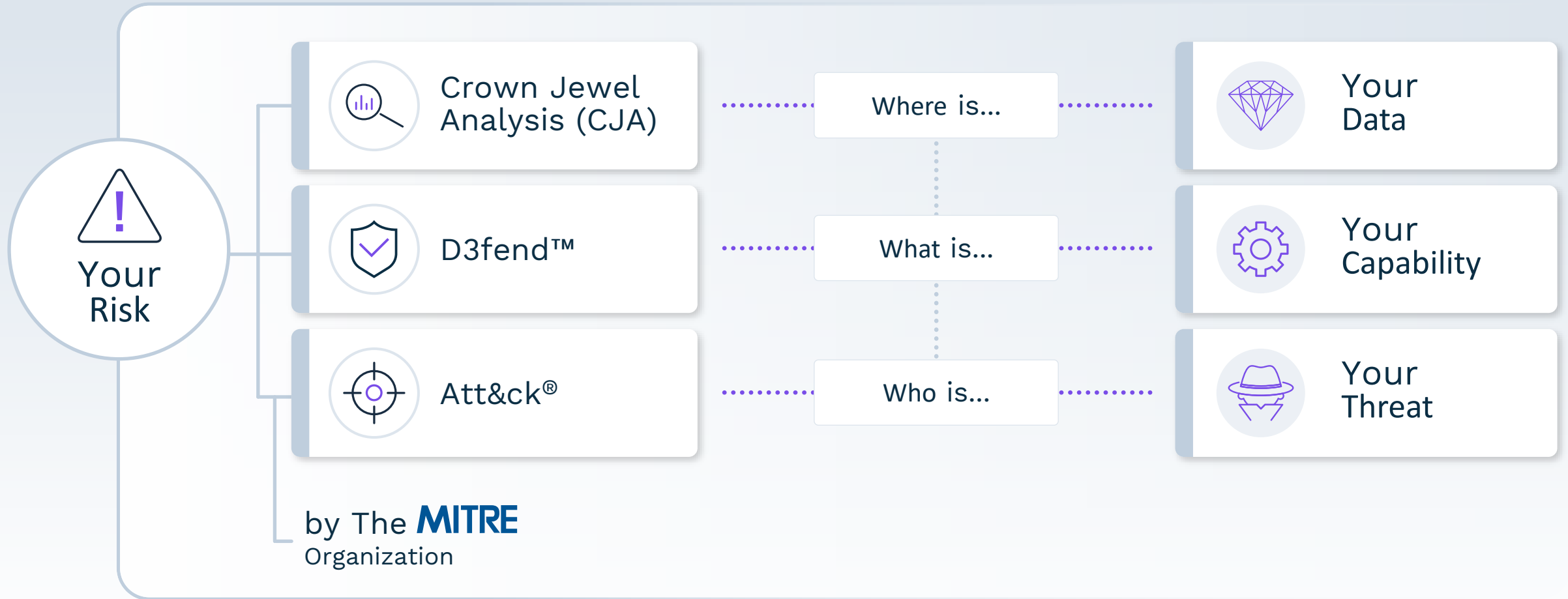
- Directs attacks away from vulnerable assets
- Reduces risk during the patch cycle
- Guards against Zero-day exploits

Perfect with Pen Testing

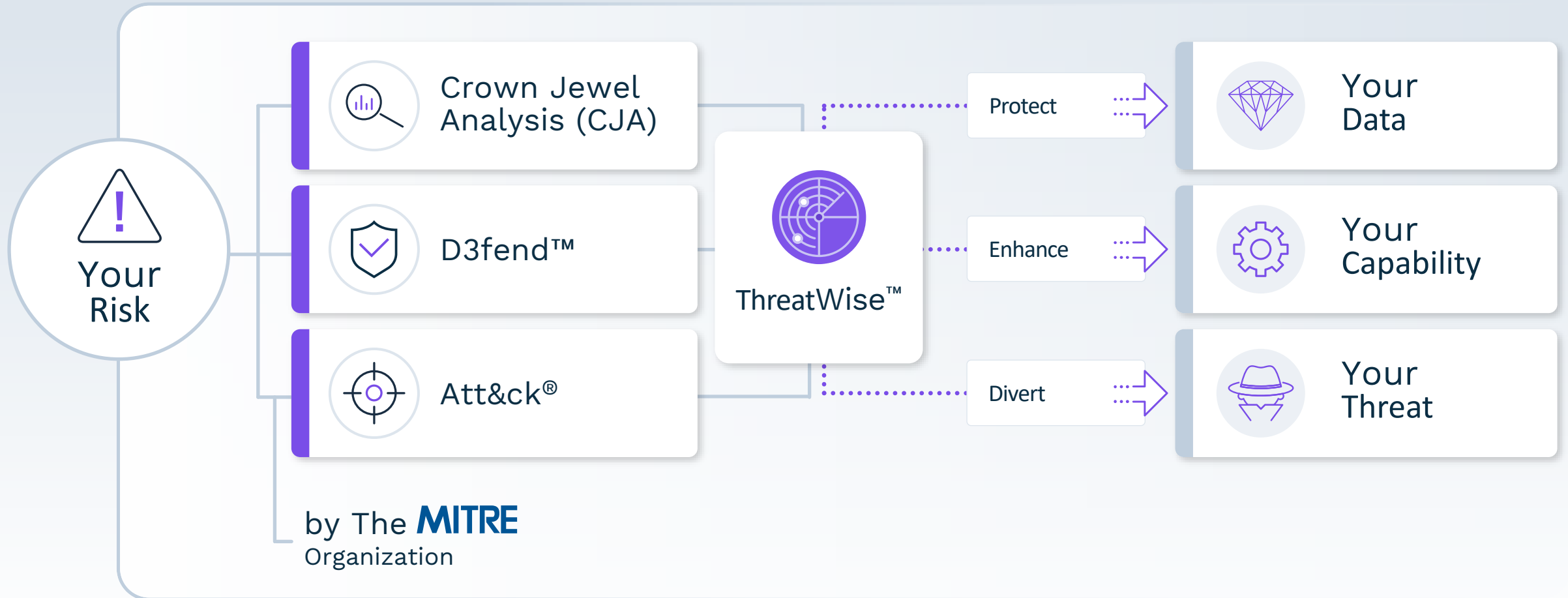


- Informs Sensor distribution
- Demonstrates value

Data Protection



Data Protection by



Closing Slides



Q & A

Try Metallic[®] for yourself
Get a free trial today at
metallic.io/trial/

Take Metallic for a test drive!

Technology is changing faster than ever.
Choose data protection that's up in minutes, agile for years.

Check us out at Metallic.io

Start your free trial today!

metallic® 
A Commvault Venture

Thank You!



Copyright 2023 Commvault Systems, Inc. All rights reserved. Metallic, Metallic and the “M Wave” logo, and the “M Wave” logo are the trademarks or registered trademarks of Commvault Systems, Inc. All third party brands, product names, service names, trademarks or registered trademarks are the property of and used to identify the products or services of their respective owners.

Appendix