
DELL Technologies
TITANIUM PARTNER
Hacker gegen Helden – Ein Tanz auf dem Daten-Drahtseil der Cyber-Sicherheit
Der Kampf um Ihre Cyber-Sicherheit hat bereits begonnen. Bleiben Sie unerpressbar!
GLOBAL INFORMATION DISTRIBUTION
MEDIALINE
MEDIALINE GROUP

Ihre Referenten

Michael Lischewski

Sr. Director Sales Germany
Dell Technologies

Mail: Michael.Lischewski@dell.com
Mobil: +49 170 6311217

Friedrich Förster

Geschäftsführer | CEO
Global Information Distribution GmbH (GID)

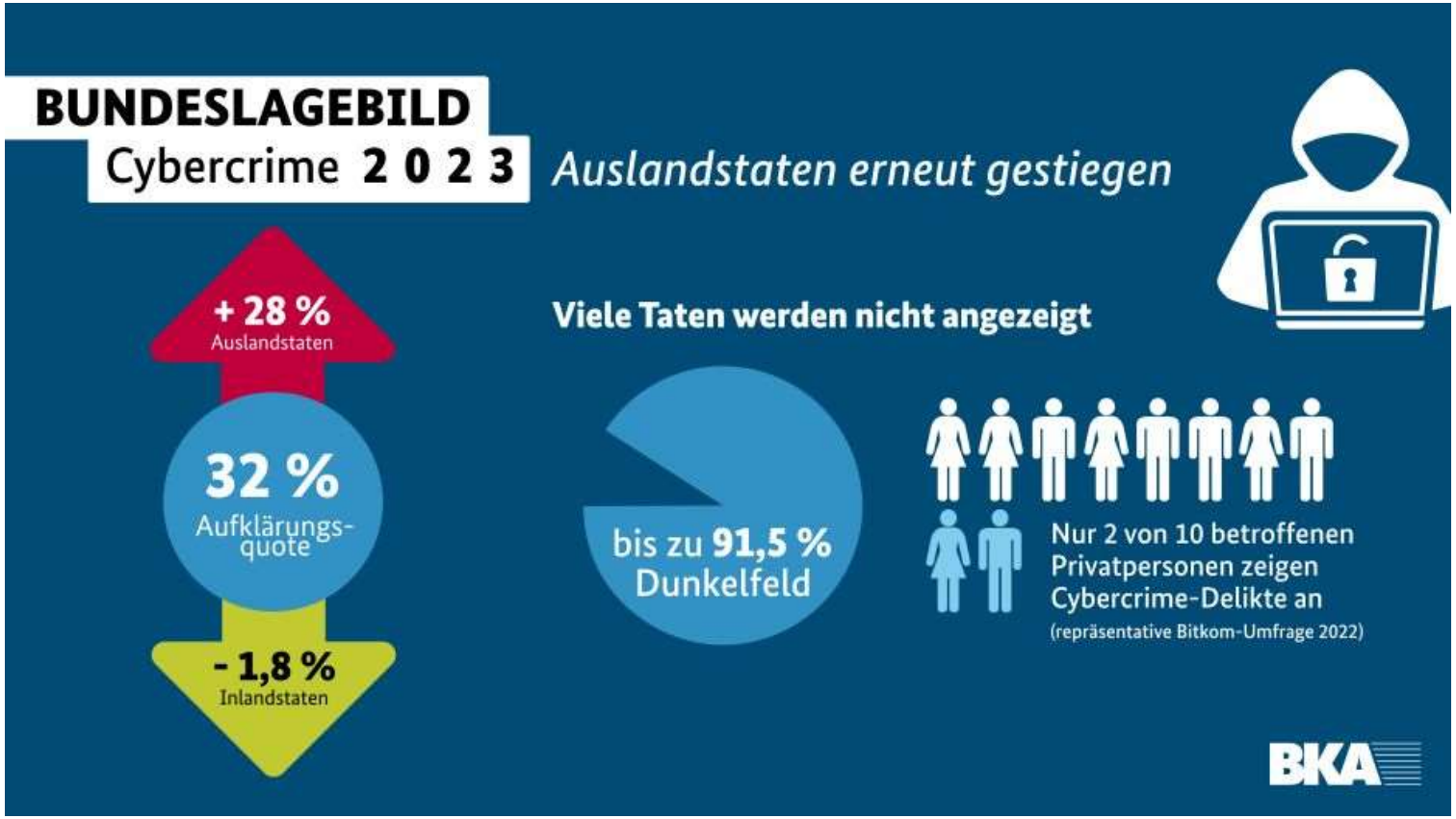
Mail: Friedrich.Foerster@gid-it.de
Mobil: +49 151 422288-12

DELL Technologies
TITANIUM PARTNER

GLOBAL INFORMATION DISTRIBUTION

Bundeslagebild Cybercrime 2023 des BKA

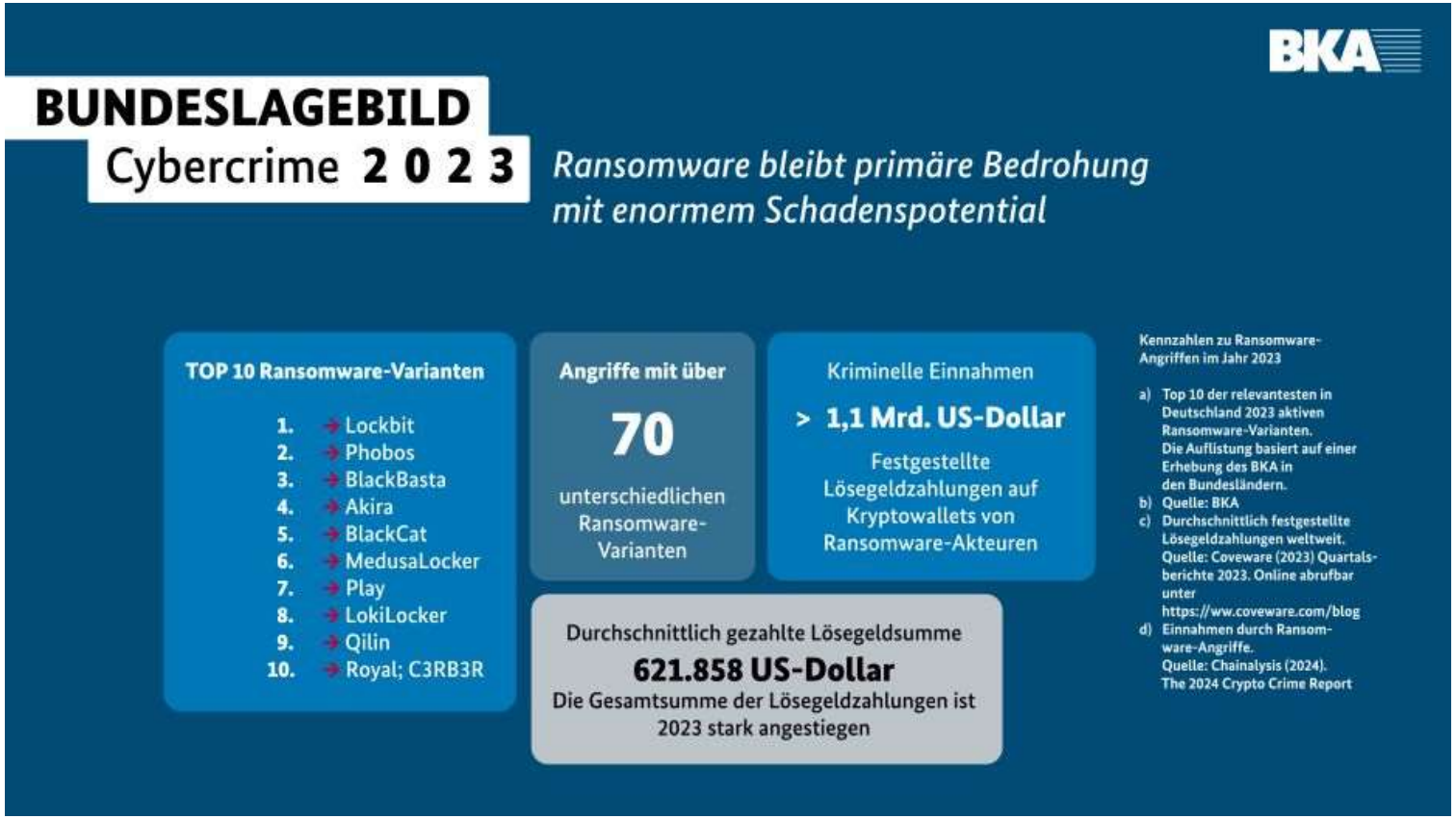
Auslandstaten sind erneut gestiegen



Quelle: Bundeskriminalamt, Bundeslagebild Cybercrime 2023, 13. Mai 2024

Bundeslagebild Cybercrime 2023 des BKA

Ransomware bleibt primäre Bedrohung



Quelle: Bundeskriminalamt, Bundeslagebild Cybercrime 2023, 13. Mai 2024

Bundeslagebild Cybercrime 2023 des BKA

DDoS-Angriffe als Mittel der Wahl

Quelle: Bundeskriminalamt, Bundeslagebild Cybercrime 2023, 13. Mai 2024

Die Frage ist nicht OB,
sondern WANN!

Ablauf einer Cyber-Attacke

Die Nachricht

>>>>> Your data is stolen and encrypted.BLOG Tor Browser

>>>>> What guarantee is there that we won't cheat you? We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's Twitter https://twitter.com/hashtag/lockbit?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.

>>>>> Warning! Do not delete or modify encrypted files, it will lead to problems with decryption of files!

>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

Ablauf einer Cyber-Attacke

Erlebnisbericht: Tag des Angriffs

08:57 Uhr	Anruf Kunde: Kompletter Ausfall der IT- dringende Bitte um Hilfe
09:00 Uhr	• Erste Sichtung durch GID-Consultant, Feststellung dass die Hardware läuft, aber alle virtuellen Maschinen aus sind • Weitere Recherchen auf dem Cluster ergeben, dass ein Starten der VMs nicht möglich ist (vmdk [= virtuelle Festplatte] nicht gefunden) und auch im Filesystem die vmdks, anstatt als <Maschinenname>.vmdk als <Maschinenname>.vmdk.CE7bB8e8 abgelegt sind • Ersteinschätzung GID-Consultant: Der Kunde ist verschlüsselt worden
09:10 Uhr	• Die Taskforce bestehend aus GID Consulting, Presales und Sales stellt dem Kunden die Notfallnummer von Dell für Incident Response & Recovery (IRR) zur Verfügung und sorgt dafür, dass die vom Kunden eingesetzten PowerProtect Data Domain Systeme unmittelbar vom Netz genommen werden
10:00 Uhr	• Eintreffen des GID-Teams am Standort des Kunden in Köln • Aufnahme erster Eindrücke und Maßnahmenkoordinierung • Sicherung von Logfiles von Firewalls, Switches, VMware und Änderung der Passwörter für die Infrastruktur sowie Abschaltung des Internetzugangs
12:00 Uhr	• VMs sind alle verschlüsselt, inkl. des vCenters, die ESXen laufen alle, die sonstige Infrastruktur scheint zunächst nicht kontaminiert zu sein • Die Firewalls (Fortinet – Fremddienstleister) hatten in dem eingesetzten Release eine Sicherheitslücke im Bereich VPN – worüber der Angreifer mutmaßlich hereingekommen ist
17:00 Uhr	• Kriminalpolizei ist vor Ort • Im Filesystem wird die Readme mit dem Erpresserschreiben gefunden • Die Bootplatte vom ESX wird durch die Kripo gesichert • GID geht davon aus, dass die Angreifer den Weg über die VPN-Sicherheitslücke in der Firewall ausgenutzt haben und die Domain-Kennwörter entwendeten • Da auch das vCenter mit Domain-Accounts verbunden war, gehen wir davon aus, dass die Angreifer diesen Weg genommen haben, weil es wesentlich einfacher und schneller ist, als die ESXen anzufassen

GLOBAL INFORMATION DISTRIBUTION

Ablauf einer Cyber-Attacke

Erlebnisbericht: Tage nach dem Angriff

Tag +1	Der Plan für die nächsten Tage ist wie folgt: • Der Dienstleister für die Firewall wird diese neu aufsetzen, um dieser wieder vertrauen zu können. • Alle Zugänge nach außen werden sehr restriktiv gehalten und nur freigegebene Webseiten werden verfügbar sein • Das geschieht, um der potenziell vorhandenen Angreifer-Software keine Chance zu geben, über irgendwelche Kanäle sich bei den Angreifern bemerkbar zu machen • Es laufen bei GID vorbereitende Maßnahmen zur Bereitstellung von Leihsystemen, um den separaten, parallelen Aufbau eines neuen, unbelasteten Systems für den Notbetrieb und als Restore-Ziel zu gewährleisten
Tag +2	• Das Dell Instant Response und Recovery (IRR) Team in Deutschland wird hinzugezogen, um die Möglichkeiten der Datenwiederherstellung für die Stakeholder beim Kunden u.a. IT und Geschäftsführung vorzustellen und einen Scoping Call durchzuführen • Empfehlung an den Kunden: parallelen Neuaufbau des Systems, um mögliche Spuren nicht zu verwischen bzw. die forensische Wiederherstellung von Daten nicht zu gefährden
Tag +3	• Eine erste PowerStore 1200-T wird als Ersatzmaschine angeliefert • Der Kunde beschafft die von GID vorgeschlagenen Komponenten zur Primär- und Sekundärspeicherinfrastruktur
Tag +7	• Der Kunde entscheidet sich, die Erpresser nicht zu bezahlen und stattdessen das Angebot der Dell IRR zur Wiederherstellung der VMs aus Data Domain und VxRail Systemen anzunehmen
Tag +8	• Rund 30% der VMs sind bereits am Vormittag durch Dell IRR recovered, am selben Abend sind es über 80% recovered, darunter der extrem wichtige Fileserver mit einer Größe von rund 1,5 TB. Die wichtigsten wiederhergestellten VMs werden auf die durch GID temporär bereitgestellte PowerStore kopiert.
Tag +10 bis +14	• Anlieferung erste Komponenten der neuen Infrastruktur • Bereitstellung eines weiteren Leihsystems vom Typ PowerScale Isilon F900 zur Auslagerung von wiederhergestellten Daten

GLOBAL INFORMATION DISTRIBUTION

Cyber-Angriff – was sind die Folgen?

Verlust-Ermittlung

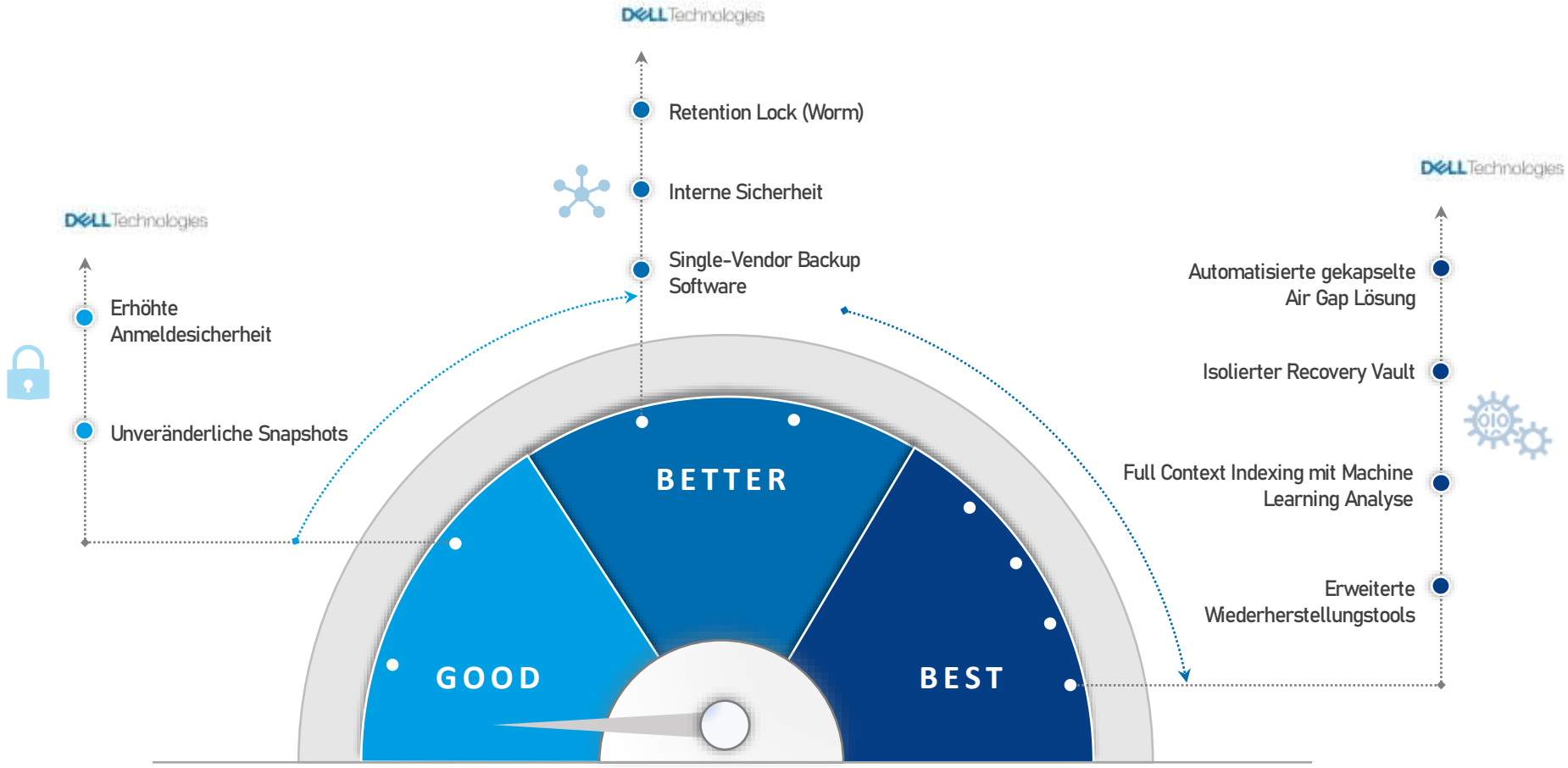
24 Tage ohne Produktion

x

Kosten pro Tag ohne Produktion

Cyber Crime: Moving the Needle

Technische Fähigkeiten von Cyber Vault und wettbewerbsfähige Marktunterscheidungsmerkmale



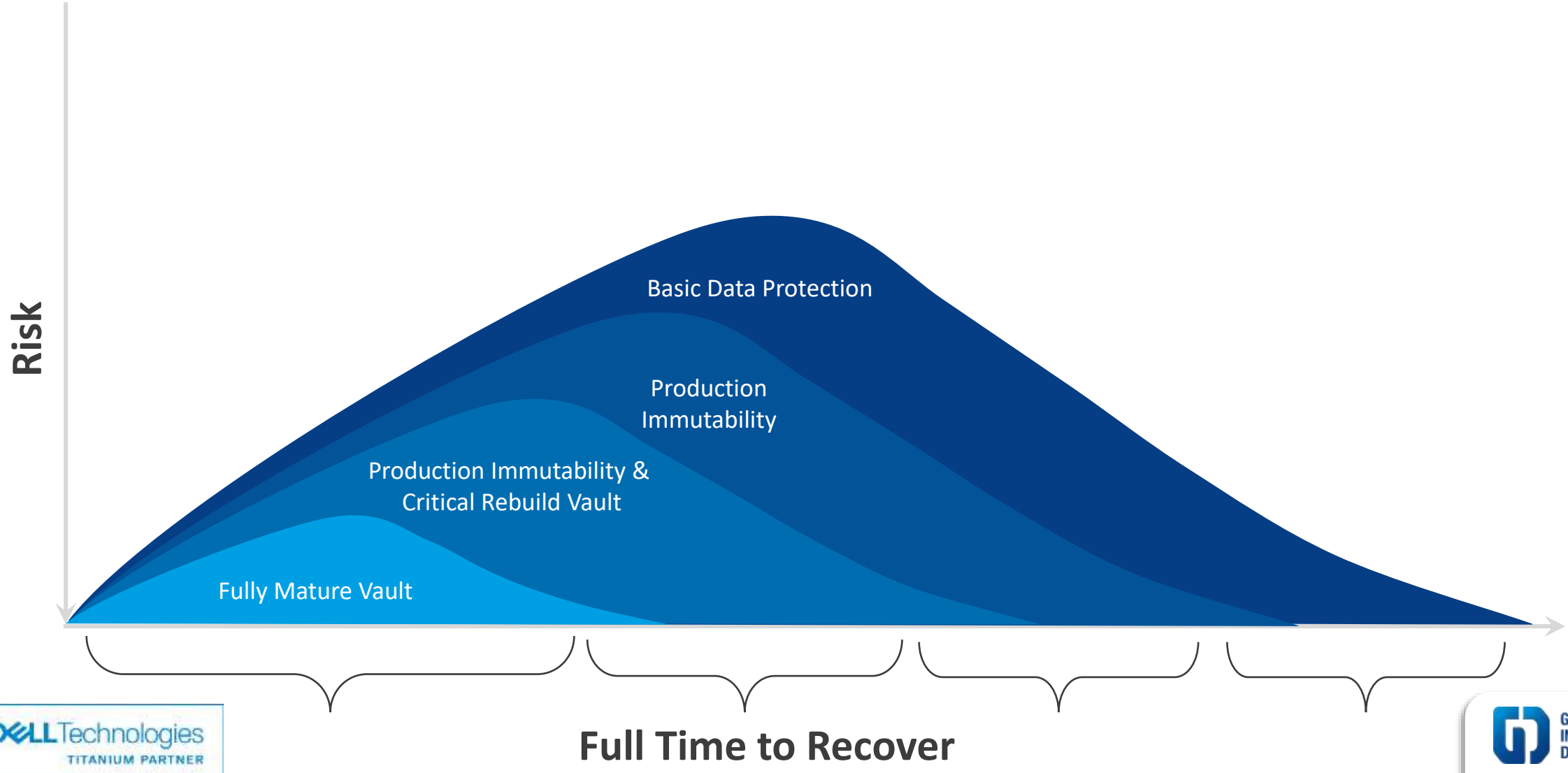
Dell Technologies Cyber Recovery ist die einzige Datenschutzlösung, die alle beschriebenen technischen Funktionen bietet.

» Kein anderes Technologieunternehmen bietet eine vollständige Architektur für Cyber-Resilienz-Lösungen.

GLOBAL INFORMATION DISTRIBUTION

Mehr Resilienz - bessere Ergebnisse

Risiken reduzieren, Wiederherstellung beschleunigen und Kosten senken



DELL Technologies TITANIUM PARTNER

GLOBAL INFORMATION DISTRIBUTION

DELL Technologies

MEDIALINE

GLOBAL INFORMATION DISTRIBUTION

MEDIALINE GROUP

BLEIBEN SIE UNERPRESSBAR!

Wir zeigen Ihnen, wie das gelingt.

Halle 6 | Stand 138

DELL Technologies
TITANIUM PARTNER

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf Ihre Fragen.

Global Information Distribution GmbH

info@gid-it.de
www.gid-it.de

Brügelmannstraße 5
50679 Köln
Tel: 0221 – 837 902 0
Fax: 0221 – 837 902 30

www.group.medialine.com

MEDIALINE GROUP