BULLWALL

RANSOMWARE SCHUTZ
FÜR KRITISCHE IT INFRASTRUKTUREN

Infosec Community Builder

20. Mai 2025

BULLWALL

EFFEKTIVE VERTEIDIGUNGSLINIE GEGEN RANSOMWARE

Ransomware Containment – RC

Stoppt die Encryption von Daten + Schutz IT Infrastruktur

Server Intrusion Protection – SIP

Stoppt unerlaubte Serverzugriffe – verhindert Exfiltration

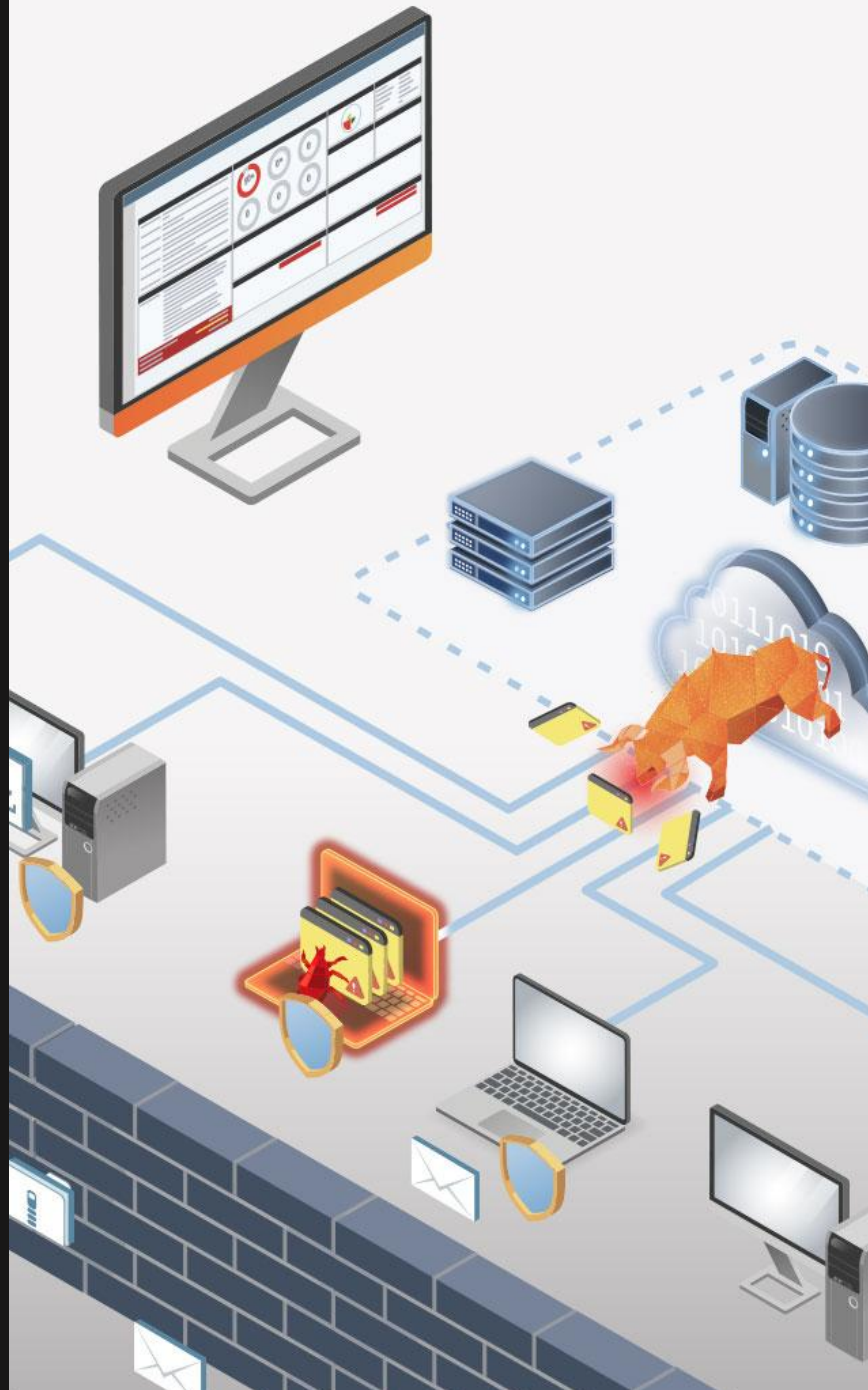
Virtual Server Protection für VMware - VSP

Schützt gezielt vSPHERE ESXi PLATTFORM vor Encryption

24x7x365 automatisierte Eindämmung gegen Ransomware
Reagiert &. handelt in **Millisekunden**
Stoppt Zero Day Exploits garantiert
– On-Prem oder Cloud Betrieb

Keine Endpoint Installation
Agentless Lösung
Einfache Inbetriebnahme
1. VM Windows 2016+
Max. 50 Dateien betroffen

Berichterstattung für GDPR,
NIS2, Kritis ready .. **Reporting**
bei einer Datenschutzverletzung
+ **sofortige Forensik** möglich
+ **Backup Recovery** der Daten



Die CYBER ANGRIFFS-KETTE

SIP

IPS SCHUTZ VOR DEM EINDRINGEN IN SERVER

RC

RANSOMWARE EINDÄMMUNG

BULLWALL

24x7 Agentlose Eindämmung
Einschließlich Zero-Day-Schwachstellen für On-Premise- und Cloud-Daten

RDP-Schutz
Einbruchschutz und zusätzliche MFA Server-Authentifizierung ohne 2.Gerät

Cyber-Versicherung
Erfüllt die Kriterien für Rabatte oder erhält die Genehmigung der Versicherungsgesellschaften

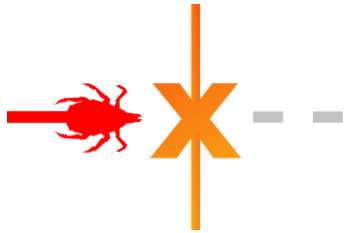
WAS BEDEUTET - RANSOMWARE-RESILIENZ ?

Ransomware-Resilienz ist die **Fähigkeit,** Ransomware Angriffe frühzeitig zu erkennen, wirksam einzudämmen und **Schäden** sofort zu **begrenzen**.

Sie ermöglicht es Unternehmen bei einem Ransomware Angriff, **souverän zu reagieren**, Daten und Prozesse schnell wiederherzustellen – um den **Geschäftsbetrieb ohne Unterbrechung nahtlos fortzusetzen.**

„BullWalls Technologie stärkt die Resilienz Ihres Unternehmens gegenüber Ransomware-Angriffen .“

Was ist ein Zero-Day-Exploit?



Ein Zero Day (auch manchmal „*0-day*“ genannt) ist eine Sicherheitslücke, die den Entwicklern der betroffenen Anwendung noch nicht gemeldet wurde, sodass sie „**null Tage Zeit**“ hatten, sie zu beheben.

Eine Zero-Day-Schwachstelle bleibt manchmal jahrelang offen, bevor sie erkannt, gemeldet und behoben wird.
Die Sicherheitslücke kann in **Hardware, Firmware, Software, fehlenden Updates oder Patches oder jedem anderen Unternehmensnetzwerk** liegen, bevor der Anbieter sich des Problems bewusst ist. In einer Untersuchung des **BSI** wurden über **2.000 Sicherheitslücken gefunden – pro Monat!** Dadurch können schädliche Aktionen wie Code-Ausführung aus der Ferne, Ransomware, Stehlen von Zugangsdaten, DoS-Angriffe oder eine Vielzahl anderer Möglichkeiten in ein System eingeschleust werden.

Ein Zero-Day-Exploit bezeichnet die Techniken und Tools (Malware), die Cyberkriminelle anwenden, um die Zero-Day-Schwachstelle anzugreifen. **Ein ZERO DAY EXPLOIT ist demnach DAS AUSNUTZEN einer solchen SICHERHEITSLÜCKE.**

Bei einem Zero-Day-Angriff handelt es sich um einen aktiven Vorgang. Ein Angreifer testet ein System so lange, bis er eine Zero-Day-Lücke findet. Der „Arbeitsprozess“ für einen Zero Day Angriff beginnt, sobald ein Angreifer die Sicherheitslücke entdeckt hat.
- Ein Zero-Day-Angriff ist, wenn im Zuge eines Zero-Day-Exploits das betroffene System erfolgreich kompromittiert wird.

Zero-Day-Sicherheitslücken können eine Kompromittierung von Organisationen verursachen, und zwar Monate, bevor sie entdeckt werden.
Sie führen zu Betriebsschäden der Organisationen ua. zu Lösegeldzahlungen durch Ransomware Lösegeld Erpressung.
Die Folge sind erhebliche Schäden die durch Encryption + Verschlüsselung von Datenbeständen und Kompromittierung von Systemen verursacht werden, Datenexfiltration, unerlaubte Veröffentlichungen… **>>> Ergo: Ausfallzeit der Organisation, Lösegeldforderung…**

ENTWICKLUNG DER RANSOMWARE-PRÄVENTION – KOMPLEXE SECURITY SYSTEME

BULLWALL

Antivirus Systeme eingeführt

Einführung von **Eindringungserkennungssystemen** und **Eindringungsschutzsysteme**

NIDS/NIPS erlangen Beliebtheit

Web Application Firewall, Malware Scanning entstehen

EDR eingeführt

Maschinelles Lernen von AI und **KI** Verbesserung

DNS Filterung, Lösungen für **Gerätesteuerung** eingeführ**t**

Email Sicherheitstools Gateways verbessert

Schulungen zur Sensibilisierung der Benutzer

Web proxies integriert mit URL Filterung

Zero Trust Ansatz Multi-layer Strategien

SOC SYSTEME Verbessern die Bedrohungserkennung und Reaktionsmaßnahmen

ANGRIFFS-FREQUENZ STEIGT stetig – KI kommt hinzu

1990 2000 2010 2020 2023

WAS HABEN DIESE ORGANISATIONEN FÜR GEMEINSAMKEITEN ?

BULLWALL

Varta – Batterie Hersteller
5000 Mitarbeiter – 8. Wochen Ausfall
+25. Mio. € an Kosten – Insolvenz ?

Motel One - Hotel Gruppe
Größte Sicherheitslücke bisher
7.5TB Datenverlust - PII Daten weg

wertach kliniken
BOBINGEN I SCHWABMÜNCHEN

Krankenhaus / Healthcare
IT Systeme komplett lahmgelegt,
Operationen mussten verschoben werden

Universität Frankfurt
Datendiebstahl + Ransomware. Komplexer Neuaufbau vom Datacenter &. Datensätze

Sixt – Auto Vermietung
2. größte Vermietungsplattform der Welt – PII Daten gestohlen + veröffentlicht

Ehrmann
Keiner macht mich mehr an.

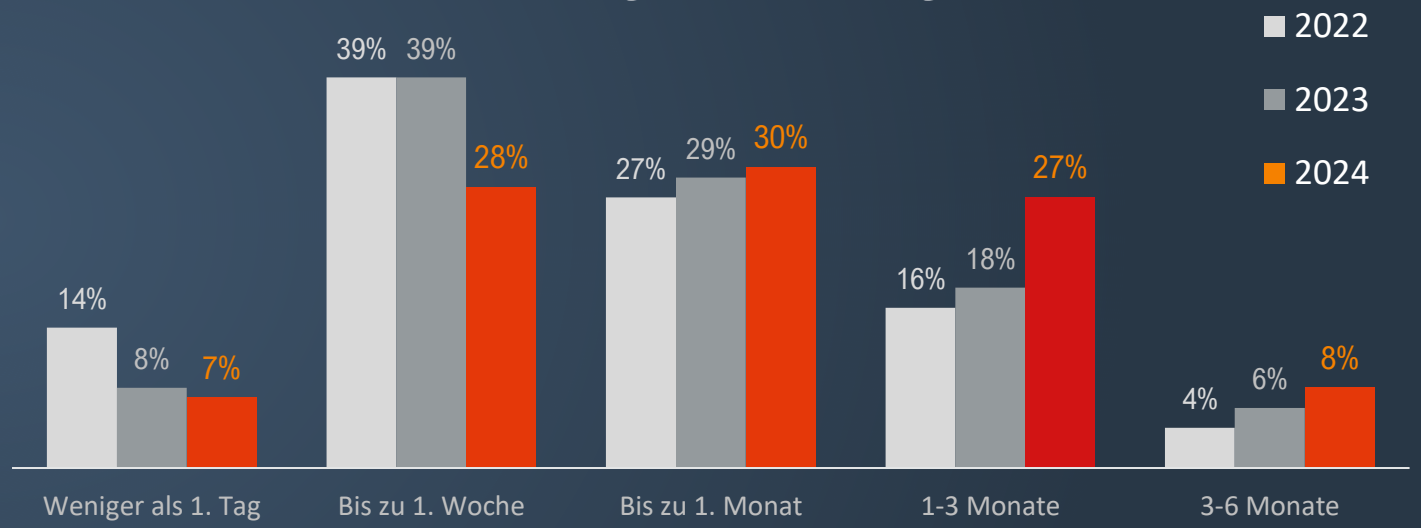
Ehrmann – Lebensmittel
Verwaltung &. Production für 14 Tage stillgelegt - Ransomware Befall

BETRIEBLICHE AUSWIRKUNGEN VON RANSOMWARE NEHMEN DEUTLICH ZU

BULLWALL

2022	2023	2024
ZUNAHME VON RANSOMWARE-ANGRIFFEN		
66%	78%	69%
Wiederherstellungs-Kosten steigen		
€1.4M	€1.82M	€2.73M

Wiederherstellungs-Zeiten steigen deutlich



Ständig steigende Angriffe

Cyberkriminelle entwickeln ihre Angriffsstrategien durch die Nutzung von Daten, KI und Schwachstellen rasch weiter

Recovery Kosten steigen

Die Zahl der Angriffe ist gestiegen.

Aber auch die Wiederherstellungskosten sind um 50 % gestiegen

Betriebliche Ausfallzeit steigt

Die Wiederherstellungskosten stehen in direktem Zusammenhang mit der Fähigkeit, sich schnell von einem Angriff zu erholen

Source: The State of Ransomware Report 2024 by Sophos

Geschäft und IT-Sicherheit müssen den Schwerpunkt auf Wiederherstellung und Resilienz legen

BULLWALL

PwC Global Crisis & Resilience Survey

Von den 2000 Befragten gaben 89 % an, dass Resilienz eine ihrer wichtigsten, eine der wichtigsten strategischen Prioritäten ihres Unternehmens ist. Viele gaben jedoch auch an, dass ihre Unternehmen noch nicht die notwendigen Schritte unternommen haben, um ein integriertes Resilienz Programm für ihr Unternehmen einzuführen, oder noch nicht einmal die Schritte festgelegt haben, um auf diesem Weg voranzukommen. Die Unternehmensleiter sind zuversichtlich, dass sie sich von einer Krise schnell erholen können, was den Tatsachen Statistiken widerspricht.

Zu vielen Organisationen fehlt es an den grundlegenden Elementen der Widerstandsfähigkeit, die für ihren Erfolg erforderlich sind.

McKinsey & Company

Die Welt erlebt ein Ausmaß an Störungen und Geschäftsrisiken wie seit Generationen nicht mehr. Einige Unternehmen gehen unter und scheitern, während andere innovativ sind, sich weiterentwickeln und sogar florieren.

Der Unterschied ist die Widerstandsfähigkeit.

TechRadar

Die CISOs von heute stehen einemSturm gegenüber. Cyberangriffe nehmen von Jahr zu Jahr zu, und neue Technologien wie KI geben Angreifern immer mehr Möglichkeiten.Gleichzeitig wächst die Menge der Daten, die CISOs verteidigen müssen. Allein im letzten Jahr berichteten 85 % der IT- und Sicherheitsverantwortlichen in der EU, dass sie von einem erheblichen Cyberangriff betroffen waren, wobei 36 % dieser Organisationen mindestens einen Ransomware-Angriff erlitten.

CISOs müssen eine Cyber-Strategie entwickeln und umsetzen, die sich auf Widerstandsfähigkeit und Wiederherstellung konzentriert - unabhängig davon, wo ihre Daten gespeichert sind.

MSN

Es ist eine unangenehme Realität, dass Cyberangriffe zunehmend unvermeidbar sind. Aber es ist die Realität. Bis vor relativ kurzer Zeit wurde der Cyber-Resilienz keine Priorität eingeräumt - nun kommen jedoch Vorschriften ins Spiel, die die Priorisierung der Cyber-Resilienz unterstützen. (DORA und NIS2) Aus diesem Grund müssen Cybersecurity-Experten eine Position der Cyber-Resilienz einnehmen, ***und sich darauf vorbereiten, sich von einem Angriff schnell zu erholen, anstatt ihn nur abzuwehren (Prävention).***

Auf Prävention, ausgerichtete Ansätze für unseren Schutz

Erfordern das Sie…

- 99% Wirksam + effektiv sind,
- 100% des gesamten Zeitraums, auf
- 100% Ihrer Angriffsfläche,
- Gegen 100% der Gefährdungen.

DAS PROBLEM IST…

ES GIBT KEINEN 100% SCHUTZ !

Der 100%ige Schutz den wir dringend brauchen ist NICHT gewährleistet- und stellt eine Schutzverletzung dar!

Das Risiko steigt von schädlicher Ransomware getroffen zu werden.

SCHWACHSTELLEN WERDEN AKTIV GENUTZT. ES FEHLT AN RESILIENZ BEI RANSOMWARE ANGRIFFEN !

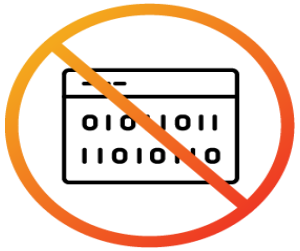
BULLWALL

BEI EINEM AKTIVEN RANSOMWARE VORFALL IM UNTERNEHMEN MÜSSEN FOLGENDE FRAGEN SCHNELL BEANTWORTEN WERDEN !

ZEIT IST EINE WICHTIGE UND SEHR KRITISCHE KOMPONENTE

- **KÖNNEN SIE IN DEN ERSTEN 30 SEKUNDEN SOFORT REAGIEREN UND HANDELN ?**

Sehen welche Daten und Files verschlüsselt wurden, und wo Sie liegen ?

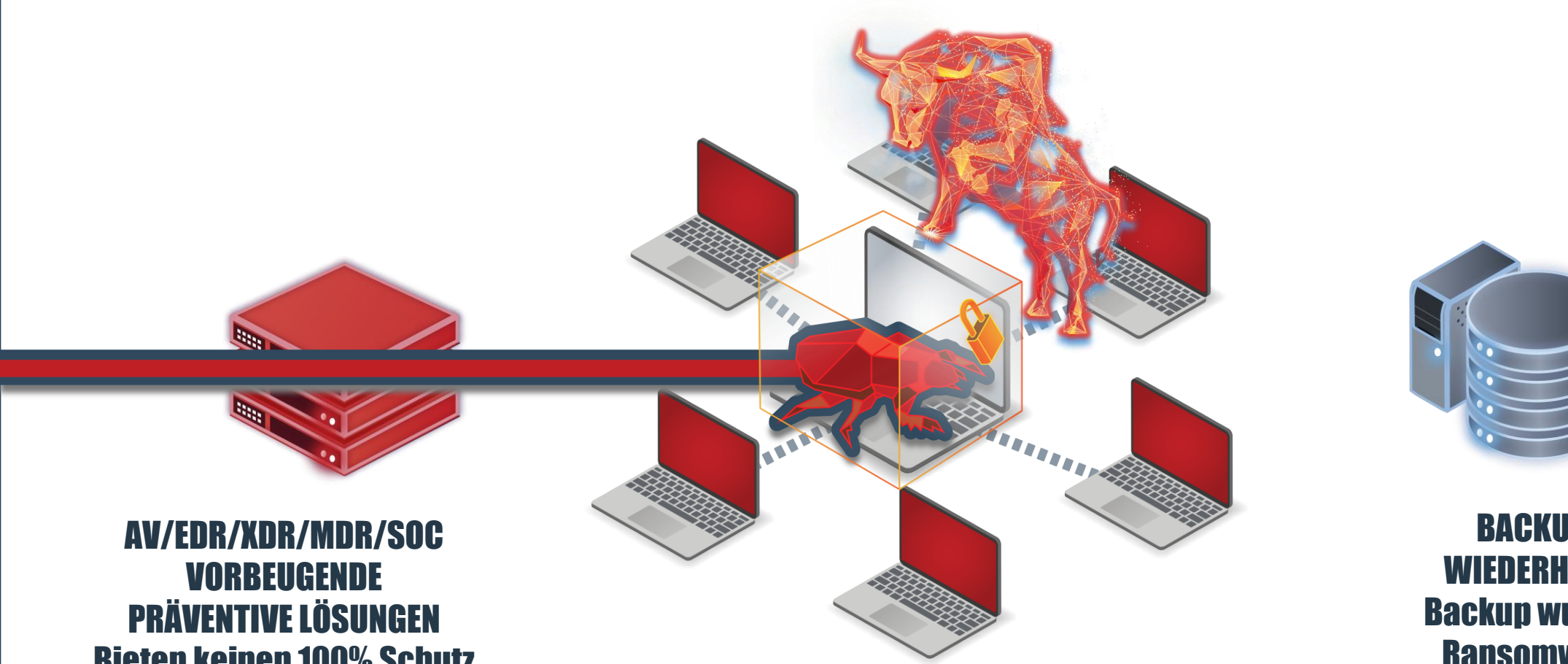


Den Angreifer sofort identifizieren / lokalisieren ? Woher kommt der Angriff ?

Die laufende Verschlüsselung stoppen ? Ausbreitung verhindern ?

EINDÄMMUNG: DAS FEHLENDE PUZZLE STÜCK BEI DER ABWEHR GEGEN RANSOMWARE

BULLWALL



AV/EDR/XDR/MDR/SOC
VORBEUGENDE
PRÄVENTIVE LÖSUNGEN
Bieten keinen 100% Schutz

BACKUP LÖSUNG
WIEDERHERSTELLUNG
Backup wurde nicht für
Ransomware gebaut

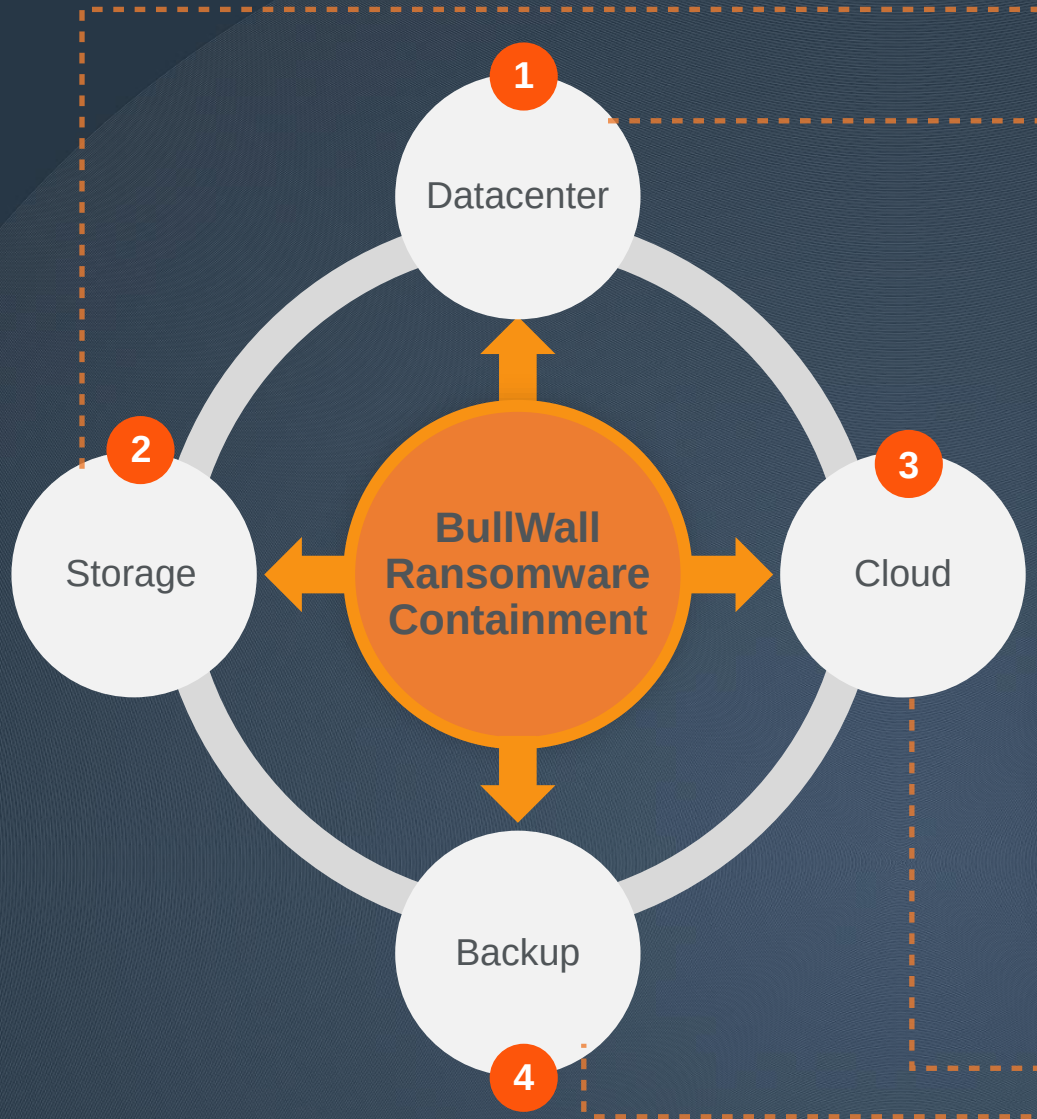
MISSING CRITICAL

CONTAINMENT LÖSUNG FEHLT - BULLWALL LIEFERT RANSOMWARE EINDÄMMUNG

BullWall schützt automatisiert die kritische IT-Infrastruktur + DATEN + DATEIEN + SERVER
<< Sorgt für dringend benötigte und fortlaufende Betriebs-Resilienz rund um die Uhr >>

SCHÜTZT DIE GANZE KRITISCHE INFRASTRUKTUR – HERZ DES BETRIEBS

BULLWALL



Erweiterter Schutz durch Bullwall

BULLWALL RANSOMWARE CONTAINMENT

Critical IT Infrastructure	Storage	Cloud Umgebungen	Backup
1	2	3	4
Vmware Plattform Domain Controllers AD (on-prem + Cloud) Application Servers Database Servers Web Servers Citrix / Azure / AWS	Windows File-servers NetAPP EMC Isilon Pure Storage Cohesity Nutanix IBM / HP / HUWAEI HITACHI	Office 365 SharePoint Seiten OneDrive Teams Google	Veeam Commvault Dell IBM Veritas Rubrik Cohesity Microsoft Arcserv Barracuda

Vollständiger Schutz der kritischen IT-Infrastruktur : Server / Plattformen / Cloud / Backup / Virtualisierung...

VEREINFACHTE DARSTELLUNG BEI EINEM ANGRIFF

BULLWALL

L

Externer Datenverkehr was aufs Unternehmen zukommt

Secure Email Gateway

Corporate Firewall

Web Gateway

Perimeter Schutzschichten

1. Verteidigungslinie

EDR, XDR, MDR, SOC Systeme …

2. Präventive Verteidigungslinie (präventiv handelnd Fokus Endgeräte Schutz)

Kompromitierter Benutzer/Gerät
wird von BullWall RC automatisiert isoliert
Ransomware Angriff sofort eingedämmt

Hier sitzt Bullwalls Containment Lösung –
"Hören" im Netzwerk zu – SMB Notificationen

Bullwall Ransomware Containment Layer

Wichtige 3. Verteidigungslinie für unsere Assets

24x7x365 ECHTZEIT SCHUTZ der KRITISCHEN IT INFRASTRUKTUR

Wohin der Ransomware Angriff und die Verschlüsselung abzielt

On-Site (SAN/NAS)
Database Servers
Virtual Machine
Cloud
Application Servers
Domain Controller

Data Storage & kritische IT Infrastruktur

Das kompromittierte Endgerät, der betroffene Benutzer wird durch **BullWall automatisiert** in Echtzeit **isoliert** aus dem aktiven AD genommen, der weitere Zugriff verhindert -**Containt / eingedämmt.** Die schädliche Ransomware Ausbreitung ist im Einsatz mit Bullwalls Lösung - **sofort eingedämmt – sofort gestoppt !**

Betrieb geht nahtlos weiter – Infrastruktur geschützt

Business as usual für das Unternehmen

CONTAINMENT: DAS FEHLENDE MODUL FÜR CYBER RESILIENZ

BULLWALL

PRÄVENTION BIETET KEINEN 100% SCHUTZ, DEN WIR RUND UM DIE UHR BENÖTIGEN

Eine **Cybersicherheitsstrategie**, die sich stark auf die **Prävention** konzentriert, ist nicht **nachhaltig und ineffektiv, Schwachstellen werden ausgenutzt**

ANGESICHTS DIESER ALARMIERENDEN STATISTIKEN ERFOLGREICHER ANGRIFFE, IST ES WICHTIG EINE ASSUME BREACH MENTALITÄT ANZUNEHMEN !

EIN ANGRIFF WIRD DURCHKOMMEN, NICHT ERKANNT DURCH DIE PRÄVENTION, RANSOMWARE LEGT LOS. DYNAMISCHE IT STRATEGIE BENÖTIGT, DIE EINEN TREFFER AUFFÄNGT.

Prävention / Vorbeugend
Verhindern blockend Scannen

SentinelOne · CROWDSTRIKE · Microsoft · Bitdefender · CHECK POINT · eset · Trellix

Blocken bekannte Attacken

Was könnte schief gehen... ?

Fehlkonfiguration, offene Schwachstellen...

Fehlende Updates Patches…

Der Agent spricht nicht mit dem Server...

Erkennen + Handeln regelmäßig nicht bei unbekannten neuen Zero Day Attacken...

MISSING CRITICAL
Containment = Eindämmung

BULLWALL

Containment schließt offene Lücken und Schwachstellen

<< STOPPT RANSOMWARE >>

AUTOMATISIERT + GARANTIERT

stoppt unbekannte Zero Day Ransomware

Wiederherstellung von max. 10-50 Dateien die betroffen sind

+FORENSIK +REPORTING +RECOVERY

Recovery / Backup
Wiederherstellung

Entscheidend für die Geschäftskontinuität

Nie gebaut worden für Ransomware Vorfälle

Was könnte schief gehen ?

- Backup Dateien infiziert
- Clean recovery Punkt finden, wo ?
- Daten Delta bei der Wiederherstellung da

IN DER HEUTIGEN CYBER STRATEGIE IST EINE „CONTAINMENT“ LÖSUNG EINE ENTSCHEIDENDE KOMPONENTE FÜR DIE RESILIENZ

WIE UNTERSCHEIDEN WIR UNS ?

BULLWALL

USER *ÖFFNET EIN* FILE

Vorhandener Security Stack Scannt, versucht zu blocken

Scannt nach Anzeichen oder Mustern von Malware in Dateien, Dokumenten

Fakt: Was die Lösungen noch nie gesehen haben oder nicht in Ihrer Datenbank vorhanden ist, wird nicht erkannt, geblockt oder gestoppt ..... Was dann ?

SentinelOne · CROWDSTRIKE · Microsoft · Bitdefender · CHECK POINT · eset

Documents, System Files, Operating Systems

Übersehen oft Zero-Day Ransomware
und andere unbekannte neue Malware.
Ransomware kann später von den Lösungen nicht mehr gestoppt werden....

USER *KREIRT* OD. *MODIFIZIERT* FILES

Bullwalls Ransomware Containment schaut auf das Verhalten von Ransomware und hört SMB Informationen im Netzwerk ab

Prüft und erkennt in Millisekunden Datei Verschlüsselungen, Veränderungen oder Beschädigungen – stoppt auch neue unbekannte zero day Attacken !

BULLWALL

SCHÜTZT 24*7*365

Documents, System Files, Operating Systems

&

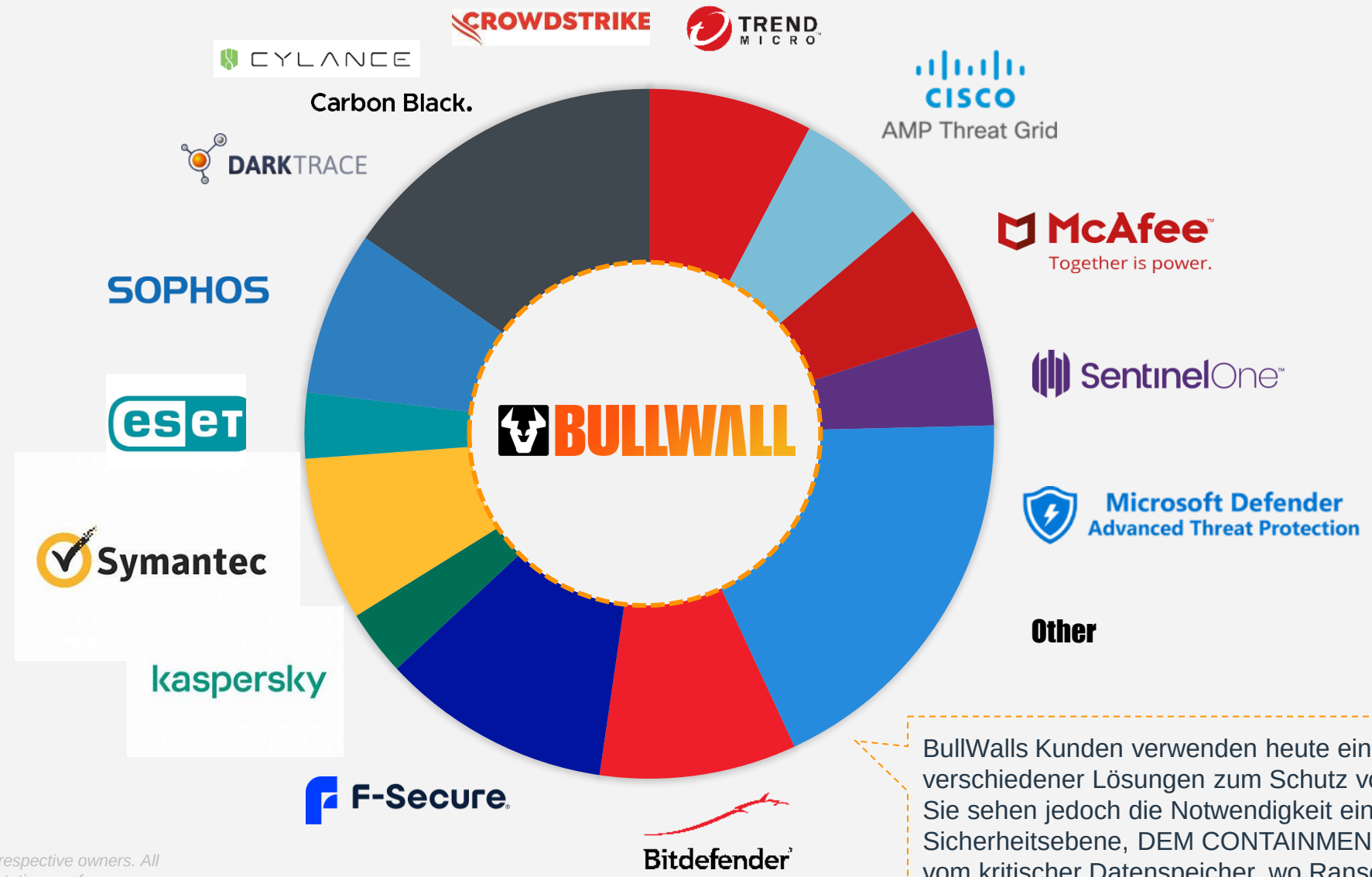
CRITICAL IT INFRASTRUCTURE
Storage / Servers / Cloud / Backup

Bullwall erkennt die unzulässige Verschlüsselung sofort und stoppt den Angriff automatisiert in Millisekunden !
Stoppt auch zero Day Ransomware ! GARANTIERT !

Keine Überschneidungen von BullWalls Lösung mit Ihren bestehenden Sicherheitssystemen

WIR INTEGRIEREN UNS NAHTLOS IN VERSCHIEDENARTIGE LÖSUNGEN / PLATTFORMEN

BULLWALL



BullWalls Kunden verwenden heute eine Vielzahl verschiedener Lösungen zum Schutz von Endgeräten. Sie sehen jedoch die Notwendigkeit einer zusätzlichen Sicherheitsebene, DEM CONTAINMENT, zur Überwachung vom kritischer Datenspeicher, wo Ransomware hinzielt.

Übersicht: BullWall Ransomware Containment

BULLWALL

- **Schützt die ganze kritische IT Infrastruktur** - On-Prem und in der Cloud
- **Agentless & einfach zu implementieren** - keine Endpunkt Installation
- **Erkennt und stoppt sämtliche Ransomware**, auch neue zero day Exploits
- **24x7 Automatische Erkennung und Handlung** vor Ransomare in Echtzeit
- **Automatische Berichterstattung möglich** bei GDPR,NIST,KRITIS Anforderungen
- **Forensik und Recovery Tools** für Ursachenforschung, für Wiederherstellung dabei

DETECT

- Aktive Datenüberwachung in Echtzeit , 365x24x7
- 28 Erkennungssensoren maschinelles Lernen mit AI, sowie KI Technologie
- Erkennt sofort unzulässige Verschlüsselungen und bösartige Ereignisse, völlig automatisiert

RESPOND

- Isoliert gefährdete Benutzer und Geräte sofort
- Integrationen mit SIEM, NAC, EDR, über RESTful API Befehle
- Alarm über email, SMS, app, etc.

RECOVER

- Identifiziert verschlüsselte Dateien zur Wiederherstellung vom Backup
- Lokalisiert gefährdete Benutzer und Geräte
- Versteht den ursprünglichen Angriffsvektor für die interne Untersuchung

REPORT

- Automatisierte Berichtserstattung über Vorfälle mit sofortigem Angriffsprotokoll
- Informiert umfassend die Unternehmensleitung
- Bereitstellung eines gesetzlichen gültigen Berichts für die Behörden

BULLWALL

RANSOMWARE - HEALTH CHECK

KLARHEIT + GEWISSHEIT BEKOMMEN

Wie reagieren meine im einsatz befindlichen Sicherheits-Tools ???

1

Sie erhalten ein Dokument mit den Voraussetzungen, um sich auf das Assessment mit BullWall vorzubereiten

Assessment dauert ingesamt 2 Stunden
*** Kostenloser Health Check ***

Vorraussetzungen schaffen
Teil 1: Installation
Teil 2: Live tests

Einrichtung und Freigabe eines Testbereichs
Security Systeme aktiv

2

Wir führen mehrere reale Angriffs-Simmulationen durch mit: bekannten, unbekannten, zero day Ransomware und wollen verstehen…

Wie reagiert Ihr Netzwerk ?
Ihre vorhandenen Security Tools ?

Wird Ihre bestehende Security reagieren? Wann wird Sie handeln, wie schnell, und überhaupt ?

Erleben Sie den Unterschied mit BullWalls Lösung in Ihrer Umgebung Wie wir Ransomware automatisiert in MS eindämmen

3

Über 95 % der Organisationen fanden die zweistündige Sitzung sehr aufschlussreich und hilfreich

Globale **Sicherheits-Beurteilung** und **Risikoabschätzung** möglich

Verstehen Sie Ihre **Widerstandsfähigkeit** bei einer Ransomware Verschlüsselung und verstehen offene Schwachstellen

Das **Assessment Ergebnis** bekommen Sie als PDF Dokument im Nachgang überschickt

VIELEN DANK
ES FOLGT -> LIVE DEMO

BULLWALL

SERVER INTRUSION PROTECTION

SCHUTZ DER SERVER
VOR RANSOMWARE
&. EXFILTRATION VON DATEN

Beibehaltung der Präventions-Schichten

RDP

Remote Desktop Protocol. Eine Möglichkeit für Administratoren, von jedem Ort der Welt aus auf Remote-Server zuzugreifen und diese zu steuern

SCHEDULED TASK MANAGER

Mit Administratorrechten kann der Angreifer per Fernzugriff Aufgaben auf den Servern planen, die Sicherheitstools herunterfahren und die anschließende Ausführung der Schadsoftware tätigen

Wie häufig ?

Etwa 95 % der Ransomware-Angriffe enthalten eine RDP und/oder einen Angriff auf den Sheduled Task Manager*.

*2023 Sophos Report

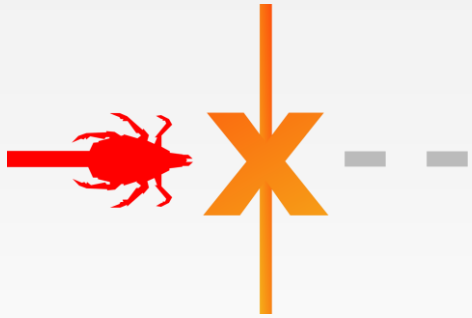
Ihre Tools können zwar viele Ransomware-Angriffe stoppen, aber sobald Sie deaktiviert sind, sind sie nutzlos.

Schutz der Server vor Ransomware &. Exfiltration

- ✓ **MFA für RDP Sitzungen:** Kein 2. Gerät notwendig, erkennt und informiert über ein schädliches Verhalten - IoC
- ✓ **Frühzeitige Erkennung von Eindringlingen** bei fehlgeschlagener MFA
- ✓ **Überwachung der Scheduled Tasks:** Verhindert die Installation von Malware
- ✓ **Unveränderliche Erfassung der Serverzugriffe:** Forensik für alle Login-Versuche

Verhindert das Eindringen

Innovative MFA. Sie identifiziert einen Eindringling und leitet ein Eindämmungsprotokoll ein, das die Verbreitung von Ransomware, die Verschlüsselung von Daten und die Exfiltration von Daten verhindert.



Stoppt das Fortschreiten

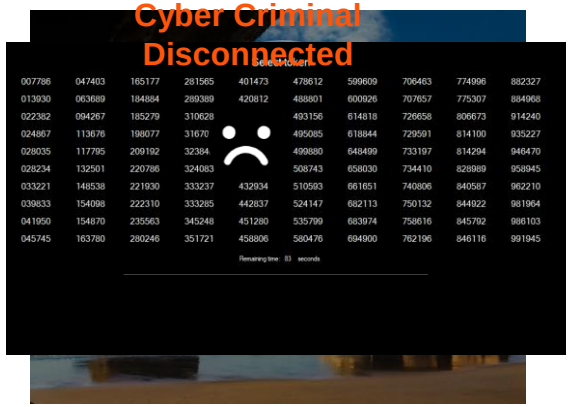
Indem der Cyberkriminelle aufgehalten wird, werden Spionage und unkontrolliertes Verhalten verhindert, und das Potenzial für eine Kompromittierung anderer Netzwerkbereiche wird effektiv unterbunden.

Schützt vor gestohlenen Zugangsdaten

Eine fehlgeschlagene MFA-Abfrage zeigt, welche Anmeldeinformationen es waren und welches Gerät kompromittiert wurde, und isolieren diesen Zugang sofort..

BULLWALL SERVER INTRUSION PROTECTION

CLIENTS/ENDPUNKTE



User/Gerät
Isoliert

NETZWERK IT INFRASTRUKTUR / DATACENTER

GERÄT KOMPROMITTIERT

Trojanisches Pferd, automatisierter oder manueller Angriff

ADMIN ZUGANGSDATEN EXTRAHIERT MIT MIMIKATZ

RDP SITZUNG GESTARTET / LOGIN IN DEN SERVER

RDP Login, fortlauf der gekaperten Sitzung

MFA CODE SEKUNDEN NACH DEM LOGIN ANGEFORDERT

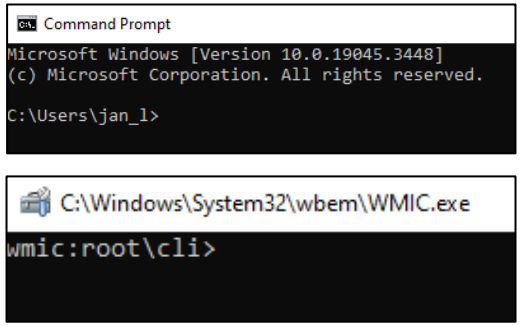
- ✓ BULLWALL SERVER INTRUSION SCHUTZ INSTALLIERT
- Token Eingabe per Handbefehl *Sicherheitsanforderungen,sehr streng*
- Token aus dem Raster auswählen (verhindert, dass Keylogger denToken lesen) *Sicherheitsanforderungen, normal*
- Schnellanmeldung feste Werte (gleicher Token, gleiche Rasterposition) *Sicherheitsstufe mittel, effizient*

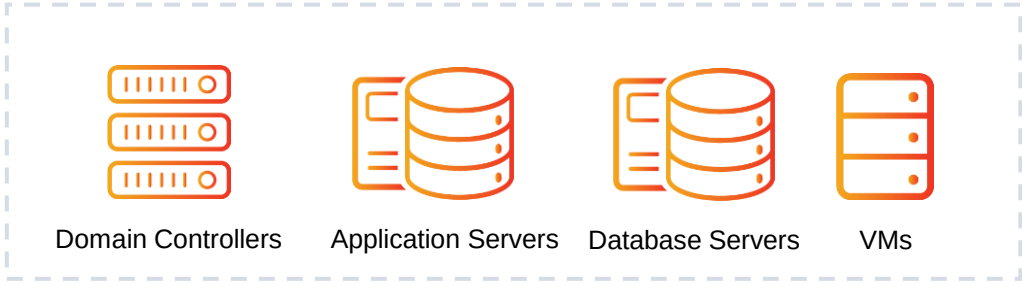
FALSCHER MFA-CODE EINGEGEBEN - ANGREIFER ENTDECKT AUTOMATISCHE 24/7 RÜCKANTWORT

- ✓ Gestohlenes Admin-Konto wird sofort gesperrt in AD (on-prem, Azure)
- ✓ Kompromittiertes Benutzerkonto wird sofort gesperrt in AD (on-prem, Azure)
- ✓ Alam ausgelöst via. (e-mail, SMS, SIEM, SOC, NOC, Service Now etc.)
- ✓ Kompromittiertes Gerät wird durch bestehende Sicherheitslösung und Integrationen isoliert

BULLWALL SERVER INTRUSION ERKENNUNG – SCHEDULED TASK ÜBERWACHUNG

CLIENTS/ENDPUNKTE



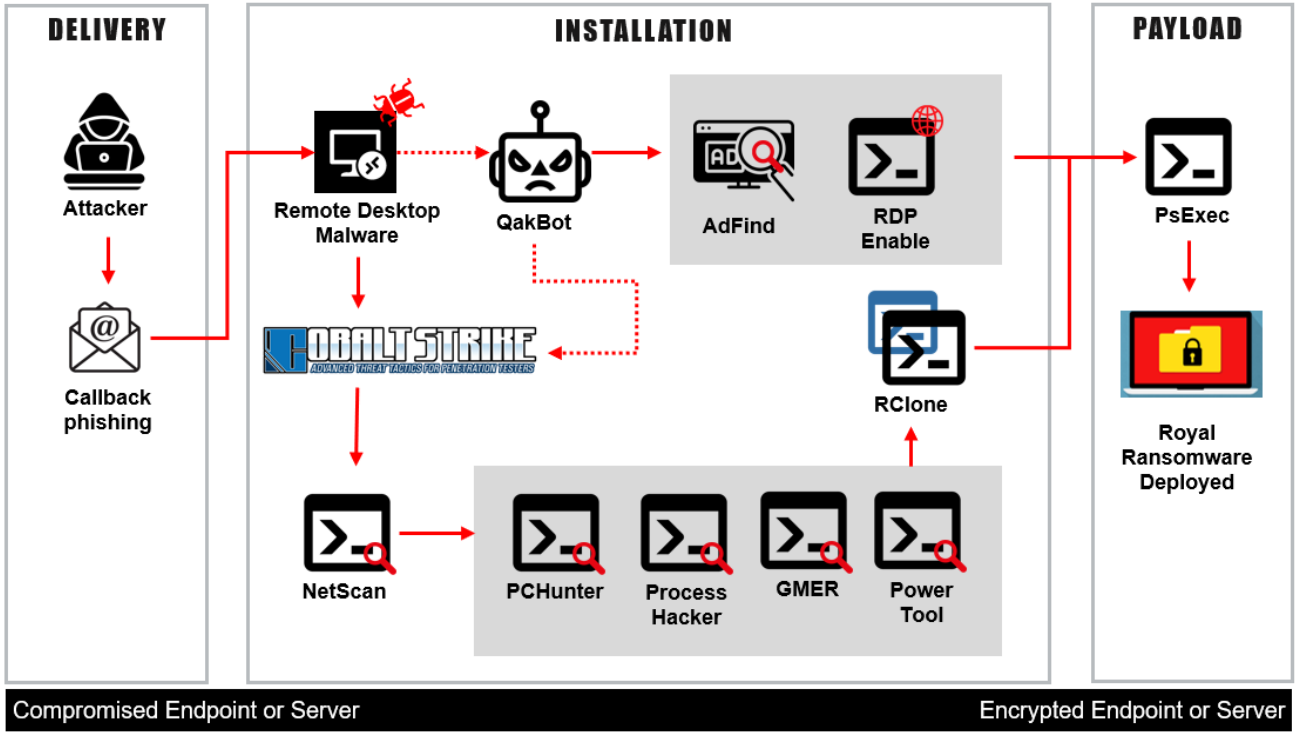


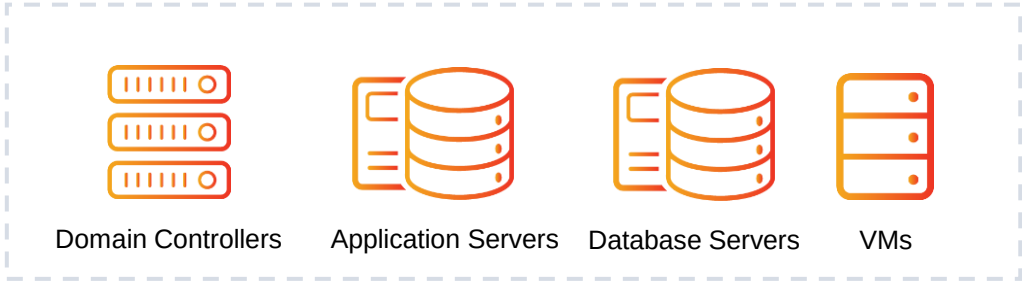
NETZWERK IT INFRASTRUKTUR / DATACENTER

SITZUNG GESTARTET / SERVER ANGEGRIFFEN

Geplante Aufgaben werden in der Regel per Fernzugriff erstellt:
Remote-Powershell, PsExec, WMIC, WMI, SMB Protokoll
Keine Anmeldung über RDP, daher wird in diesem Fall die MFA-Autorisierung nicht abgefragt

BULLWALL SERVER INTRUSION DETECTION – SCHEDULED TASK MONITORING





NETZWERK IT INFRASTRUKTUR / DATACENTER

SITZUNG GESTARTET / SERVER ANGEGRIFFEN

Geplante Aufgaben werden in der Regel per Fernzugriff erstellt:
Remote-Powershell, PsExec, WMIC, WMI, SMB Protokoll
Keine Anmeldung über RDP, daher wird in diesem Fall die MFA-Authentifizierung nicht abgefragt.

CYBER KRIMINELLE NUTZEN STANDARD WERKZEUGE WIE

Cobolt Strike, Mimikatz, MegaSync, AdFind, PCHunter, NetScan, PowerTool, GMER sind Produkte der Hacker, um alle sicherheitsrelevanten Dienste zu deaktivieren, die laufen.

SITZUNG GESTARTET / SERVER ANGEGRIFFEN

Geplante Aufgaben werden in der Regel per Fernzugriff erstellt:
Remote-Powershell, PsExec, WMIC, WMI, SMB Protokoll
Keine Anmeldung über RDP, daher wird in diesem Fall die MFA-Authentifizierung nicht abgefragt.

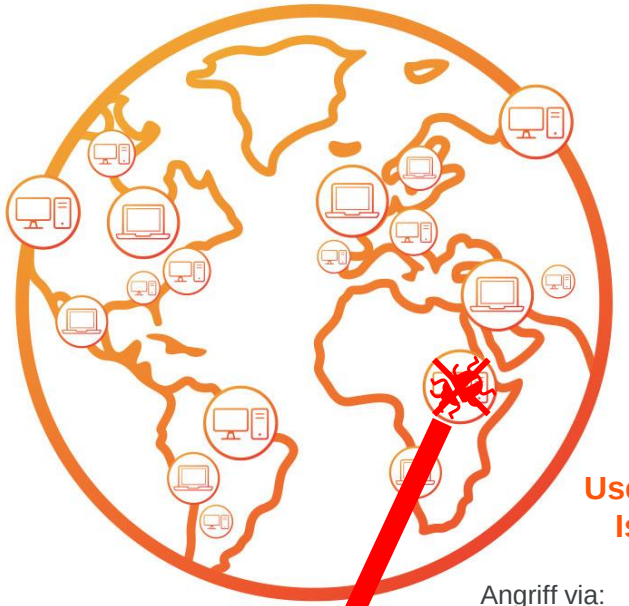
CYBER KRIMINELLE NUTZEN STANDARD WERKZEUGE WIE

Cobolt Strike, Mimikatz, MegaSync, AdFind, PCHunter, NetScan, PowerTool, GMER sind Produkte der Hacker, um alle sicherheitsrelevanten Dienste zu deaktivieren, die laufen.

NETZWERK IT INFRASTRUKTUR / DATACENTER

BULLWALL SERVER INTRUSION DETECTION – SCHEDULED TASK MONITORING

CLIENTS/ENDPOINTS



Cyber Criminal
Disconnected

User/Device
Isolated

Angriff via:
Remote-Powershell, PsExec, WMIC,
WMI, SMB Protokoll

Domain Controllers | Application Servers | Database Servers | VMs

NETZWERK IT INFRASTRUKTUR / DATACENTER

SITZUNG GESTARTET / SERVER ANGEGRIFFEN

Geplante Aufgaben werden in der Regel per Fernzugriff erstellt:
Remote-Powershell, PsExec, WMIC, WMI, SMB Protokoll
Keine Anmeldung über RDP, daher wird in diesem Fall die MFA-Authentifizierung nicht abgefragt

CYBER KRIMINÄLLE NUTZEN STANDARD WERKZEUGE WIE

Cobolt Strike, Mimikatz, MegaSync, AdFind, PCHunter, NetScan, PowerTool, GMER sind Produkte der Hacker, um alle sicherheitsrelevanten Dienste zu deaktivieren, die laufen.

SCHEDULED TASK MONITORING (STM)

- ✓ Verdächtige Aufgaben erstellt
- ✓ Ungewöhnliche Aufgaben erstellt
- ✓ Jobverwaltung gekapert - ausgeführte Datei mit bösartiger Datei vertauscht

SERVER ANGEGRIFF AUTOMATISCHE 24/7 RÜCKANTWORT

- ✓ Alam ausgelöst via. (e-mail, SMS, SIEM, SOC, NOC, Service Now etc.)
- ✓ Gestohlenes Admin-Konto wird sofort gesperrt in AD (on-prem, Azure)
- ✓ Angefangene Aktivität gelöscht
- ✓ Kompromittiertes Benutzerkonto wird sofort in AD blockiert (On-Prem, Axure)
- ✓ Kompromittiertes Gerät und/oder durch Integration der bestehenden Sicherheitslösungen

Verwenden Sie VMware / ESXi / vSphere für das Management Ihres Hypervisors auf dedizierten Infrastrukturen/Servern oder in der Cloud?

BullWalls erweiterter Schutz für VMware / vSphere / ESXi-Plattform und -Systeme

WARUM SIE SCHUTZ FÜR VMware / vSphere / ESXi Umgebungen benötigen

BULLWALL

- Ransomware-Angriffe zielen zunehmend auf VMware vSphere- und ESXi-Plattformen ab, legen virtuelle Server lahm und machen wichtige IT-Infrastrukturen unzugänglich

- Cyberkriminelle schalten Unternehmen aus, indem sie VMware-Plattformen direkt über SSH oder durch Verschlüsselung von Images von außen ausnutzen

- **Bestehende Sicherheitslösungen gehen nicht auf dieses spezielle Risiko für VMware ein - um diese Lücke zu schließen, müssen Sie Ihr Sicherheitspaket erweitern. BullWall schließt diese kritische Lücke mit VSP und schützt ganz gezielt diesen Business kritischen Bereich**

BULLWALL VIRTUAL SERVER PROTECTION - Übersicht

Security Funktionen

1. Verbessert die SSH-Sicherheit auf der ESXi-Plattform mit MFA und OLTP
2. Überwacht laufende Prozesse auf der ESXi-Plattform,
   um aktive Bedrohungen zu erkennen und Verschlüsselung sofort zu stoppen
3. Erkennt die Dateiverschlüsselung oder Beschädigung von VMware-Systemdateien

und identifiziert die Verschlüsselung von Images:
Daten der bereitgestellten VM-Dateien/Host-Dateien die wir schützen
(VMX, VMDK, VMSD, VMXF, VRAM).
Und andere Fileformate wie (OVA, VI, vCloud, ISO, FLP)

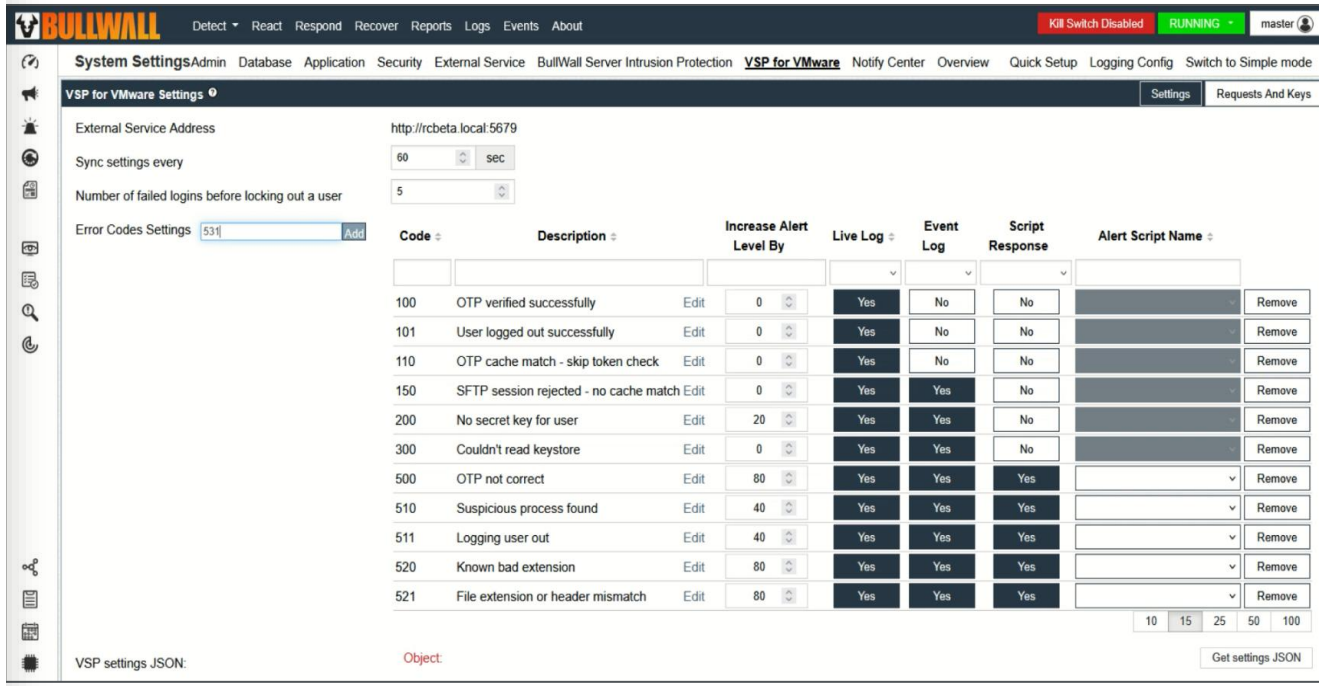
THIS IS PROTECTION YOU DO NOT HAVE TODAY !

BULLWALL VIRTUAL SERVER PROTECTION - RESPONSE OPTIONS

BullWall Virtual Server Protection bietet automatisiert Alarmierungs- und Isolierungsfunktionen

Mit der bestehender BullWall Ransomware Containment-Konsole können Sie:

1. **Senden** von Warnmeldungen per E-Mail, Syslog oder von Ereignisprotokollen
2. **Direkte** Integration mit SIEMs, MSP-Dashboards oder internen Systemen
3. **Sperren** von Benutzeranmeldeinformationen in AD (Cloud und On-Premise) auf jedem Domänencontroller und auf lokalen ESXi-Konten
4. **Sperren** von Geräten und Benutzern mit VPN-Verbindungen
5. **Isolierung** von Client-Geräten und Benutzern über EDR/XDR-Integration
6. **Automatische** Erstellung von Tickets in Supportsystemen (z. B. ServiceNow)
7. **Erweitern** Sie den Schutz durch vollständige Integration in Ihr bestehendes Sicherheitssystem.



Umfang der Installation / Implementierung der Lösung:

1. Die BullWall ESXi-Komponente wird auf dem ESXi-Server installiert
2. HTTPS-Zugang zum BullWall RC-Server ist erforderlich, um Dashboards zu aktualisieren und Plug-ins für Isolationsskripte auszuführen (sowohl bereits vorhandene als auch neue Skripte)
3. Die Installation dauert in der Regel 1-2 Stunden und kann zu Schulungs- und Validierungszwecken in einer Nicht-Produktionsumgebung getestet werden
4. Unterstütze Versionen sind:

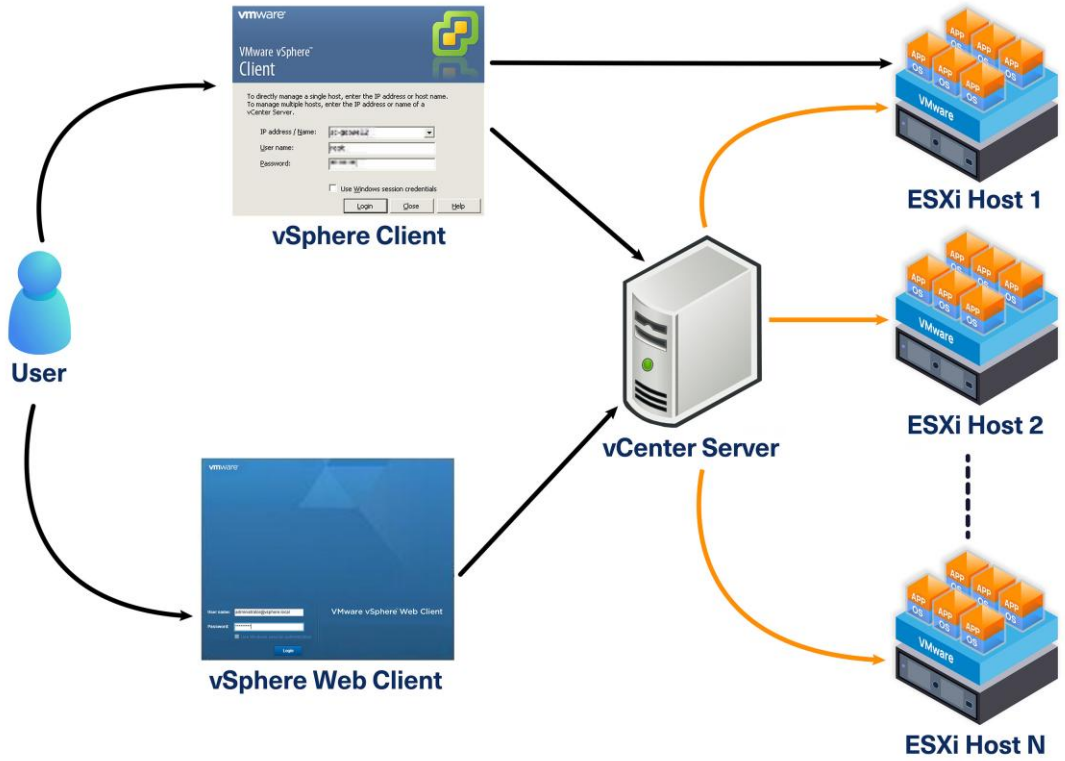
Kompatibel mit VMware und ESXi 7.0 und 8.0

vmware vSphere

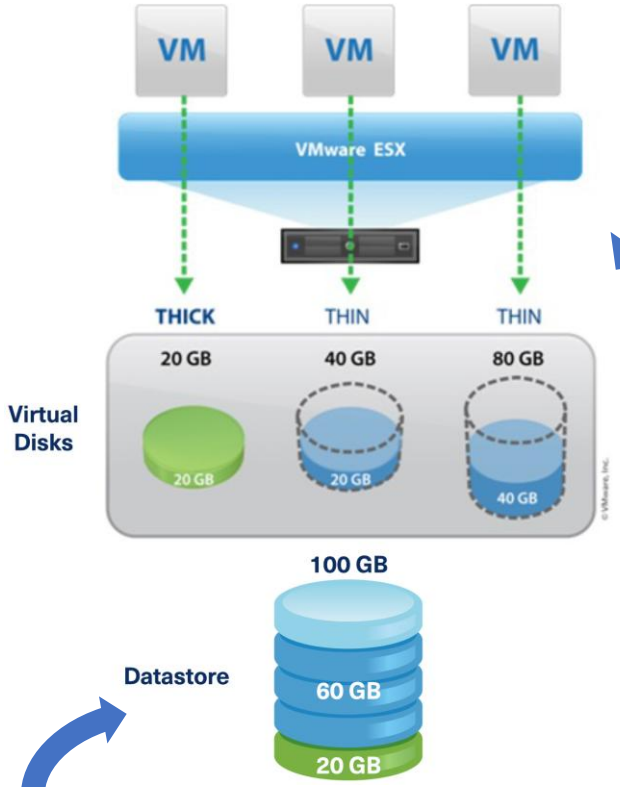
VMware ESXi™

EINFACHE UND SCHNELLE INSTALLATION

BullWall Virtual Server Protection-Anwendungen, die auf ESXi-Hosts installiert werden, um den Zugriff und die Verschlüsselung von außen/von der Speicherseite aus zu verhindern



MFA-Schutz für die Anmeldung auf ESXi-Hosts über SSH



Auf ESXi-Hosts installierter Schutz

Überwacht Prozesse, Dateien und Formate auf Datenspeichern und virtuellen Festplatten über NFS und internen Speicher

GARTNER: ” „DER BLITZ IN DER FLASCHE“ ”

BULLWALL

Gartner®

“ Niemand hat das, was RansomContainment von Bullwall bietet; es ist einzigartig auf dem Markt als Active Defense, das sowohl die Cyber- als auch die Datenresilienz verbessert.

“ Ich habe RansomCare meinen Unternehmen empfohlen, bevor ich überhaupt mit Ihnen gesprochen habe, weil ich im Internet ein Video gefunden habe, das zeigt, welche Probleme es löst. Ich habe es satt, dass Leute denken: „Es geht nicht um das OB, sondern um das WANN.

“ Ich sage meinen Kunden, dass es mir egal ist, wie gut ihr EDR-System ist. Es wird Zero-Day-Angriffe nicht aufhalten, die wir im letzten Jahr x Mal gesehen haben und die innerhalb von Tagen als Waffe eingesetzt wurden, z. B. Log4J, das Conti innerhalb von 72 Stunden verwendet hat. Deshalb brauchen sie RansomCare im Rücken.

“ RansomContainment ist eine der beeindruckendsten Lösungen, die ich seit Jahren gesehen habe. Niemand sonst hat eine automatische Antwort auf Ransomware-Angriffe entwickelt, wie BullWall es getan hat.

DIE FOLGENSCHÄDEN VERSTEHEN / BERECHNEN

NUMBER OF USERS ON THE NETWORK
How many users are in the Active Directory?
excl. service accounts

Users in the AD

RANSOMWARE IMPACT
What percentage of employees will be impacted by a ransomware attack?

0
users offline

TECHNOLOGY DEPENDENT
How dependent are employees on technology to conduct normal operations?

Dependency on IT

AVERAGE EMPLOYEE COSTS
What is the average hourly cost per employee?
include wages, pension, and indirect costs such as office rental, etc.

Total cost per employee

According to Coveware, downtime is still the costliest aspect of a ransomware attack. In Q2 of 2022, the average firm experienced 24 days of downtime, a 3-day increase from 2020.

OFFLINE SERVICES
How many hours will employees experience downtime while IT professionals restore online services following a ransomware attack?
One workday is equivalent to 8 hours.

24 days = 192 hours

FILE RESTORATION
How many hours will it take for a single employee to recreate lost files that were unrecoverable from the data backup?

COST OF DOWNTIME
You might not have the budget for additional protection. However, do you have the budget to cover the cost of recovering from a potentially devastating incident? The below calculation is just a loss of productivity, typically only 20-35% of the entire recovery cost.

$0

KOSTENRECHNER FÜR AUSFALLZEITEN

Wie viel würde ein Ransomware-Angriff Ihr Unternehmen kosten?

Link zu BullWalls <<< Cost of Downtime Calculator in EUR | BullWall