DataStore AG . Pfadackerstrasse 6 . 8957 Spreitenbach . Switzerland
T +41 56 419 71 71 . info@datastore.ch . www.datastore.ch

BullWall im Überblick – Einsatz, Nutzen und Integration

Moderne Sicherheitsarchitekturen setzen auf ein Zusammenspiel verschiedener Lösungen wie EDR, XDR und NDR, um Bedrohungen frühzeitig zu erkennen und abzuwehren. Jede dieser Technologien hat ihre spezifischen Stärken und trägt wesentlich zur IT-Sicherheit bei.
Dennoch können gezielte Angriffe – insbesondere Ransomware – bestehende Schutzmechanismen umgehen. Hier setzt Bullwall als zusätzliche Schutzebene an und ergänzt die vorhandenen Systeme um eine spezialisierte Containment-Schicht.

BullWall – Last Line of Defense

BullWall erweitert bestehende Sicherheitslösungen um eine zusätzliche Verteidigungsebene und übernimmt die Rolle der „Last Line of Defense" – also der letzten Verteidigungslinie, wenn Schadsoftware wie Ransomware bereits in das Netzwerk gelangt ist und von anderen Schutzmechanismen wie EDR, XDR oder NDR nicht vollständig gestoppt werden konnte.

Im Unterschied zu klassischen Sicherheitslösungen, die primär auf die Erkennung von Schadcode, Signaturen oder Verhaltensmustern setzen, überwacht BullWall gezielt Dateien auf Netzwerkfreigaben sowie auf cloudbasierten Speicherorten wie Google Drive, Microsoft 365 (Teams Sites, SharePoint, OneDrive). Unautorisierte Verschlüsselungsaktivitäten werden dabei in Echtzeit erkannt und gestoppt. Zusätzlich kommen Indicators of Compromise (IOCs) zum Einsatz, um bekannte Bedrohungen frühzeitig zu identifizieren.

Der Fokus von BullWall liegt auf dem Ergebnis einer Veränderung – konkret darauf, ob eine Datei kompromittiert (z. B. verschlüsselt) wird oder nicht. Dadurch entsteht eine effektive Schutzschicht, die bestehende Sicherheitsmechanismen sinnvoll ergänzt und den Schutz von kritischen Datenbeständen erhöht.

BullWall im Zusammenspiel mit klassischen Sicherheitslösungen

BullWall versteht sich als sinnvolle Ergänzung zu etablierten Sicherheitslösungen wie EDR, XDR und NDR. Während diese Technologien Bedrohungen anhand von Verhaltensanalysen, Telemetriedaten und Netzwerkverkehr erkennen, setzt BullWall direkt auf der Dateiebene an und überwacht gezielt Dateien. Dadurch können auch Ausbrüche auf bisher unbekannten Ransomware-Typen erkannt, gestoppt und deren Auswirkungen verhindert werden – selbst dann, wenn die Verschlüsselung oder Exfiltration von Daten bereits begonnen hat.

Bestehende Lösungen bieten häufig keine verlässliche Erkennung von Ransomware und deren Auswirkungen. BullWall ergänzt diese Architektur gezielt und bietet zusätzlichen Schutz für Bereiche, die von klassischen Endpoint-Lösungen oft nicht erreicht werden. So entsteht ein ganzheitlicher und mehrschichtiger Schutz, der die Resilienz der gesamten IT-Infrastruktur erhöht.

Innovative Schutzmechanismen für moderne IT-Infrastrukturen

Moderne Sicherheitsarchitekturen sind bereits mehrschichtig aufgebaut und kombinieren verschiedene Lösungen wie z. B Firewall, EDR, XDR und NDR. BullWall ergänzt diese Schutzmechanismen durch spezialisierte Funktionen, die gezielt dort greifen, wo klassische Lösungen an ihre Grenzen stossen.

Als letzte Verteidigungsebene erkennt und blockiert BullWall aktive Verschlüsselungsversuche in Echtzeit und verhindert so den finalen Schaden, beispielsweise die Kompromittierung von Dateien.

- **Ransomware Containment (RC):** Innovativer, agentenloser Schutz – keine Installation auf Endpoints nötig. RC sichert automatisch kritische Infrastrukturen, insbesondere Dateien auf Dateifreigaben und in Cloud-Speichern.
- **Server Intrusion Protection (SIP):** Der SIP-Agent verhindert gezielt laterale Bewegungen innerhalb der Infrastruktur und erschwert damit das Ausspionieren durch Angreifer erheblich. Exfiltration von Daten oder die Vorbereitung weiterer Angriffe werden bereits im Vorfeld unterbunden. Auch Hyper-V-Umgebungen profitieren von diesem Schutz.
- **Virtual Server Protection (VSP):** Der VSP-Agent bietet gezielten Schutz für virtuelle Serverumgebungen (VMware), den Zugriff über SSH, die Überwachung von Systemprozessen sowie den Schutz der Verschlüsselung von Systemdateien und Daten der virtuellen Maschinen, einschliesslich der virtuellen Festplatten. Ransomware-Aktivitäten innerhalb virtualisierter Systeme werden erkannt und gestoppt, bevor sie Schaden anrichten können.
- **Sofortige Isolation:** Erkennt BullWall eine Ransomware-Aktivität, wird die kompromittierte Benutzer-ID oder das betroffene Gerät automatisch isoliert – bevor sich die Verschlüsselung ausbreiten kann.
- **Nahtlose Integration:** BullWall lässt sich über REST/JSON-APIs problemlos in das bestehende IT-Sicherheits-Ökosystem (wie EDR/XDR/NDR, SIEM oder NAC) integrieren und ergänzt deren Vorfallmanagement durch Echtzeit-Containment.

Fazit

BullWall ergänzt moderne Sicherheitsarchitekturen als innovative „Last Line of Defense“. Die Lösung schützt agentenlos mit RC automatisch kritische Infrastrukturen wie Dateien auf Dateifreigaben und in Cloud-Speichern. Mit SIP wird die Ausbreitung von Angriffen durch die gezielte Verhinderung lateraler Bewegungen und Datenexfiltration innerhalb der Infrastruktur erschwert. VSP bietet spezialisierten Schutz für VMware-basierte Systeme und erkennt Ransomware-Aktivitäten frühzeitig. Durch die Assume-Breach-Mentalität, die nahtlose Integration und die gezielten Schutzfunktionen erhöht BullWall die Resilienz der gesamten IT-Umgebung und sorgt dafür, dass kritische Daten zuverlässig geschützt werden. Damit ist BullWall eine wertvolle Ergänzung für ein ganzheitliches Sicherheitskonzept.