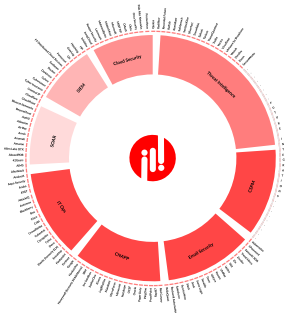


METRON'S PORTFOLIO OF SECURITY INTEGRATIONS

THIRD-PARTY SECURITY INTEGRATIONS SUPPORTED BY METRON



METRON ADVANTAGE



Fully Managed

Complete oversight on the end-to-end process of development, customization, app certification, and continued on-demand support.



Streamlined

Avian Security maintains coding standards, merges PRs, and coordinates with the security teams for all updates.



Abstract

Get started within 24 hours with up to 2x-3x cost savings compared to in-house.



Zero Risk

Fried cost and no
upfront payment.
Invoiced only after
delivery.

AbuseIPDB

AbuseIPDB

Category: TIP

AbuseIPDB is a project dedicated to helping combat the spread of hackers, spammers, and abusive activity on the Internet. It offers a central blacklist for webmasters, system administrators, and other interested parties to report and find IP addresses that have been associated with malicious activity online.

AIMS

AIMS

Category: CISM

AIMS 3 is a scalable, web-based CISM software made up of a variety of core components, optional components, and interfaces that provide solutions to meet the needs of your current operation and your needs in the future. With AIMS, users can access all aspects of their maintenance operation from any location with Internet access, at any time.

Integrations: Palo Alto Networks - IoT, Palo Alto Networks - Cortex XSOAR (formerly Demisto)

AlienVault

AlienVault

Category: SIEM

Open Threat Exchange is the neighborhood watch of the global intelligence community. It enables private companies, independent security researchers, and government agencies to openly collaborate and share the latest information about emerging threats, attack methods, and malicious actors, promoting greater security across the entire community.

Integrations: Devco

AT&T

AT&T Alien Labs

Category: TIP

AT&T Alien Labs is the threat intelligence unit of AT&T Cybersecurity that delivers tactical threat intelligence that powers resilient threat detection and response — even as your IT systems evolve and adversaries change their tactics, techniques, and procedures (TTPs).

AT&T USM Anywhere

Category: SIEM, Cloud Security

USM Anywhere centralizes security monitoring of networks and devices in the cloud, on premises, and in remote locations, helping you to detect threats virtually anywhere.

Integrations: SentinelOne

Aqua Security

Aqua Security

Category: CNAPP

Aqua Security Platform is a Cloud Native Application Protection Platform (CNAPP) built to safeguard cloud-native applications throughout their entire lifecycle, from code to cloud and back. It's a highly integrated platform that addresses the unique security challenges posed by containerized, serverless, and cloud-based applications.

Armis

Armis

Category: IoT Security, OT Security, MSS, CPS Protection Platform, ITSM

Armis Central, the cyber exposure management platform, is powered by its AI-driven Asset Intelligence Engine, which sees, secures, protects and manages billions of assets around the world in real time.

Integrations: Palo Alto Networks - IoT, SentinelOne, IBM QRadar, AWS Security Lake

Aruba

01 | Aruba Central

Category: Enterprise Wired and Wireless LAN Infrastructure

Aruba Central is a cloud-based networking solution that empowers IT with AI-powered insights, intuitive visualizations, workflow automation, and edge-to-cloud security to manage campus, branch, remote, data center, and IoT networks from one dashboard.

Integrations: Palo Alto Networks - IoT, Palo Alto Networks - Cortex XSOAR (formerly Demisto)

02 | Aruba ClearPass

Category: NAC, Enterprise Wired and Wireless LAN Infrastructure

Aruba Networking ClearPass for Zero Trust Security helps to authenticate, authorize, and enforce secure network access control with role-based network policies based on Zero Trust Security.

Alien Labs OTX

Alien Labs OTX

Category: SIEM

Open Threat Exchange (OTX) is a threat data platform that allows security researchers and threat data producers to share research and investigate new threats.

Amazon

01 | [Amazon GuardDuty](#)

Category: TP

GuardDuty combines ML and integrated threat intelligence from AWS and leading third parties to help protect your AWS accounts, workloads, and data.

Integrations: SentinelOne, SentinelOne UEM, SentinelOne SCV, Sema4 XDR

02 | [Amazon Security Lake](#)

Category: Data Lake

Amazon Security Lake automatically centralizes security data from AWS environments, SaaS providers, on premises, and cloud sources into a purpose-built data lake stored in your account.

Integrations: Palo Alto Networks - IoT, SentinelOne

03 | [AWS AppFabric](#)

Category: IT Ops

AppFabric connects SaaS applications across your organization. IT and security teams can then easily manage and secure applications using a standard schema, and employees can complete everyday tasks faster using generative AI.

Integrations: SentinelOne

04 | [AWS CloudTrail](#)

Category: GPS

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and cost auditing of your AWS account.

05 | [AWS CloudWatch](#)

Category: APM

Amazon CloudWatch is a service that monitors applications, responds to performance changes, optimizes resource use, and provides insights into operational health. By collecting data across AWS resources, CloudWatch gives visibility into system-wide performance and allows users to set alarms, automatically react to changes, and gain a unified view of operational health.

Integrations: SentinelOne

06 | [AWS S3 Bucket](#)

Category: Public Cloud Storage Service

Amazon Simple Storage Service (Amazon S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. S3 is built to store and retrieve any amount of data from anywhere.

Integrations: SentinelOne

07 | [AWS Security Hub](#)

Category: CSRM

AWS Security Hub allows you to automate security best practice checks, aggregate security alerts into a single place and format, and understand your overall security posture across all of your AWS accounts.

Integrations: SentinelOne

Amazon

08 | [AWS ELB](#)

Category: Application Delivery Controllers (ADC)

AWS ELB is a load balancing service within Amazon Web Services (AWS) that distributes incoming traffic across multiple servers to ensure high availability and scalability of applications.

Integrations: SentinelOne

09 | [Amazon DynamoDB](#)

Amazon DynamoDB is a serverless, NoSQL, fully managed database with single-digit millisecond performance at any scale.

Integrations: JupiterOne

10 | [AWS Systems Manager](#)

AWS Systems Manager is the operations hub for AWS applications and resources and a secure end-to-end management solution for hybrid and multicloud environments that enables secure operations at scale.

Integrations: JupiterOne

11 | [AWS Network Firewall](#)

AWS Network Firewall provides fine-grained control over network traffic with customizable firewall rules. Integrated with AWS Firewall Manager, it centralizes security across VPCs for better protection.

Integrations: JupiterOne

12 | [Amazon Relational Database Service](#)

Amazon RDS simplifies database management with automated provisioning, scaling, and backups. It supports multiple engines and offers advanced features for performance optimization and cost management.

Integrations: SentinelOne

Anomali

[Anomali](#)

Category: SIEM, SOAR

The Anomali platform is a cloud-native security operations platform (SOP) designed to improve visibility, threat detection, and response for organizations. It tackles security with a powerful combination of analytics, intelligence, automation, and AI.

ArcSight

[ArcSight](#)

Category: SIEM, SOAR

ArcSight is a cybersecurity product that provides big data security analytics and intelligence software for security information and event management (SIEM) and log management.

Integrations: Cybermasson CEF Forwarder

At-Bay

At-Bay

Category: EPP

By combining insurance with security into one, At-Bay brings the incentives, scale, and expertise needed to bridge the SaaS (Server Message Block) cyber security gap.

Integrations: GSuite, CrowdStrike Zero Trust

Atlassian

01 | Atlassian JIRA (on-prem)

Category: IT Ops

Atlassian JIRA (on-prem) is a project management and issue tracking software deployed and managed within your own IT infrastructure.

Integrations: JupyterOne

02 | Atlassian JIRA Forge (cloud)

Category: IT Ops

Atlassian Forge (Cloud) is a platform for developers to build and deploy add-ons and apps for both Jira and Confluence. It provides developers with the tools and infrastructure needed to create, test, and distribute their applications to users in the Atlassian ecosystem.

Integrations: JupyterOne

03 | JIRA ServiceDesk Template

Category: IT Ops

Jira Service Management (JSM) is a comprehensive service desk and IT service management (ITSM) solution built on top of the popular Atlassian Jira platform. It's designed to help organizations streamline their service delivery processes, improve customer satisfaction, and meet ITSM best practices.

Integrations: Jira

AttackIQ

AttackIQ

Category: Breach and Attack Simulation (BAS)

AttackIQ is a cybersecurity platform designed to help organizations simulate and measure their ability to withstand cyberattacks. It blends a range of technologies and approaches, such as Purple Teaming, Threat Library, etc., to create a comprehensive security validation solution.

Box

Box

Category: Collaboration platform

Box is a cloud-based content management and collaboration platform that prioritizes security to protect sensitive data and ensure compliance.

Integrations: Workio

Auth0

Auth0

Category: Access Management

Auth0 identity platform helps to add sophisticated authentication and authorization to your applications. It allows you to centralize and manage users from multiple identity providers and give them branded, seamless sign-up and login experiences.

BeyondTrust

BeyondTrust

Category: OT Security, Access Management

BeyondTrust is a comprehensive privileged access management (PAM) platform that helps organizations protect their most sensitive assets by securing, managing, and auditing privileged accounts and access.

Integrations: SentinelOne

Bluecat Networks

Bluecat IPAM

Category: IPAM

Bluecat IPAM (IP Address Management) is a comprehensive software platform designed to help organizations manage and optimize their IP address space. It offers a wide range of features and benefits, making it a valuable tool for businesses of all sizes.

Integrations: Palo Alto Networks - IoT

CheckPoint

01 | CheckPoint

Category: OT Security

Check Point provides comprehensive cybersecurity solutions that protect organizations from attacks across networks, endpoints, cloud, mobile, and IoT devices. It offers a wide range of products and services that address various aspects of cybersecurity.

02 | CheckPoint SandBlast

Category: OT Security

Check Point SandBlast is a comprehensive suite of security solutions designed to protect organizations against advanced threats, zero-day attacks, and targeted malware. It offers multiple layers of protection, including network, endpoint, and cloud-based defenses.

03 | CheckPoint Firewall

CheckPoint's Quantum Firewalls offer advanced network security with features like remote access VPN, SASE, and SD-WAN, defending against IoT, DDoS, and Zero Day attacks.

Integration: SentinelOne

Cisco

01 | Cisco Duo

Category: Access Management

Cisco Duo is a cloud-based multi-factor authentication (MFA) solution that helps organizations improve their security posture by adding an extra layer of protection to access control. It goes beyond traditional password-based authentication by requiring users to provide a second factor of verification, making it significantly harder for attackers to gain unauthorized access.

Integrations: SentinelOne

02 | Cisco Firepower

Category: Network Firewall

Cisco Firepower is a comprehensive suite of next-generation firewall (NGFW) and security solutions from Cisco, designed to protect your network against various cyber threats.

03 | Cisco Meraki

Category: Enterprise Wired and Wireless LAN Infrastructure (WLAN)

Cisco Meraki allows you to configure security for Internet-connected devices, routers, switches, firewalls and WiFi networks your company uses through an Internet-connected browser.

Integrations: Palo Alto Networks - IoT, Samsung XDR

04 | Cisco Secure Email

Category: Email Security

Cisco Secure Email, formerly known as Cloud Email Security, is a cloud-based email security solution designed to protect your organization from sophisticated phishing attacks, ransomware, and other email-borne threats.

Integrations: Times

05 | Cisco Secure Endpoints

Category: EPP

Cisco Secure Endpoint is a cloud-delivered endpoint protection platform (EPP) that safeguards your organization's devices against a wide range of cyberthreats. It combines prevention, detection, and response capabilities to protect Windows, macOS, Linux, iOS, and Android devices from malware, ransomware, phishing attacks, zero-day exploits, and other sophisticated threats.

Integrations: Times

06 | Cisco Umbrella

Category: DLP

Cisco Umbrella is a cloud-delivered security platform that offers comprehensive protection against threats at the DNS (Domain Name System) and IP (Internet Protocol) layers. It acts as a first line of defense, blocking threats before they reach your network or endpoints, and provides broad visibility and control over internet access.

Integrations: Times

Cisco

07 | Cisco WLC

Category: Enterprise Wired and Wireless LAN Infrastructure

Cisco WLC, which stands for Wireless LAN Controller, plays a crucial role in managing and orchestrating Cisco wireless access points (APs) within a network. It's the brain behind the operation, providing centralized control, security, and optimization for your Wi-Fi environment.

Integrations: Palo Alto Networks - IoT

ArmorBlox

ArmorBlox

Category: DLP, Email Security

ArmorBlox uses the latest techniques in machine learning (ML) and artificial intelligence (AI) to protect organizations against identity-based attacks and data loss.

Integrations: SentinelOne

Cloudflare

Cloudflare

Category: Email Security, Cloud Infrastructure and platform services (CIPS) [Strategic Cloud Platform Services]

Cloudflare is a cloud-based web performance and security tool, which helps firms, in the public and private sectors with protection and speed acceleration of websites applications, and other internet services against hackers.

Cribl

Cribl

Category: Event Stream Processing

Cribl is a data observability and processing platform that empowers organizations to control, optimize, and secure their observability data at scale. It helps make observability data more usable, cost-effective, and secure for security analytics, IT operations, and DevOps teams.

Integrations: Times

Criminal IP

Criminal IP

Category: TIP

Criminal IP is a Cyber Threat Intelligence (CTI) search engine that scans the Internet for open ports and devices to discover and track potentially malicious IP addresses and domains. It aims to provide insights into potential threats and vulnerabilities, helping individuals and organizations make informed security decisions.

Integrations: SentinelOne, Times

CrowdStrike

01 | CrowdStrike Falcon Endpoint

Category: EPP

CrowdStrike Falcon Endpoint is a cloud-based endpoint protection platform (EPP) that safeguards your devices against a wide range of cyber threats. It combines innovative prevention, detection, and response capabilities to protect endpoints like laptops, desktops, servers, and mobile devices from malware, ransomware, phishing attacks, zero-day exploits, and advanced threats.

Integrations: DevOps

02 | CrowdStrike Falcon Intel

Category: TIP

CrowdStrike Falcon Intel is a comprehensive threat intelligence platform that goes beyond just data collection. It offers actionable insights and proactive threat hunting capabilities to empower security teams in preventing and mitigating cyberattacks.

03 | CrowdStrike Zero Trust

CrowdStrike Zero Trust secures any device, user, or workload by continuously verifying access and stopping breaches in real-time across your cloud and on-premise network.

Integrations: AI-Guy

CyberArk

01 | CyberArk

Category: OT Security, Access Management

CyberArk offers enterprise identity security platform, protecting identities and critical assets by enabling zero trust and enforcing least privileges.

02 | CyberArk EPM

Category: Access Management

CyberArk Endpoint Privilege Manager (EPM) helps remove local admin rights while improving user experience and optimizing IT operations.

Integrations: SentinelOne

Cybereason

01 | Cybereason

Category: SOC, MDR, EDR, EPP

The Cybereason Defense Platform is a unified security platform that goes beyond traditional endpoint protection and detection by offering automated breach prevention, advanced detection, and comprehensive response capabilities.

Integrations: Splunk, ServiceNow SecOps, SDK Osta, SDK ZScaler, ServiceNow ITSM, K50AR, Forwarder, Sandbox, SOC-Google, Forwarder_AggsFlow, HashingSandbox, Splunk AddOn, SDK Oracle, SOC_NetScope, Analytics Dashboard, BM Orusar, Splunk SOAR (Formerly Phantom), BM SOAR (Formerly Resilient), Splunk ES, Cybereason SDK

Cybereason

02 | Cybereason CEF Forwarder

Category: IT Ops

A Cybereason CEF (Common Event Format) forwarder is a tool or module designed to forward security event data in the Common Event Format to a centralized logging or security information and event management (SIEM) system for analysis and correlation. This helps organizations to monitor and respond to security incidents effectively by aggregating and analyzing data from various sources within their IT environment.

Integrations: Arcsight, Cybereason

03 | Cybereason XDR

Category: XDR

Cybereason XDR predicts, understands, and ends cyber attacks by fusing varied telemetry sources into visual attack stories: MalOps Intelligence operations.

Integrations: NetScopes, Palo Alto Networks - Prisma Cloud, Microsoft Defender for Endpoint, Microsoft Entra ID, GCP Security Command Center, Google Workspace (Formerly G Suite), OPSRAT MetaDefender IT Access

04 | Cybereason EDR

Category: EDR

Cybereason EDR is an endpoint detection and response (EDR) solution designed to protect organizations from advanced cyber threats. It leverages advanced analytics, artificial intelligence, and machine learning to provide comprehensive visibility and real-time response capabilities.

Integrations: Google SecOps (Formerly Google Chronicle), Cybereason

Cyber Insurance

Cyber Insurance

Category: TIP

Cyberinsurance is a contract an entity can purchase to help reduce the financial risks associated with doing business online. In exchange for a monthly or quarterly fee, the insurance policy transfers some of the risks to the insurer.

Integrations: SentinelOne

Cycognito

Cycognito

Category: External Attack Surface Management (EASM)

Cycognito tackles a crucial yet often overlooked aspect of cybersecurity: understanding your external attack surface. Imagine it as a comprehensive threat map of everything attackers could potentially target - websites, apps, misconfigured resources, exposed data, and even forgotten assets.

Cylera

Cylera

Category: CPS Protection Platform

Cylera provides a platform for IoT security and intelligence, aiming to improve data richness, security strength, and response times for organizations. This can help protect critical assets, including people, data, privacy, and business continuity.

Integrations: IBM QRadar

Cylus

Cylus

Category: CPS Protection Platform

Cylus, also known as CylusOne, is a specialized cybersecurity platform designed to protect operational technologies (OT) used in critical infrastructure sectors like rail, energy, and water treatment. Unlike traditional IT security solutions, Cylus understands the unique characteristics and vulnerabilities of OT systems, offering targeted protection against cyberattacks specifically targeting these environments.

Integrations: ServiceNow

Darktrace

Darktrace

Category: NDR, OT Security, CPS Protection Platform, Email Security

Darktrace addresses the challenge of insider threat and advanced cyber-attacks through its unique ability to detect previously unidentified threats in real time, as manifested in the emerging behaviors of the network, devices and individuals.

Integrations: Safelinx

Devo

Devo

Category: SIEM, SOAR

Devo platform enables security and operations teams to address common use cases including centralized logging, SIEM, compliance, fraud detection, and more. The platform includes tightly integrated applications for security and IT teams.

Integrations: ServiceNow App, Malwarebytes, Cyren Protect, Ws, Autotomx, Microsoft Defender, MS 365 Defender Incident, Oracle Cloud Logs, ThreatStack, JumpCloud, HackerOne, SumoLogic, Snowflake, Tails, GitHub, CrowdStrike, AlienVault, Veritas, Salesforce, MS-Office 365, MS 365 Defender, MS-Defender for Cloud-Apps, Tanium, SumoLogic, CrowdStrike Falcon Endpoint, Threat Quotient, Data, T433, Malwarebytes Nebula, Microsoft Defender for Endpoint, Microsoft Defender For Cloud Apps, Slack, XSOAR

F5 Distributed Cloud Services

F5 Distributed Cloud App Infrastructure Protection (AIP)

Category: CNAPP

ThreatStack is a Cloud Security Platform (CSP) designed to protect cloud-native applications and infrastructure from cyber threats. It provides comprehensive visibility, threat detection, and response capabilities across multi-cloud environments, including AWS, Azure, and Google Cloud.

Docker

Docker

Category: Application platform, Container management

Docker provides a suite of development tools, services, trusted content, and automations, used individually or together, to accelerate the delivery of secure applications.

Integrations: Times

Elastic (formerly ELK)

Elastic (formerly ELK)

Category: SIEM, EDR, EPP

The Elastic Stack, also known as the ELK Stack, is a powerful and open-source platform for searching, analyzing, and visualizing data of all shapes and sizes.

Integrations: HP

Exabeam

Exabeam

Category: SIEM

Exabeam provides a cloud-native architecture for rapid data ingestion, hyper-quick query performance, powerful behavioral analytics for next-level insights that other tools miss, and automation that changes the way analysts do their jobs.

ExtraHop

ExtraHop

Category: NDR

ExtraHop is a network detection and response (NDR) platform that provides deep visibility and insights into your network traffic, helping you uncover threats, prevent breaches, and ensure the performance and security of your IT environment.

Integrations: SentinelOne

Flashpoint

Flashpoint

Category: TIP

Flashpoint is a cybersecurity platform developed by Palo Alto Networks. It offers threat intelligence, investigation, and response capabilities, helping organizations identify and mitigate cyber threats.

Integrations: SentinelOne, AbuseIPDB, Google Workspace (formerly G Suite)

ForeScout

ForeScout

Category: NAC, OT Security, IoT Security, GPS Protection Platform

ForeScout is a powerful network security and asset management platform designed to discover, classify, manage, and secure all connected devices within your organization's network, including IT, IoT, k/MT, and OT assets. It helps you stay ahead of evolving cyber threats and maintain compliance with security regulations.

Integrations: ServiceNow App, MalwareBytes, Cylance Protect, Ws, Antivirus, Microsoft Defender, MS 365 Defender Incident, Oracle Cloud Logs, ThreatStack, JumpCloud, HackerOne, SunMIDM, Snowflake, Teal, GitHub, CROWDStrike, AlienVault, Veem, Salesforce, MS Office 365, MS 365 Defender, MS Defender for Cloud-Apps, Tanium, SunMIDM, CrowStrike Falcon Endpoint, Threat Quantum, Ota, TAP, Netula, Microsoft Defender for Endpoint, Microsoft Defender For Cloud Apps, Slack, iSCAR, SentinelOne - Deep Visibility

Fortinet

01 | FortiAnalyzer

Category: SOAR

FortiAnalyzer is a log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, enabling simplified security operations, proactive identification and remediation of risks, and complete visibility of the entire attack landscape.

02 | FortiGate Cloud

Category: Enterprise Wired and Wireless LAN Infrastructure

FortiGate Cloud or FortiCloud is a robust cloud-based management and security analytics platform offered by Fortinet, designed to simplify the provisioning, configuration, and management of your FortiGate NGFWs and SD-WAN devices. It caters to both small and medium-sized businesses (SMBs) and Managed Service Providers (MSPs).

Integrations: SentinelOne, SentinelOne - Purple AI

Fortinet

03 | FortiManager

Category: IT Ops

FortiManager enables centralized management with automation-driven network configuration, visibility, and security policy management.

Integrations: SentinelOne

04 | Fortinet NGFW

Category: Network Firewall

Fortinet's NGFW platform offers a comprehensive suite of security solutions designed to protect organizations against a wide range of threats. It's a cornerstone of Fortinet's Security Fabric, a cybersecurity mesh architecture that integrates multiple security elements to create a collaborative and adaptive defense system.

Integrations: Honeywell (Formerly SCADA/Secops)

05 | Fortinet Security Fabric

Category: SIEM

Fortinet Security Fabric is a comprehensive cybersecurity platform that aims to create a broad and integrated defense system across an organization's entire digital infrastructure. It goes beyond traditional standalone security solutions by weaving together multiple security elements—including firewalls, intrusion prevention systems (IPS), endpoint protection, cloud security, and more—into a cohesive and adaptive fabric.

06 | FortiOS

Category: Enterprise Wired and Wireless LAN Infrastructure

FortiOS ties all the Security Fabric's security and networking components together to ensure seamless integration. This enables the convergence of networking and security functions to deliver a consistent user experience and resilient security posture across all manner of environments including on-premises, cloud, hybrid, and converging IT/OT/IoT infrastructure.

07 | FortiSIEM

Category: SIEM

FortiSIEM delivers powerful security information and event management (SIEM) with user and entity behavior analytics (UEBA). It is the backbone of your security operations team, delivering capabilities ranging from automatically building your inventory of assets to applying cutting-edge behavioral analytics to rapidly detect and respond to threats. FortiSIEM is the industry's only security operations platform with a fully robust configuration management database (CMDB).

Integrations: SentinelOne

08 | FortiSOAR

Category: SOAR

FortiSOAR helps IT/OT security teams thwart attacks by centralizing incident management and automating the myriad of analyst activities required for effective threat investigation and response. Using FortiSOAR as a central operations hub to standardize and accelerate these workflows enforces best practices and allows analysts to focus on what matters most to protect the organization.

Git

01 | [GitHub](#)

Category: Enterprise Agile Planning, Application security testing (AST)

GitHub is a powerful online platform for software development and project management that has become the central hub for millions of developers and organizations around the globe. It offers a suite of features designed to streamline collaboration, version control, and code management.

Integrations: Devs

02 | [GitLab](#)

Category: Enterprise Agile Planning, Application security testing (AST)

GitLab is a comprehensive open-source DevOps platform that provides a full suite of tools for software development, project management, and operations. It aims to streamline the entire software development lifecycle, from planning and coding to testing, deployment, and monitoring.

Integrations: Trello

Google

01 | [GCP Security Command Center](#)

Category: Cloud Infrastructure and platform services (CIPS) (Strategic Cloud Platform Services)

Google Cloud Security Command Center (SCC) is a centralized security and risk management platform for Google Cloud Platform (GCP). It provides comprehensive visibility into your GCP resources, helps you identify and prioritize security risks, and enables you to take action to mitigate these risks.

Integrations: JupiterOne, Cyberason XDR, Palo Alto Networks - Big Security, SentinelOne

02 | [Google BigQuery](#)

Category: Cloud Database

BigQuery is a powerful, serverless, and highly scalable cloud-based data warehouse offered by Google Cloud Platform (GCP). It allows organizations to analyze massive datasets and extract insights in a fast and efficient manner.

03 | [Google SecOps](#)

Category: SIEM

Chronicle is a cloud-native data ingestion, analysis, and search platform designed for cybersecurity teams to investigate and respond to threats more effectively. It sits at the core of Google Cloud's security offerings, empowering analysts with unparalleled speed, scale, and precision in handling security incidents.

Integrations: Bloodhound, Doppel

04 | [Google Cloud Storage](#)

Category: Public Cloud Storage Service

Google Cloud Storage (GCS) is a highly scalable and reliable object storage service offered by Google Cloud Platform (GCP). It allows you to store any type of data, from small files to massive datasets, in a secure and durable manner. GCS delivers exceptional performance, flexibility, and cost-effectiveness, making it ideal for a wide range of use cases.

Integrations: Times

Google

05 | [Google Workspace \(formerly GSuite\)](#)

Category: Collaboration Platform

Google Workspace is a cloud-based suite of productivity and collaboration tools designed to help individuals, teams, and organizations work together more effectively. It offers a variety of integrated applications that can be accessed from anywhere with an internet connection, making it ideal for remote and hybrid work environments.

Integrations: SentinelOne, Cyberason XDR

06 | [GCP VPC Flow Logs](#)

Category: Cloud Security

GCP VPC Flow Logs are logs that record all network traffic entering and leaving Google Cloud Platform (GCP) Virtual Private Clouds (VPCs), providing detailed information about network activity and potential security concerns.

Integrations: SentinelOne

07 | [GCP Audit Logs](#)

Category: Cloud Security

GCP Audit Logs are logs that record system events and user actions within GCP resources, offering a comprehensive audit trail for security analysis and compliance purposes.

Integrations: SentinelOne

GrayLog

[GrayLog](#)

Category: SIEM

Graylog provides answers to your team's security, application, and IT infrastructure questions by enabling you to combine, enrich, correlate, query, and visualize all your log data in one place.

Integrations: Times

HackerOne

[HackerOne](#)

Category: Application Crowdttesting Services

HackerOne is a leading bug bounty platform and vulnerability disclosure platform (VDP) that connects organizations with a global community of ethical hackers, also known as "white hat hackers." It facilitates a secure and collaborative environment for organizations to discover and remediate security vulnerabilities in their software, systems, and infrastructure.

Integrations: Devs

Honeywell (formerly SCADAfence)

Honeywell (formerly SCADAfence)

Category: OT Security, CPS Protection Platform

SCADAfence secures industrial networks by acting as a cybersecurity guardian protecting against threats and optimizing operations.

Integrations: Fortinet NGFW, PaloAlto, Splunk, Splunk OT, Splunk Enterprise Security (ES), IBM QRadar, ServiceNow - Service Graph Connectors, ServiceNow Security Incident Response (SIR)

HP

HP

Category: EPP

HP Inc. develops personal computers, printers and related supplies, as well as 3D printing services.

Integrations: Splunk OT, Elastic (formerly ELK)

IBM

01 | IBM QRadar

Category: SIEM

IBM QRadar is a leading Security Information and Event Management (SIEM) platform that helps organizations monitor their IT infrastructure for security threats and incidents. It analyzes and correlates data from various sources, including network devices, security appliances, servers, applications, and cloud platforms, providing a unified view of your security posture.

Integrations: Wg, Cyberason, Safebreach, Zscaler, Digital Shadows, VMware CarbonBlack, SentinelOne, Armita

02 | IBM SOAR (formerly Resilient)

Category: SOAR

IBM Security QRadar SOAR with Resilient Orchestration (often referred to simply as IBM SOAR Resilient) is a comprehensive Security Orchestration, Automation, and Response (SOAR) platform designed to empower security teams in streamlining incident response workflows and improving their efficiency.

Integrations: Cyberason, Digital Shadows

Joe Sandbox

Joe Sandbox

Category: Security Solutions

A cloud-based platform for malware analysis and threat detection. It provides organizations with tools to analyze suspicious files and URLs for malicious behavior, helping them identify and mitigate potential threats.

JumpCloud

JumpCloud

Category: Security Solutions

JumpCloud's open directory platform makes it possible to unify your technology stack across identity, access, and device management, in a cost-effective manner that doesn't sacrifice security or functionality.

Integrations: Civo

JupiterOne

JupiterOne

Category: CAASM, ITRM

JupiterOne helps organizations gain holistic visibility and control over their entire cyber asset attack surface. It empowers security teams to identify, prioritize, and manage security risks across all IT assets, including devices, cloud resources, code repositories, users, and more.

Integrations: Checkpoint, Armita, CyberArk EPM, Trend Micro Cloud One, CyberArk Adaptive, Symantec Endpoint, MS Azure, GCP Security Command Centre, Oracle Cloud Infrastructure, Kubernetes, ServiceNow, Atlassian Jira Forge (cloud), CrowdStrike, Tenable Vulnerability Management (formerly Tenate.io), SonarQube, Gwyls, ZenDesk, Snowflake, Amazon DynamoDB, J-Frog - Artifactory, Thred Micro vision One, Confluent Cloud, ABB Network Firewall, OCI Cloud Guard, Atlassian Jira (on-prem), ServiceNow, Secaneorks Taegis XDR

Kivera

Kivera

Category: Cloud Security Protection Platforms (CSPP)

Kivera is a cloud-based platform designed to inspect and monitor APIs for security vulnerabilities and potential threats. It provides comprehensive visibility into your API environment, helping organizations secure their APIs and prevent unauthorized access, data breaches, and other security incidents.

Lacework

Lacework

Category: CNAPP, CSPM

Lacework offers a data driven CNAPP platform that correlates data from across your cloud to keep your environment safe. It automatically makes sense of all your cloud data and uses it to better protect your entire environment — from build time through runtime.

MalwareBytes

01 | MalwareBytes

Category: EDR, MDR, EPP

MalwareBytes Business Platform is an all-in-one cybersecurity solution for businesses, protecting against a wide range of threats on endpoints, networks, and identities.

Integrations: Devs, SentinelOne, Tines

02 | MalwareBytes Nebula

Category: SIEM, TIP, EDR, XDR, MDR

A cloud-hosted security platform that maximizes limited resources, covering ThreatDown Endpoint Protection, EDR, and MDR solutions.

Integrations: Devs

MatterMost

MatterMost

Category: Collaboration platform

Mattermost is an open-source, self-hosted messaging platform designed for secure and efficient collaboration within organizations. It offers a robust set of features and capabilities that make it a compelling alternative to proprietary messaging tools like Slack or Microsoft Teams.

Integrations: Tines

Mandiant

Mandiant

Category: SIEM, SOCs, SOAR, MDR, EDR

The Mandiant platform, known as Mandiant Advantage, is a multi-vendor XDR (Extended Detection and Response) platform and cybersecurity intelligence product combined. It's designed to help organizations of all sizes detect, investigate, and respond to sophisticated cyber threats more effectively.

Integrations: SentinelOne

Microsoft

01 | Azure Blob

Category: Public Cloud Storage Service

Azure Blob Storage is Microsoft's object storage solution for the cloud. It's designed to store massive amounts of unstructured data in a highly scalable and cost-effective way.

Microsoft

02 | Microsoft Azure Event Hub

Category: CDP

Microsoft Azure Event Hubs is a fully managed, real-time data ingestion service that can collect massive amounts of data from various sources and process them in a scalable and reliable manner. It's designed for high-volume and high-throughput scenarios, making it ideal for handling streams of data from devices, sensors, websites, applications, and more.

Integrations: SentinelOne

03 | Microsoft Defender for Cloud Apps

Category: Security Service Edge

Defender for Cloud Apps is a Cloud Access Security Broker (CASB) from Microsoft, protecting your organization against cloud app risks and threats. It acts as a gatekeeper, monitoring and controlling data flow between your users and cloud apps.

Integrations: Devs

04 | Microsoft Defender for Endpoint

Category: EDR, EPP

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

Integrations: Devs, Cyberason XDR

05 | Microsoft Defender for Identity

Category: Insider Risk Management Solutions

Microsoft Defender for Identity helps protect your organization's on-premises identities from advanced threats and manage identity risk.

06 | Microsoft Entra ID (Azure AD)

Category: Access Management

With Microsoft Entra ID (formerly called Azure AD), you can safeguard your organization with a cloud identity and access management solution that connects employees, customers, and partners to their apps, devices, and data.

Integrations: SentinelOne, Palo Alto Networks - IoT, Palo Alto Networks - Cortex XSOAR (formerly Demisto), Keeper Security

07 | Microsoft EventHub - Email Defender

Category: Email Security

Microsoft Event Hub - Email Defenses refers to a feature or service provided by Microsoft within its ecosystem, likely aimed at enhancing email security. This could involve analyzing email traffic, detecting and mitigating threats such as phishing attempts, malware, or spam, and providing insights or alerts to administrators for proactive defense measures.

Integrations: SentinelOne

08 | Microsoft Intune

Category: Unified Endpoint Management (UEM)

Microsoft Intune is a cloud-based endpoint management solution that enables organizations to manage, secure, and configure devices used by their employees, including mobile devices, laptops, desktops, and virtual machines.

Integrations: SentinelOne

Microsoft

09 | Microsoft PowerBI

Category: Analytics and business intelligence (ABI) platform

Microsoft Power BI is a business intelligence (BI) platform that allows you to connect to, visualize, analyze, and share data to gain meaningful insights and make data-driven decisions. It offers a suite of tools and features designed to make data exploration and comprehension accessible for both technical and non-technical users.

10 | Microsoft SCCM

Category: IT Ops

Microsoft SCCM stands for System Center Configuration Manager. It's a comprehensive management solution used by IT professionals to deploy, manage, and update devices and applications within an organization's network. SCCM enables centralized control over software distribution, patch management, operating system deployment, and inventory tracking across a wide range of devices, including desktops, laptops, servers, and mobile devices.

Integrations: Palo Alto Networks - IoT, Palo Alto Networks - Cortex XSOAR (formerly Demisto)

11 | Microsoft Sentinel

Category: SIEM, SOAR

Formerly known as Azure Sentinel, Microsoft Sentinel is a cloud-native security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution that empowers organizations to collect, analyze, and respond to security threats across their entire IT environment.

Integrations: Digital Shadows, Sema4 XDR

12 | Microsoft Teams

Category: Collaboration Platform

Microsoft Teams is a cloud-based collaboration platform that goes beyond simple messaging. It acts as a central hub for teams and organizations to communicate, collaborate, and manage projects efficiently.

Integrations: SentinelOne, Votio

13 | MS 365 Defender

Category: SIEM, EDR, NDR, XDR

Microsoft 365 Defender stands as a comprehensive cloud-based security platform within the Microsoft 365 ecosystem, designed to safeguard your organization from advanced cybersecurity threats across various attack vectors.

Integrations: SentinelOne, Devs

14 | MS Office 365

Category: Collaboration platform

Microsoft Office 365, often referred to as simply Office 365, is a comprehensive, cloud-based suite of productivity applications and services designed to empower individuals and organizations to create, collaborate, and communicate more effectively.

Integrations: SentinelOne, Devs, SentinelOne - Purple AI, Sema4 XDR

Microsoft

15 | MS Azure

Category: Cloud infrastructure and platform services (IaaS) (Strategic Cloud Platform Services)

Microsoft Azure, often simply referred to as Azure, is a comprehensive, public cloud computing platform that offers a wide range of services and resources to help organizations build, deploy, and manage applications and services over the internet. It provides a flexible, scalable, and cost-effective platform for a vast array of IT needs, from simple web hosting to complex enterprise solutions.

Integrations: Wotio, Digital Shadows, JupiterOne

16 | Microsoft Defender XDR

Category: XDR

Microsoft Defender XDR is an Extended Detection and Response (XDR) platform from Microsoft that offers comprehensive threat detection, investigation, and response capabilities across endpoints, cloud workloads, and identities.

Integrations: Palo Alto Networks - IoT

Mimecast

Mimecast

Category: Enterprise Information Archiving

Mimecast's platform is a multi-layered cloud-based cybersecurity solution specifically designed to protect organizations from email-borne threats and enhance email security. It acts as a comprehensive shield for your email environment, offering numerous features that work together to safeguard your data, maintain business continuity, and empower efficient email management.

Integrations: Safelink, SentinelOne

MISP TIP

MISP TIP

Category: TIP

MISP is an open-source Threat Intelligence Platform designed specifically to foster collaborative threat intelligence sharing and analysis within trusted communities. It enables organizations to aggregate, store, analyze, and share structured threat intelligence data in a secure and standardized manner, empowering them to proactively defend against evolving cyber threats.

Infoblox

NetMRI

Category: Network Automation Platform

NetMRI is a network management software product developed by Infoblox that provides comprehensive network change and configuration management (NCFM) capabilities. It empowers network administrators to automate routine tasks, gain deeper insights into their network infrastructure, and proactively address potential issues.

Netskope

01 | [Netskope](#)

Category: Security Service Edge

Netskope Security Cloud Platform stands as a comprehensive cloud-based platform that delivers Secure Access Service Edge (SASE) architecture for organizations. SASE combines security services like cloud access security broker (CASB), zero-trust network access (ZTNA), advanced threat protection (ATP), and data loss prevention (DLP) into a unified platform, simplifying security across cloud, web, and private applications accessed from anywhere, on any device.

Integrations: SentinelOne

02 | [Netskope Cloud Log Shipper](#)

Category: Security Service Edge

Netskope Cloud Log Shipper (CLS) is a powerful integration module within the Netskope platform specifically designed to streamline security logging management. It allows you to forward all or a subset of your customer tenant event and alert logs to Security Information and Event Management (SIEM) platforms, data lakes, and Extended Detection and Response (XDR) systems.

OAuth

02 | [OAuth](#)

Category: IT Ops

OAuth is an authorization framework that allows users to grant secure third-party access to their data and accounts, without having to share their passwords. It acts as a middleman between the user, the third-party application (like a login button on a website), and the actual service provider (like Facebook or Google).

OCSEF

05 | [OCSEF](#)

Category: Standard

The Open Cybersecurity Schema Framework (OCSEF) is a collaborative, open-source effort by AWS and leading partners in the cybersecurity industry. OCSEF provides a standard schema for common security events, defines varying criteria to facilitate schema evolution, and includes a self-governance process for security log producers and consumers. The public source code for OCSEF is hosted on GitHub.

Okta

02 | [Okta](#)

Category: Access Management

Okta platform manages and secures user identities, granting smooth access to applications while enhancing security through centralized control and strong authentication.

Integrations: Duo, SentinelOne

Oracle

01 | [Oracle](#)

Category: Cloud database, Analytics and business intelligence (ABI) platform

Oracle Platform encompasses a broad range of cloud-based and on-premise software and infrastructure technologies for enterprise computing.

Integrations: Dvao

02 | [Oracle Cloud Analytics](#)

Category: Analytics and business intelligence (ABI) platform

The Oracle Analytics platform is a cloud-native service that provides the capabilities required to address the entire analytics process including data ingestion and modeling, data preparation and enrichment, and visualization and collaboration, without compromising security and governance.

03 | [Oracle Cloud Fusion](#)

Category: Enterprise resource planning (ERP) platform

Oracle Cloud Fusion Middleware is a collection of software products enabling integration and communication between different technologies and applications.

04 | [Oracle Cloud Logs](#)

Category: IT Ops

Oracle Cloud Logs refer to the records of activities, events, and errors generated within the Oracle Cloud infrastructure and services. These logs provide insights into the performance, security, and operational aspects of Oracle Cloud resources, allowing administrators to monitor, troubleshoot, and optimize their cloud environment effectively.

Integrations: Dvao

05 | [Oracle Cloud Infrastructure](#)

Category: Cloud Security

Oracle Cloud Infrastructure (OCI) is a cloud computing platform offered by Oracle that provides a wide range of services including compute, storage, networking, databases, and analytics, allowing businesses to build, deploy, and manage applications in the cloud.

Integrations: JupiterOne

06 | [OCI Cloud Guard](#)

Oracle Cloud Guard enhances security for OCI by detecting threats, addressing misconfigurations, and monitoring suspicious activities. It offers comprehensive visibility and easy management of cloud security.

Integrations: JupiterOne

Orca Security

02 | [Orca Security](#)

Category: CNAPP, CSPM

Orca Security Platform is a cloud-native vulnerability management and security platform that stands out through its agentless and context-aware approach.

Integrations: SentinelOne, Tines

Palo Alto Networks

01 | Palo Alto Networks - Cortex XSOAR (formerly Demisto)

Category: SOAR

Cortex XSOAR is a comprehensive security orchestration, automation, and response (SOAR) platform developed by Palo Alto Networks. It empowers security teams to streamline incident response, automate repetitive tasks, and strengthen their overall security posture.

Integrations: Tenable, Aruba, Forescout, AIRM, CrowdStrike, Tanium, Qualys, Aruba Central, Microsoft SCCM, SentinelOne, Cyberason, Palo Alto Networks - Dig Security, Palo Alto Networks - IoT

02 | Palo Alto Networks - Dig Security

Category: Data Security Posture Management (DSPM)

Dig Security (or Palo Alto Networks - Dig Security) is a cloud-native data security platform that addresses the challenges of protecting sensitive data in today's complex, multi-cloud environments. It goes beyond traditional data security tools by combining Data Security Posture Management (DSPM), Data Loss Prevention (DLP), and Data Detection and Response (DDR) capabilities into a unified platform.

Integrations: Jira, PagerDuty, ServiceNow, IBM, Palo Alto Networks - Cortex XSIAM (formerly Demisto), Slack, MS Azure, GCP Security Command Center

03 | Palo Alto Networks - IoT

Category: IoT Security, MSS

Palo Alto Networks IoT Security is a comprehensive solution designed to protect and manage Internet of Things (IoT) devices within your network. Here's a breakdown of its key features and value proposition:

Integrations: Aruba Central, AIRM, Anomali, Armit, Cisco WLC, Forescout, Microsoft SCCM, Palo Alto Networks - Prisma Cloud, Tanium, Tenable Vulnerability Management (formerly Tenable.io), Tenable Security Center (formerly Tenable.sc), Rapid7, Aruba, CrowdStrike, Qualys, Bluecat IPAM, ServiceNow, Net MGR, Microsoft Entra ID, Cisco Meraki, Resilient AssetCentre, Microsoft Defender XDR, Palo Alto Networks - Cortex XSOAR (formerly Demisto), ServiceNow - Service Graph Connectors

04 | Palo Alto Networks - Panorama

Category: IT Ops

Palo Alto Networks Panorama is a centralized management platform that allows you to configure, monitor, and update Palo Alto Networks firewalls from a single interface.

Integrations: Honeywell (formerly SCADAForce)

05 | Palo Alto Networks - Prisma Cloud

Category: CNAPP, CSPM, Security Service

Palo Alto Networks Prisma is a cloud-delivered security platform offering comprehensive protection across various areas of your IT infrastructure and applications. It encompasses several distinct yet integrated services, working together to provide a holistic security posture.

Integrations: Palo Alto Networks - IoT, Safebreach

Palo Alto Networks

06 | Prisma Access Parser

Category: Security Service Edge

Palo Alto Prisma Access Parser refers to a set of tools and functionalities within the Palo Alto Prisma Access platform used to process and analyze logs and data generated by user and device activity when navigating through the secure access gateway.

Integrations: SentinelOne

07 | Palo Alto Networks - Xpanse

Category: XDR

Xpanse is an active attack surface management solution that helps your organization actively discover, learn about and respond to unknown risks in all connected systems and exposed services.

Integrations: IBM QRadar

08 | Palo Alto Networks - Cortex XSIAM

Category: SIEM

Cortex XSIAM (pronounced as "X-Siam") is a powerful extended security intelligence and automation management (XSIAM) platform developed by Palo Alto Networks. It aims to unify and automate various security functions to give organizations a comprehensive view of their security posture and enable faster, more effective threat detection and response.

10 | Palo Alto Networks - Minemeld

Category: TIP

Minemeld is an open-source threat intelligence platform (TIP) that streamlines the aggregation, processing, and sharing of threat intelligence data across your security infrastructure. Developed by Palo Alto Networks, it empowers organizations to gather, analyze, and leverage threat intelligence from various sources to proactively defend against cyber threats.

Integrations: SentinelOne

11 | Palo Alto Networks - Cortex XDR

Category: XDR

Cortex XDR delivers comprehensive threat protection by analyzing enterprise-wide data. It enhances SOC efficiency, improves visibility, and reduces security operation costs by consolidating tools and leveraging AI.

Integrations: SentinelOne

Keeper Security

Keeper Security

Category: Access Management

Keeper Security is an easy-to-use platform that unifies critical components of identity and Access Management and enables zero-trust transformation.

Integrations: Snowflake, Tenable Security Center (formerly Tenable.sc), Tenable Vulnerability Management (formerly Tenable.io), Cisco

Prometheus

01 | [Prometheus](#)

Category: IT Ops

Prometheus is an open-source systems monitoring and alerting toolkit originally built at SoundCloud. It is now a standalone open source project and maintained independently of any company.

Integrations: Times

02 | [Prometheus Pushgateway](#)

Category: IT Ops

The Prometheus Pushgateway is a component of the Prometheus monitoring system designed to handle metrics from short-lived jobs or batch processes that wouldn't be captured by Prometheus's regular scraping interval.

Integrations: Times

ProofPoint

01 | [ProofPoint](#)

Category: DLP, Email Security, Enterprise Information Archiving, Security Service Edge

Proofpoint's platform is a comprehensive, cloud-based security suite designed to protect organizations from a wide range of cyber threats.

Integrations: SentinelOne

02 | [Proofpoint - TAP](#)

Category: SIEM, XDR

Proofpoint TAP identifies and blocks advanced email threats, including phishing, ransomware, and weaponized documents. It also mitigates risks in cloud apps with adaptive controls for dangerous URL clicks.

Integrations: SentinelOne XDR, SentinelOne - Purple AI

Qualys

[Qualys](#)

Category: AST, CMPP

Qualys is a leading provider of a unified platform for IT security and compliance, delivering end-to-end solutions from a single SaaS interface.

Integrations: Palo Alto Networks - IoT, Palo Alto Networks Cortex XSOAR (Formerly Demisto), JupiterOne, SentinelOne

Radiflow

[Radiflow](#)

Category: OT Security

Radiflow provides a comprehensive industrial cybersecurity platform designed to protect critical infrastructure and industrial control systems (ICS) from cyberattacks.

Integrations: Splunk, ServiceNow - Vulnerability Response, ServiceNow - Service Graph Connectors

Rapid7

01 | [Rapid7 InsightVM](#)

Category: Vulnerability Assessment

Rapid7 InsightVM is a comprehensive vulnerability management platform designed to help organizations identify, prioritize, and remediate vulnerabilities in their IT infrastructure and applications.

Integrations: SentinelOne

02 | [Rapid7 InsightIDR](#)

Category: SIEM, XDR

Rapid7 InsightIDR is a cloud-based security platform designed for Extended Detection and Response (XDR). It provides comprehensive threat detection, investigation, and response capabilities to help organizations swiftly identify and address potential threats across their entire IT environment.

Integrations: SentinelOne

Recorded Future

[Recorded Future](#)

Category: TIP

Recorded Future is an independent threat intelligence cloud platform that enables organizations to identify and mitigate threats across cyber, supply-chain, physical and fraud domains, and are trusted to get real-time, unbiased and actionable intelligence.

Integrations: SentinelOne

Red Canary

[Red Canary](#)

Category: MDR

Red Canary delivers cloud-based security services. It allows defenders to win against rapidly evolving adversaries by preparing for, detecting, and responding to security incidents. It exists with the singular purpose to improve security for organizations of all sizes.

Integrations: SentinelOne

Reftab

[Reftab](#)

Category: Access Management

Reftab is a cloud-based fixed asset management platform designed to simplify and streamline the way organizations track and manage their physical assets, like laptops, tools, furniture, and even supplies.

Integrations: Times

ReliaQuest

01 | ReliaQuest

Category: MDR

ReliaQuest offers a comprehensive security operations platform known as GrayMarker. It tackles multiple facets of security operations, aiming to unify threat detection and investigation, manage vulnerability, and more.

02 | Digital Shadows

Category: TIP

Digital Shadows (acquired by ReliaQuest) identifies unwanted exposure, protect against external threats, and minimize digital risk. The platform helps to minimize these risks by detecting data loss, securing the online brand, and reducing the attack surface.

Integrations: IBM QRadar, SPLUNK-PHANTOM, IBM SOAR - RESILIENT, McAfee, JiraServiceCenter, ServiceNow, Azure Sentinel, ServiceNow ITSM

Remidiant

Remediant Threat Enrichment

Category: TIP

Remediant's Threat Enrichment Platform (TEP) is now a part of Netwrix. It empowers security teams to transform raw threat data into actionable insights.

Integrations: SentinelOne

Rockwell Automation

Rockwell AssetCentre

Category: TIP

Rockwell FactoryTalk AssetCentre provides you with a centralized tool for securing, managing, versioning, tracking and reporting automation related asset information across your entire facility.

Integrations: Palo Alto Networks - IoT

Safebreach

Safebreach

Category: BAS

SafeBreach offers a breach and attack simulation (BAS) platform that enables organizations to proactively test and validate their security controls against real-world attacks.

Integrations: ServiceNow, IBM QRadar, Mimecast, Darktrace, STR TANGI, Palo Alto Networks - Prisma Cloud, Securonix, AnsysITL, Huxera - SSIEM Replacement (SOC), ThreatConnect, ThreatQuotient, Trend Micro Vision One

Salesforce

Salesforce

Category: Analytics and Business Intelligence (ABI) Platform, Collaboration platform

Salesforce Platform lets you build custom apps, automate workflows, and dig deeper into data to create personalized customer experiences. It's all about empowering businesses to adapt, streamline, and grow, making it a powerful tool for organizations of all sizes.

Integrations: SentinelOne, D3YO

SentinelOne

01 | SentinelOne

Category: EDR, MDR, EPP, CNAPP, XDR

SentinelOne Singularity is an innovative endpoint security platform that goes beyond traditional antivirus by leveraging powerful AI and machine learning to proactively protect your endpoints from sophisticated cyber threats.

Integrations: Amazon Security Lake, Watchtower, Vital Signs Report, SMTP Server, MS Office 365, MS 365 Defender, Salesforce, Microsoft Azure Event Hub, CyberArk CFM, Microsoft Intune, ExtraHop, Conditional Access Policy, Microsoft EventHub - Email Defender, Watchdog Outgoing API response, AWS S3 Bucket, Cisco Duo, AT&T USM Anywhere, Google Workspace, Onyx Security, SMTP Relay, Red Canary, MalwareBytes, ICAP Interceptor, Microsoft Teams, Palo Alto-Milestone, Zscaler, Remediant Threat Enrichment, Recorded Future V2, Rapid7 InsightsDR, Rapid7 VM, Coda Secure, McAfee, FortiSVM, Flashpoint, Aftab, Armorbox, BeyondTrust, Hatching, Mandiant, Criminal IP, Proofpoint, Microsoft Entra ID (formerly Azure AD), SentinelOne - Attivo, CiscoFTD Parser, FortiGate-PortManager Parser, Remote-ops, Pager Duty, Palo Alto Networks - Cortex XSOAR, IBM QRadar, Ciso, Mimecast, Netskope, AWS AppFabric, AWS ELB, AWS CloudWatch, Amazon GuardDuty, AWS, AWS Security Hub, GCP Security Command Center, SentinelOne - Singularity XDR, Slack, Tenable Vulnerability Management (formerly Tenable.sc), Palo Alto Networks - Cortex XDR, CheckPoint Firewall, FortiGate, Qualys, Amazon Relational Database Service (RDS), Palo Alto Networks - Firewall, Recorded Future

02 | SentinelOne - Attivo

Category: SOAR

Attivo provides network security services. It focuses on providing advanced network security threat detection technology for deployment on premise or as a cloud based service.

Integrations: SentinelOne

03 | SentinelOne - Deep Visibility

Category: SIEM

SentinelOne's "deep visibility" refers to its capability to provide detailed insight into endpoints and networks, allowing organizations to monitor and analyze activity at a granular level. This includes tracking processes, user behavior, file modifications, network connections, and other relevant data to detect and respond to security threats effectively.

Integrations: D3YO

SentinelOne

04 | [SentinelOne - Remote-Ops](#)

Category: XDR

This app allows SentinelOne RemoteOps customers to enrich data with relative incident information and to extend mitigation operations.

Integrations: SentinelOne

05 | [SentinelOne - Purple AI](#)

SentinelOne's Purple AI is an AI solution designed to enhance security team efficiency and provide insights into organizational vulnerabilities and transform cybersecurity operations.

Integrations: Slack, MS Office 365, ZScaler, FortGate, Palo Alto Networks - Firewall

06 | [SentinelOne - Singularity XDR](#)

Category: XDR

Singularity XDR provides unmatched visibility, protection, and response capabilities at cloud scale. It stops threats quickly and accurately, creating actionable insights while reducing security costs.

Integrations: SentinelOne

ServiceNow

01 | [ServiceNow](#)

Category: IT Ops, Vulnerability Assessment, SCAR, Enterprise Agile Planning, ITSM

ServiceNow is an all-encompassing ecosystem for workflow automation and digital transformation. The ServiceNow platform easily integrates with other tools, letting users manage projects, teams and customer interactions using a variety of apps and plugins.

Integrations: Safesearch, Digital Shadows, JupiterOne

02 | [Service Graph Connectors](#)

Category: IT Ops

The Service Graph Connectors from ServiceNow are powerful tools that bridge the data gap between your CMDB (Configuration Management Database) and various IT tools and platforms.

Integrations: Honeywell (formerly SCADAForce), Radflow, Palo Alto Networks - IoT

03 | [Vulnerability Response](#)

Category: Vulnerability Management

ServiceNow's Vulnerability Response is a feature that helps organizations manage and respond to cybersecurity vulnerabilities efficiently. It enables teams to identify, prioritize, and remediate vulnerabilities across their IT infrastructure by centralizing vulnerability data, automating workflows, and facilitating collaboration between security and IT teams.

Integrations: Radflow

04 | [ServiceNow CMDB](#)

Category: Cloud database

ServiceNow CMDB is a central repository where you catalog and visualize all your IT assets, their relationships, and their configurations.

ServiceNow

05 | [ServiceNow ITSM](#)

Category: ITSM

ServiceNow ITSM is your IT service maestro, harmonizing incidents, requests, and changes into a seamless symphony. It streamlines operations, reduces downtime, and keeps users happy, making your IT service delivery sing like a professional orchestra.

Integrations: Cyberason, Digital Shadows

06 | [ServiceNow SecOps](#)

Category: IT Ops

ServiceNow SecOps unites people, processes, and technology to protect your organization against evolving threats and respond swiftly to attacks.

Integrations: Cyberason

07 | [Security Incident Response](#)

Category: SCAR

ServiceNow SIR is a platform that streamlines security incident response. It helps teams collaborate, automate tasks, and track incidents for faster threat resolution.

Integrations: Honeywell (formerly SCADAForce)

Snowflake

[Snowflake](#)

Category: Cloud database

Snowflake scales your data like a cloud giant, crunching and storing everything from tiny to titanic, fueling insights in seconds, not eons.

Integrations: Dvvo, JupiterOne, Keeper Security

Snyk

[Snyk](#)

Category: CMAPP, Application security testing (AST)

Snyk shields your entire software lifecycle from the shadows of vulnerabilities, making every line of code and container shine with security.

Splunk

01 | [Splunk Enterprise Security \(ES\)](#)

Category: SIEM

Splunk Enterprise Security (ES) is your cybersecurity command center, transforming raw data into actionable intelligence to shield your organization from threats and ensure digital resilience.

Integrations: Cyberason, SCADAForce

Splunk

02 | [Splunk OnCall](#)

Category: SIEM

Splunk OnCall is your digital first responder for incident management, transforming frantic scrambling into calm, coordinated action.

Integrations: Times

03 | [Splunk Operational Technology \(OT\)](#)

Category: IT Ops

Splunk (AI Industrial Asset Intelligence) specifically tackles the challenge of unleashing the power of Operational Technology (OT) data within the broader Splunk platform. Imagine it as a translator and interpreter for your industrial sensors and machines, extracting valuable insights from their raw data to optimize and safeguard your industrial operations.

04 | [Splunk SOAR \(Phantom\)](#)

Category: SOAR

Splunk SOAR (formerly Phantom) is a security orchestration, automation, and response (SOAR) solution. The Splunk Phantom platform combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools to help you orchestrate security workflows, automate repetitive security tasks, and quickly respond to threats.

05 | [Splunk \(Cloud and On-Prem\)](#)

Category: SIEM

Splunk, in both cloud and on-prem versions, devours your IT data deluge, transforming it into actionable insights like a digital alchemist. Its cloud offerings, swift and scalable, empower real-time analysis. On-prem options grant granular control, ideal for sensitive data or compliance needs. Whether in the cloud or on your own turf, Splunk illuminates your IT operations, guiding decisions and optimizing performance.

Integrations: Doppel

Sumo Logic

[Sumo Logic](#)

Category: SIEM, SOAR

Sumo Logic is a cloud-native Continuous Intelligence Platform that helps organizations manage and gain insights from their log and machine data.

Integrations: Wotni, Doppel

Tanium

01 | [Tanium](#)

Category: EDR, Unified Endpoint Management (UEM), Vulnerability Assessment

Tanium XDR Core is a foundation for all Tanium solutions that enables you to answer fundamental questions about your endpoint environment and break down silos between IT operations and security.

Integrations: Palo Alto Networks - IoT, Palo Alto Cortex XSOAR (Formerly Demisto), Devo

Tanium

02 | [Tanium - Core](#)

Category: Endpoint Management (EDM)

Tanium Core is a cybersecurity platform designed to provide real-time visibility and control over endpoints within an organization's network. It offers features such as asset discovery, endpoint management, threat detection, and incident response, allowing organizations to rapidly identify and remediate security issues across their IT infrastructure.

Integrations: Times

03 | [Tanium - Threat Response](#)

Category: IT Ops

Tanium Threat Response is a feature within the Tanium cybersecurity platform that enables organizations to swiftly detect, investigate, and respond to security threats across their IT infrastructure. It provides real-time visibility into endpoint activities, facilitates rapid threat detection, and supports quick incident response actions to mitigate potential risks effectively.

Integrations: Times

Tenable

01 | [Tenable Vulnerability Management](#)

Category: Vulnerability Assessment

Tenable Vulnerability Management (TVM) empowers you to see and fix vulnerabilities across your digital attack surface, proactively safeguarding your organization from cyber threats.

Integrations: Palo Alto Networks - IoT, SentinelOne

02 | [Tenable Security Center](#)

Category: Vulnerability Assessment

Tenable Security Center focuses primarily on on-premises vulnerability management. It scans traditional IT infrastructure like servers, desktops, and network devices.

Integrations: Palo Alto Networks - IoT

ThreatQuotient

[ThreatQuotient](#)

Category: SOAR, TIP

ThreatQuotient is a Threat Intelligence Platform (TIP) designed to unify and streamline threat intelligence operations for organizations of all sizes. It serves as a central hub where security teams can collect, analyze, and operationalize threat data from various sources, empowering them to make informed decisions, prioritize actions, and strengthen their defenses against cyber threats.

Integrations: Devo, Safebreach

Tines

Tines

Category: SOAR

Tines is a no-code automation platform specifically designed for security teams. It empowers them to easily build custom workflows (called Stories) using "actions" and "events" to automate repetitive tasks, streamline incident response, and strengthen their overall security posture.

Integrations: JIRA, CloudBark, IBM Cloud, Google Security Command Centre Alerts (Story Library), Okta, Reset a password (Story Library), CarbonBlack, QSO, Secure Endpoints, Reflot, JupiterOne Endpoints, Google Workspace, Veeva, Google, Cloud Storage, Azure Sentinel, Jira-Servicedesk, Wazuh, Azure Blob, GitLab, Prometheus, GrayLog, Analyst One, Splunk OnCall, JupiterOne-GrafTrace, Aqua Security, Cribl, Criminal IP, Docker, Cisco Umbrella, Cisco Secure Email, Malwarebytes, Dracastory, MatterMost, Tanium - Threat Response, Tanium - Core

Trellix

Trellix (formerly FireEye)

Category: XDR, NDR, EDR, DLP, EPP, CNAPP

Trellix, previously known as FireEye and McAfee, offers a comprehensive cybersecurity platform designed to protect organizations from an ever-evolving threat landscape. It goes beyond traditional siloed solutions by integrating Extended Detection and Response (XDR), endpoint security, network security, cloud security, and other capabilities into a unified platform.

Uptycs

Uptycs

Category: EDR, CNAPP, XDR

Uptycs is a unified CNAPP and XDR platform designed to help organizations secure their entire attack surface, encompassing everything from cloud infrastructure and containers to endpoints and web applications. It provides comprehensive visibility, threat detection, and response capabilities across this diverse landscape, empowering security teams to proactively defend against cyber threats and ensure compliance.

SevenAI

SevenAI

SevenAI collects alert data from multiple sources to identify incidents. It uses AI to gather additional relevant information related to the alerts and, if required, correlates this data with various sources to analyze the root cause of the incidents.

Integrations: SentinelOne, Splunk

Veeam

Veeam

Category: Enterprise Backup and Recovery Software Solution, ITRO (IT Resilience Orchestration)

Veeam is a unified data protection and recovery platform designed to help organizations safeguard critical business data across both physical and virtual environments. It goes beyond traditional backup and recovery by providing enhanced security, visibility, and automation for managing your data across hybrid and multi-cloud ecosystems.

VirusTotal

VirusTotal

Category: TP

VirusTotal is a free online platform that analyzes suspicious files and URLs for malware, viruses, and other threats. It leverages the power of over 70 antivirus engines and other scanning tools to provide comprehensive threat detection.

VMRay

VMRay

Category: TP

VMRay is a solution for advanced malware analysis and threat detection. It uses innovative technologies to help organizations deeply understand sophisticated cyber threats and effectively protect their systems from targeted attacks.

VMware by Broadcom

01 | VMware by Broadcom - Carbon Black

Category: EDR, EPP, OT Security

VMware Carbon Black is a unified platform offering comprehensive endpoint and workload protection against modern cyber threats. It combines various security capabilities to achieve prevention, detection, and response across physical and virtual environments, from workstations to cloud workloads.

Integrations: Zscaler Sandbox Update V7, IBM QRadar, Intel sgx and go through the ci apps

02 | Broadcom

Category: EPP, UEM, DLP, EDR

Broadcom encompasses a vast array of hardware, software, and security solutions across various domains, including cyber security, enterprise software, and more.

Votiro

Votiro

Category: Email Security

Votiro is a content security platform that protects organizations from zero-day malware, ransomware, and other advanced threats embedded within files.

Integrations: Box, Surio Logic, MS Azure, SMTP Connector, ICAP Connector, Microsoft Teams, Zscaler, Netscape, Microsoft Sentinel, Salesforce, MD Teams Connector

Wazuh

Wazuh

Category: SIEM, EDR

Wazuh is a free and open source platform used for threat prevention, detection, and response. It is capable of protecting workloads across on-premise, virtualized, containerized, and cloud-based environments.

Wiz

Wiz

Category: CNAPP, CSPM

Wiz offers comprehensive cloud security that goes beyond traditional point solutions. It combines prevention, active detection, and response capabilities to safeguard your cloud infrastructure, workloads, and applications across multiple providers like AWS, Azure, GCP, and more.

Integrations: Dvao, Splunk, IBM QRadar, Palo Alto Networks - Dig Security, SentinelOne

Zerofox

01 | Zerofox

Category: TIP

Zerofox is an always-on, full-spectrum external threat intelligence, protection and response solution that provides organizations with comprehensive visibility and protection across the surface, deep and dark web.

Integrations: IBM QRadar

02 | ScoutPrime

Category: SOAR

ScoutPrime acts as an "outside-in" defense shield for your organization, providing a comprehensive view of your threat landscape beyond your perimeter.

Zoom

Zoom

Category: Collaboration platform

Zoom empowers seamless interaction through its unified suite of video conferencing, messaging, phone, and collaboration tools, boosting productivity and team engagement.

Zscaler

Zscaler

Category: Security Service Edge, OT Security, CSPM, DLP, CNAPP

Zscaler transforms network security with a cloud-delivered platform that eliminates traditional perimeters and enables secure access to apps and data from any device, anytime, anywhere.

Integrations: SentinelOne, SentinelOne - Purple AI

42Gears

SureMDM

Category: Unified Endpoint Management (UEM)

SureMDM by 42Gears is an intuitive and powerful MDM solution and app available for Android, iOS/iPadOS, Windows, Linux, macOS, Wear OS, VR, and IoT platforms. With SureMDM, IT teams can secure, monitor, and manage company-owned devices for dedicated use, as well as employee-owned devices used to access company data (BYOD).

Integrations: Dvao

STIX TAXII

STIX TAXII

Category: XDR

STIX/TAXII is a collaborative effort to improve cyber threat information sharing. STIX defines a common language for threat data, and TAXII securely shares it between systems.

Integrations: Safesearch

Okta

Okta Workforce Identity

Category: IAM

Okta Workforce Identity is A cloud-based identity and access management (IAM) solution that simplifies employee access to applications and resources, enabling centralized control and secure authentication.

Integrations: SamurAI XDR

Hatching

01 | Hatching

Category: TIP

Hatching identifies and uncovers new or emerging cyber threats and attacks. It involves closely monitoring various sources of threat intelligence, analyzing patterns and behaviors, and proactively detecting potential security risks before they escalate into full-blown incidents.

Integrations: SentinelOne

02 | Hatching Triage

Category: TIP

Hatching Triage by Hatching is a cloud-based sandboxing and malware analysis platform designed for rapid threat detection and analysis. It enables security teams to quickly and efficiently examine suspicious files and URLs to determine their malicious intent and behavior.

1Password

1Password

Category: IAM

1Password is a password manager that securely stores and manages user credentials, offering features like password generation, multi-factor authentication, and secure sharing capabilities.

Integrations: SamurAI XDR

Automox

Automox

Category: Unified Endpoint Management (UEM)

Automox is a cloud-native patching platform that automates patch management across Windows, macOS, Linux, and third-party software. It aims to simplify and enhance security by removing the burden of manual patching processes.

Integrations: Dvvo

Trend Micro

01 | Trend Micro Cloud One

Category: GMAP, CSPM

Trend Micro Cloud One is a cloud-based security platform offering comprehensive protection for endpoints and workloads across hybrid cloud environments. It provides features like endpoint security, threat detection and response, compliance management, and data loss prevention, all managed through a centralized console.

Integrations: JupiterOne

02 | Trend Micro Apex One

Category: EPP

Trend Micro Apex One protection offers advanced automated threat detection and response against high level threats. Apex One provides actionable insights, expanded investigative capabilities, and centralized visibility.

Integrations: SamurAI XDR

03 | Trend Micro Vision One

Trend Vision One supports diverse hybrid IT environments, automates and orchestrates workflows, and delivers expert cybersecurity services, so you can simplify and converge your security operations.

Integrations: JupiterOne

Pager Duty

Pager Duty

Category: IT Ops

PagerDuty is a real-time operations platform that empowers teams to manage incidents, prevent disruptions, and ensure seamless digital experiences.

Integrations: SentinelOne

SamurAI XDR

SamurAI XDR

Category: XDR

SamurAI XDR is a cloud-based security platform categorized as Extended Detection and Response (XDR). It's designed to help organizations identify and respond to cyber threats.

Integrations: 1Password, Okta Workforce Identity, Cisco Meraki, Microsoft Sentinel (formerly Azure Sentinel), Trend Micro Apex One, Armitage GuardDuty, MS Office 365, Proofpoint - TAP

PingOne

PingOne

Category: Access Management, IoT Security

PingOne is a cloud-based identity and access management (IAM) platform developed by Ping Identity. It provides a comprehensive suite of services for managing user identities, access rights, and authentication across your entire organization, both on-premises and in the cloud.

Hunters Security

Hunters - SIEM Replacement (SOC)

Category: SIEM

Hunters SOC platform provides unlimited data ingestion, built-in detection, engineering, and automated data correlation and investigation to overcome volume, complexity, and false positives.

Integrations: Safebreach

Sonar

SonarQube

Category: Application Security Testing (AST)

SonarQube is a self-managed, automatic code review tool that systematically helps you deliver clean code. It integrates into your existing workflow and detects issues in your code to help you perform continuous code inspections of your projects.

Integrations: JupyterOne

Silverfort

Silverfort

Category: User Authentication

Silverfort shields sensitive data across any endpoint, cloud, or container, wrapping everything in invisible encryption while granting seamless access for authorized users, making data breaches a distant memory.

SecureWorks

Category: XDR

SecureWorks Tsegis XDR

Secureworks Tsegis XDR offers detection, response and an open platform built from the ground up to integrate market-leading technologies.

Integrations: Safebreach, JupyterOne

Kubernetes

Kubernetes

Kubernetes, also known as K8s, is an open source system for automating deployment, scaling, and management of containerized applications. It simplifies managing complex applications in a cloud-native environment.

Integrations: JupyterOne

Zendesk

Zendesk

Category: Collaboration Platform

Zendesk is a cloud-based customer service platform designed to help businesses manage and improve their interactions with customers. It offers a suite of tools to handle customer inquiries, complaints, and requests efficiently.

Integrations: JupyterOne

JFrog

JFrog Artifactory

JFrog Artifactory is a platform for managing and storing various types of software packages and artifacts. It serves as a central repository for developers and DevOps teams to share and manage code, libraries, and other build components efficiently.

Integrations: JupyterOne

Vectra

Vectra

Category: XDR

Vectra is a hybrid attack surface visibility and detection platform powered by Artificial Intelligence (AI). It empowers organizations to see and stop sophisticated cyberattacks across their entire infrastructure.

Zix

Zix

Category: Email Security, Enterprise Information Archiving

Zix is an enterprise solution for email encryption, threat protection and email archiving that helps businesses with productivity, security, and compliance.

Slack

Slack

Category: Collaboration platform

Slack swaps emails for streamlined chats and channels, fueling teamwork with instant messaging, file sharing, and integrations, making collaboration a breeze in the digital age.

Integrations: Palo Alto Networks - Dig Security, SentinelOne

Blackberry

CylanceProtect

Category: IoT Security, EPP

CylancePROTECT is an AI-powered endpoint protection platform (EPP) that uses artificial intelligence (AI) and machine learning (ML) to proactively prevent threats, rather than relying on reactive signature-based detection. It works by analyzing the behavior of files and processes to determine whether they are malicious, even if they have never been seen before.

Integrations: Devs

ThreatConnect

ThreatConnect

Category: TIP

ThreatConnect offers robust threat intelligence feeds and data services to manage, operationalize, and consolidate intelligence from multiple sources, including open-source, commercial, and internal data.

Integrations: Safebreach

Doppel

Doppel

Category: TIP

Doppel provides AI-powered threat detection and takedown across domains, social media, and digital marketplaces, offering comprehensive, automated protection against external threats in real-time.

Integrations: Google SecOps (formerly Google Chronicle), Splunk, Sumo Logic

Confluent

Confluent Cloud

Confluent Cloud is a fully managed data streaming platform built on Apache Kafka. It provides a cloud-native solution for organizations to process and analyze large volumes of data in real-time.

Integrations: JupiterOne

LogRhythm

LogRhythm

Category: SIEM, NDR

LogRhythm provides security operations center (SOC) services to our customers build their strongest defense and maximize return on investment.

OPSWAT

OPSWAT MetaDefender IT Access

OPSWAT MetaDefender uses advanced technologies to protect IT and OT environments from malware, zero-day attacks, and other advanced threats. It integrates seamlessly with existing infrastructure to safeguard data.

Integrations: Cybereason XDR

Analyst1

Analyst1

Category: SOAR

Analyst1's platform uses machine learning and artificial intelligence to analyze data from multiple sources and provide insights into potential threats.

Integrations: Safebreach

Contact Us

✉ prakash@metronlabs.com
🌐 www.metronlabs.com
☎ +1 888 840 3282 (USA)



**Better Security Through
Integration. Automation. Playbooks.**