Radically Minimize Your Attack Surface

Protect Your Infrastructure, Applications, and Data with Industry-Leading Cloud Security

Monitoring/Visibility

Monitor Your Applications

Monitor the availability, usage, and performance of your software applications, whether hosted or on-premises. Track live metrics streams, events, requests and response times.

Monitor Your Infrastructure

Analyze and optimize the performance of your infrastructure, including Virtual Machines (VMs), storage, and databases. Monitor your VMs on a single map.

Monitor Your Network

Monitor and diagnose networking issues without logging into your VMs. Trigger a packet capture, analyze network security group flow logs, diagnose routing issues, and gain visibility and control over your network.

Detect Threats for VMs and Servers

Monitor and protect your VMs. Get alerts and remediation suggestions from all supported security platforms in an easy-to-use format.

Detect Fileless Threats

Identify fileless attack toolkits, techniques, and behaviors.

Detect Network-based Threats

Get alerts on suspicious network traffic activity.

Detect Non-Traditional Attack Techniques

Analyze memory at the time of a crash to detect attack techniques not easily detected by traditional disk-based approaches.

Monitor File Integrity

Validate the integrity of operating system and application software files against a known baseline to identify changes that might indicate an attack.

Centralize Management through the Dashboard

Receive alerts when a threat is detected on the resources and services you're protecting. From the dashboard, you can pivot to perform a detailed investigation to uncover the scope of the attack.

Gain Insights from Your Data

Analyze, interact with, and quickly derive insights from huge volumes of operational data in a powerful analytics platform. Use smart analytics and machine learning algorithms to isolate anomalies and detect problems quickly.

Security/Protection

Integrate with Microsoft Defender ATP

Gain comprehensive Endpoint Detection and Response (EDR) capabilities. Spot abnormalities, detect and respond to advanced attacks on server endpoints.

Lock Down Inbound Traffic to Your VMs

Lock down inbound traffic to your Virtual Machines (VMs), reducing exposure to attacks while providing easy access to connect to VMs when needed.

Protect Your Web Applications

Protect your web applications from bot attacks and common web vulnerabilities such as SQL injection and cross-site scripting using a Web Application Firewall.

Provide Secure User Authentication

Provide hassle-free and secure access to your network, systems, and all applications with Secure Single Sign-on (MFA, X.509, AES), enhanced with Zero Trust & CAuth, reliability, regulatory compliance and workforce flexibility.

Scan Your Virtual Machine for Vulnerabilities

Scan your virtual machines for vulnerabilities. The vulnerability scanner included with Security Center is powered by Qualys and widely recognized as the leading tool for identifying vulnerabilities in real time across your VMs. This feature is only available if third-party licenses have been acquired to perform scanning and installation.

Use Security Rules to Allow or Deny Network Traffic

Use security rules to allow or deny inbound/outbound network traffic to/from several types of resources.

Control and Manage Disk Encryption

Control and manage disk encryption keys and secrets, while ensuring that all data in the VM disks are encrypted at rest in storage.

Improve Your Incident Median Time to Mitigation

See and stop threats before they cause harm. Get a birds-eye view across the enterprise and makes threat detection and response smarter and faster with AI.

Gain a Graphical View of Your Network (Map)

Gain recommendations and insights for hardening your network resources from a graphical view with security overlays.

Assess and Analyze Network Security

Analyze the security state of your resources for network security best practices. When Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed controls to harden and protect your resources.

Harden Your Machines Against Malware

Control which applications run on your machines to help harden your machines against malware.

Manage Security Keys

Easily create and control the keys used to encrypt your data.

Apply NSGs to Filter Traffic

Improve your network security posture by applying network security groups (NSG) to filter traffic to and from resources.

Discover Endpoint Protection Solutions, including:

- Windows Defender (Microsoft Antimalware)
- System Center Endpoint Protection (Microsoft Anti-Malware)
- Trend Micro – all Versions*
- Symantec v12.1.1100+
- McAfee v10+ (Windows & Linux*)
- Sophos V9+ (Linux)*

*The coverage state and supporting data is currently only available in the Log Analytics workspace associated with your protected subscriptions.

Assess Vulnerabilities, including:

- Missing OS patches assessment
- Security misconfigurations assessment
- Disk encryption assessment
- Third-party vulnerability assessment

Compliance

Simplify Regulatory Compliance

Use helpful dashboards and reports to streamline the process for meeting regulatory compliance requirements.

Identity and Access

Monitor Identity

Monitor identity activities, you can take proactive actions before an incident takes place or reactive actions to stop an attack attempt.

View Recommendations to Protect Individual User Security

View recommendations for all subscriptions and the severity based on security assessments.

View and Act on Recommendations thru a Visual Dashboard

Gain recommendations such as:

- Enable MFA for privileged accounts on your subscription
- Remove external accounts with write permissions from your subscription
- Remove privileged external accounts from your subscription