Mandiant

DATASHEET

Attack Surface Management

Common Use Cases

- Identify shadow IT: Continually monitoring for shadow IT provides visibility of the known systems, and a running list of these assets to your security team, so they can keep watch for anything out of the ordinary. Your security team will receive daily summaries of new assets and technologies added.
- Multicloud asset discovery: A centralized view of hybrid and multicloud environments allows security teams to answer critical questions when it matters most.
- Mergers and acquisitions due diligence: Your organization can take preventative measures during an acquisition with visibility into that acquisition's unknown systems and a running list of assets. The security team can specify security posture requirements before and after the transaction closes.
- Subsidiary monitoring: Assess the external security posture of each subsidiary, while enabling each to maintain autonomy. Mandiant ASM comes with role-based access controls (RBAC), equipping each organization to independently monitor and manage its own attack surface scope. All while centralizing visibility for the parent organization.

See your organization through the eyes of the adversary

IT environments are designed to be dynamic. They evolve organically, through cloud computing, unsecured networks, SaaS deployments, containers, microservices, IoT devices, applications, infrastructure and data that are often added without adhering to organizational security policies. Legacy sprawl, orphaned infrastructure and an increasingly distributed workforce are ever-present complications.

Even with custom tools security teams cannot easily see the entirety of their rapidly expanding attack surface and address its challenges. Mandiant Attack Surface Management (ASM), combines extended enterprise visibility and continual monitoring capabilities infused with the latest Mandiant Threat Intelligence to help organizations discover exposures and analyze internet assets across today's dynamic, distributed and shared environments.

Comprehensive Extended Enterprise Visibility

Mandiant ASM enables organizations to discover and analyze Internet-facing assets across today's dynamic, distributed, and shared environments, while continually monitoring the external ecosystem for exploitable exposures.

Mandiant ASM module generates comprehensive visibility of the extended enterprise through continual discovery that illuminates assets, alerts on risk and enables security teams to operationalize intelligence with incredible speed and agility. Mandiant ASM identifies business relationships across infrastructure and removes sprawl through comprehensive visibility of known and unknown assets. This enables cyber security teams to inventory their assets and investigate any discovered exposures.

Tools designed before the cloud era only support static work locations and a limited set of devices and applications running behind a network firewall. Mandiant ASM is purpose built to support dynamic, distributed IT for the most demanding security teams.

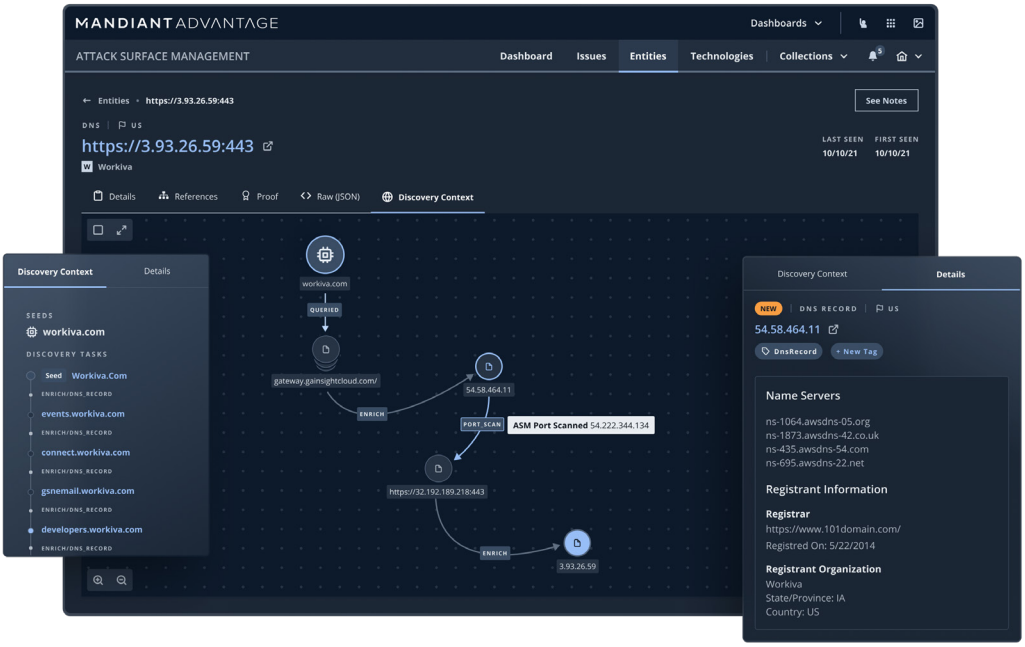

FIGURE 1. Assess external asset relationships and dependencies to better understand the attack surface.

Continual Exposure Monitoring

Enable cyber security teams to monitor and assess assets and infrastructure, including software stacks and configurations. Attack Surface Management works in real time to detect changes and exposures to identify exploitable vulnerabilities while building a safety net for cloud adoption and digital transformation. The module helps cyber security teams quickly understand threats and other risks to discovered assets so they can be triaged.

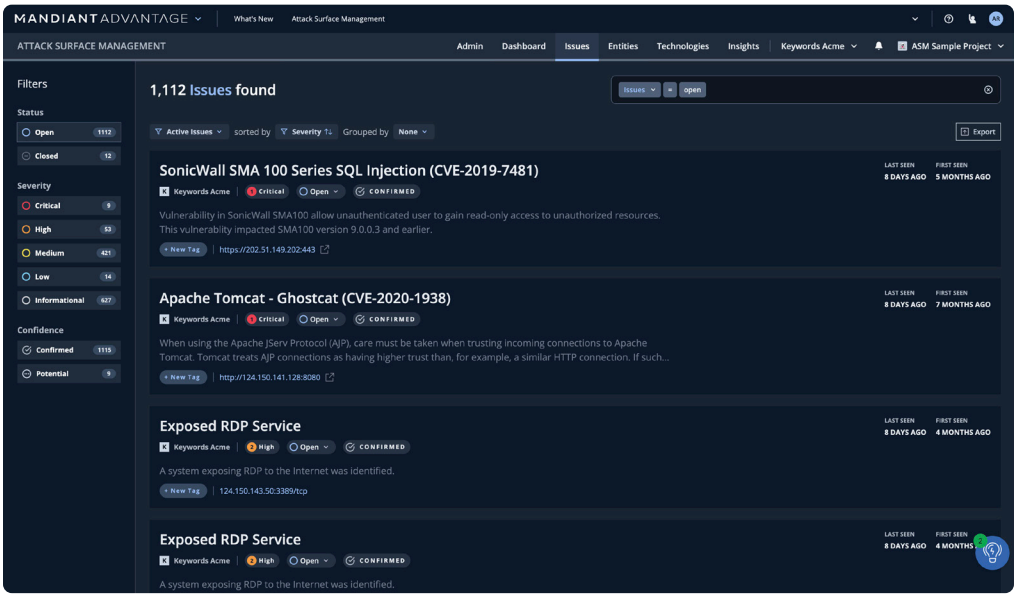

FIGURE 2. Investigate and prioritize security issues based on the potential impact to the organization.

Operationalize Expertise and Intelligence

Empower security operations to mitigate real-world threats. Mandiant expertise and threat intelligence are automatically applied to the attack surface to determine what is exposed and continuously monitor risk. This module integrates with existing workstreams, notifies cyber security teams as new assets are added to the environment and alerts on any exposures.

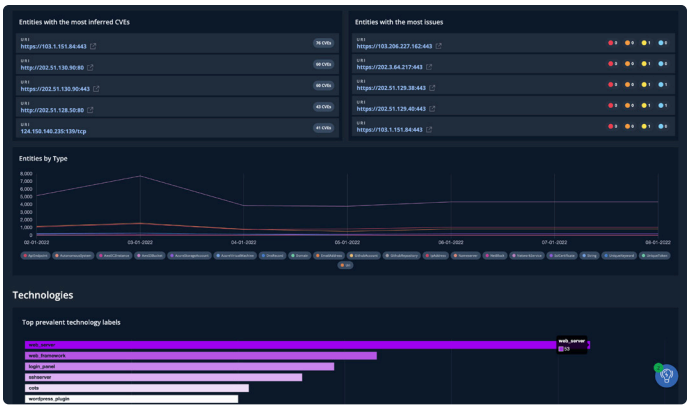

FIGURE 3. Analyze and communicate trends and insights from around the external ecosystem.

Key Features

- **Continual monitoring:** Control how often asset discovery and analysis are conducted with daily, weekly, or on-demand scans.
- **Technology and service identification:** Get an inventory of applications and services running in the external ecosystem.
- **Outcome-based asset discovery:** Specify the type of asset discovery workflow run against the attack surface based on specific outcomes or use cases.
- **Active asset checks:** Active asset checks are benign payloads or scripts designed from Mandiant IOCs and frontline intelligence, and are used to validate when an asset is susceptible to exploitation.

Outcomes

Organizations with Attack Surface Management can take advantage of several high-value outcomes:

- **Deeper understanding of your technology ecosystem:** Discover assets and cloud resources using a multitude of integrations and techniques and identify partner and third-party relationships. Examine asset composition, technologies, and configurations in the wild.
- **Continuous asset monitoring to stay ahead of threats:** Monitor infrastructure in real time to detect changes and exposures, while building a safety net for cloud adoption and digital transformation.
- **Empowerment of security operations to mitigate real-world threats:** Automatically apply Mandiant expertise and intelligence to see exposed areas of the attack surface.

More Integrations, More Visibility

Find more assets and address security issues faster. Mandiant ASM constantly monitors for risks introduced to the organization and integrates with the following vendors to automatically pull assets and cloud resources into the discovery workflow:

- Akamai DNS Edge
- AWS
- Azure
- Google Cloud
- GitHub
- GoDaddy
- Cloudflare
- DNS Made Easy

Action on Attack Surface Insights

Prioritize and remediate security issues directly from established security operations workflows. You can use available integrations or the Mandiant ASM API to operationalize information from the attack surface. Available integrations include:

- Splunk
- ServiceNow
- Jira
- Teams or Slack (via webhook)
- Chronicle Security Operations

Learn more at https://cloud.google.com/security/products/attack-surface-management?hl=en