MANDIANT
NOW PART OF Google Cloud

MANDIANT ADVANTAGE DATASHEET

Attack Surface Management

Competitive edge

Attack Surface Management provides comprehensive asset discovery and risk mitigation to enable the safe adoption of new technology and processes that speed innovation. Your organization can become more competitive by:

- Supporting remote hybrid work
- Protecting beyond the edge of the perimeter
- Scaling to the largest environments
- Managing cloud computing and shadow IT
- Embedding governance into workflows
- Building supply chain resilience
- Extending security policy outside the enterprise

See yourself through the eyes of the attacker

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 Advantage Attack Surface Management, a module of the Mandiant Advantage platform, combines extended enterprise visibility and continuous monitoring capabilities infused with the latest Mandiant Advantage Threat Intelligence to help organizations discover exposures and analyze internet assets across today's dynamic, distributed and shared environments.

Comprehensive Extended Enterprise Visibility

Attack Surface Management provides cyber security teams with a comprehensive, true view of their environment through the eyes of the attacker. This module operationalizes attacker intelligence to transform security programs from reactive mode to proactive.

Attack Surface Management discovers and analyzes internet assets across today's dynamic, distributed, and shared environments. This module generates comprehensive visibility of the extended enterprise through continuous discovery that illuminates assets, alerts on risk and enables security teams to operationalize intelligence with incredible speed and agility. Attack Surface Management 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. Attack Surface Management is purpose built to support dynamic, distributed IT for the most demanding security teams.

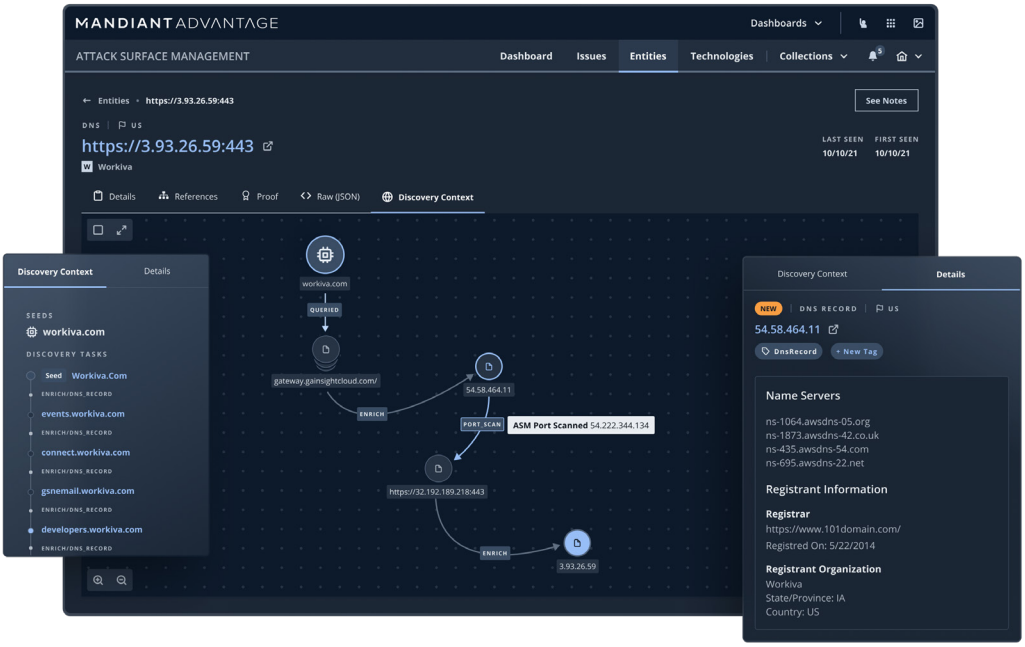

FIGURE 1. Assess external asset relationships and dependencies to better understand the attack surface.

Continuous 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.

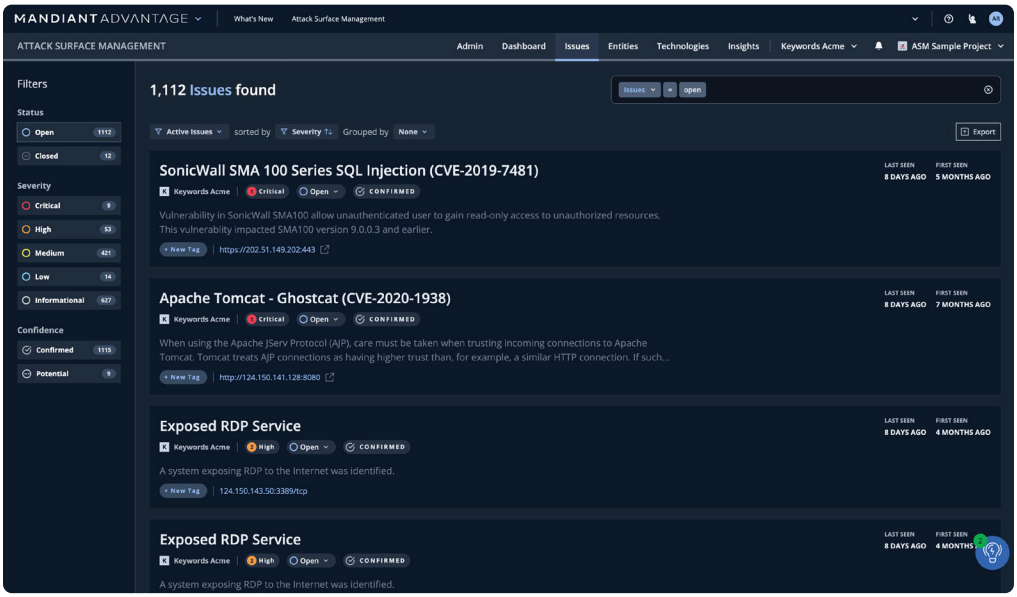

FIGURE 2. Investigate and prioritize security issues based on the potential impact to the organization.

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.

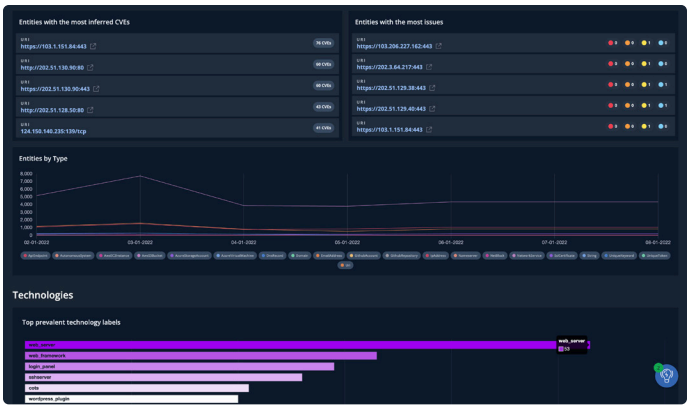

FIGURE 3. Analyze and communicate trends and insights from around the external ecosystem.

By the Numbers

Attack Surface Management includes:

- 250+ Integrated Data Sources: Expanded discovery scope through sources and techniques.
- 15+ Categorized Asset Types: Broad asset visibility across the entire ecosystem
- 60k+ Identified Technologies: Deeper analysis of technologies and configurations
- 350+ Active Checks: Validate asset exposures to exploits seen in the wild.

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. Attack Surface Management 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 Platform
- GitHub
- GoDaddy
- Cloudflare

Action on Attack Surface Insights

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

- Splunk
- ServiceNow
- Jira
- Teams or Slack (via webhook)

Learn more at **www.mandiant.com/asm-free**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
(703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant® has been a trusted partner to security-conscious organizations. Today, industry-leading Mandiant threat intelligence and expertise drive dynamic solutions that help organizations develop more effective programs and instill confidence in their cyber readiness.

MANDIANT
NOW PART OF Google Cloud