Protecting supply chains and third-party vendor connections | Mandiant

By Mandiant

Published: 2022-06-06 · Archived: 2026-04-05 17:41:41 UTC

Protecting your digital assets and brand is difficult in itself, but when you rely on supply chains, share proprietary information with vendors and subsidiaries or are involved with a merger or acquisition transaction, the complexity increases exponentially. The difficulty arises when users you don't know, and systems you don't own or have complete control over, now have access to your network and vice versa. Vendor contracts may be drawn up to include requirements for certain technology and updates within a set window, but execution is often out of your hands.

To address these scenarios and others, industry analysts coined the term digital risk protection which uses a combination of products and services to protect assets and data from external threats. Together they provide visibility into the open, deep and dark web, externally facing assets including cloud, and provide contextual information on the tactics, techniques and procedures (TTPs) currently used by threat actors. With early knowledge of this information, security professionals can better anticipate attacks and make proactive adjustments.

The Mandiant digital risk protection solution, offered as products or services, addresses these scenarios and many others.

- Mandiant Advantage Threat Intelligence is derived from intelligence by over 300 security analysts across 23 countries to give organizations relevant threat intelligence so they can focus on the threats that matter to their business now and take action.
- Mandiant Advantage Digital Threat Monitoring helps detect and respond to external threats by monitoring the internet, including the deep and dark web, providing early notification of malicious actors targeting an organization and provides notification of data and credentials leaks for quicker response.
- Mandiant Advantage Attack Surface Management discovers and analyzes internet assets across today's dynamic, distributed and shared environments. It is designed to continually monitor discovered assets for exposures and enables intelligence and red teams to operationalize and inform risk management.
- Mandiant Cyber Threat Profile is a service that provides a composite picture of the most important and relevant identified cyber threats an organization is facing and how those threats are likely to materialize, impacting the organization and its partners.

Individually these products and services can provide glimpses into threat actors, the dark web and vulnerable, exposed assets. When used together they can provide security professionals with visibility outside their organization, the ability to identify high-risk attack vectors, malicious orchestration from the deep and dark web as well as campaign execution on the open web. They can also provide contextual information on threat actors and their tactics, techniques and procedures necessary to create a comprehensive cyber threat profile, helping users to stay relentless in their fight to protect their digital assets, their supply chain and their brand.

The M-Trends 2022 report shows that supply chain compromise rose to the second most common initial infection vector in 2021 at 17% of intrusions investigated by Mandiant. Monitoring supply chain vendors for active threat actor chatter and exposures is as important as trying to secure subsidiaries and conducting compromise assessments in connection with a merger or acquisition. Mandiant helps monitor and provide visibility into these complex situations.

The following use cases show how digital risk protection from Mandiant can help protect these complex relationships:

Use case #1

1. Threat Intelligence provides details on an espionage-driven threat actor targeting supply chain compromise as their primary initial infection vector.
2. With this intelligence, a monitor is set up in Digital Threat Monitoring for all supply chain vendors looking for potential malicious targeting. This triggers an alert showing dark web forum chatter targeting both you and your vendor.
3. Attack Surface Management starts monitoring supply chain vendors looking for potential vulnerabilities in external-facing assets. A publicly accessible AWS S3 bucket is identified as being accessible by unauthenticated users.
4. The security team reaches out to the vendor to make them aware of the vulnerable S3 bucket and potential targeting. The security team would also kick off a breach analysis to determine if they have already been breached.

Use case #2

1. Attack Surface Management identifies a Webmin installation that is vulnerable to CVE-2019-15107.
2. Threat Intelligence reports that CVE-2019-15107 has a High Risk Rating and Mandiant has observed exploitation in the wild.
3. The security team updated the Webmin installation and added to a monitor in Digital Threat Monitoring which turns up a conversation from a dark web forum detailing how threat actors were using spear phishing campaigns to get Webmin users to open a specially crafted webpage.
4. Knowing this, the security team initiates incident response actions to investigate a potential compromise.

Whether you are looking to protect supply chain, subsidiary connections or day-to-day operations, digital risk protection from Mandiant offers products or services designed to deliver a comprehensive cyber threat profile with the critical steps needed to prepare for an attack.

Posted in

- Security & Identity
