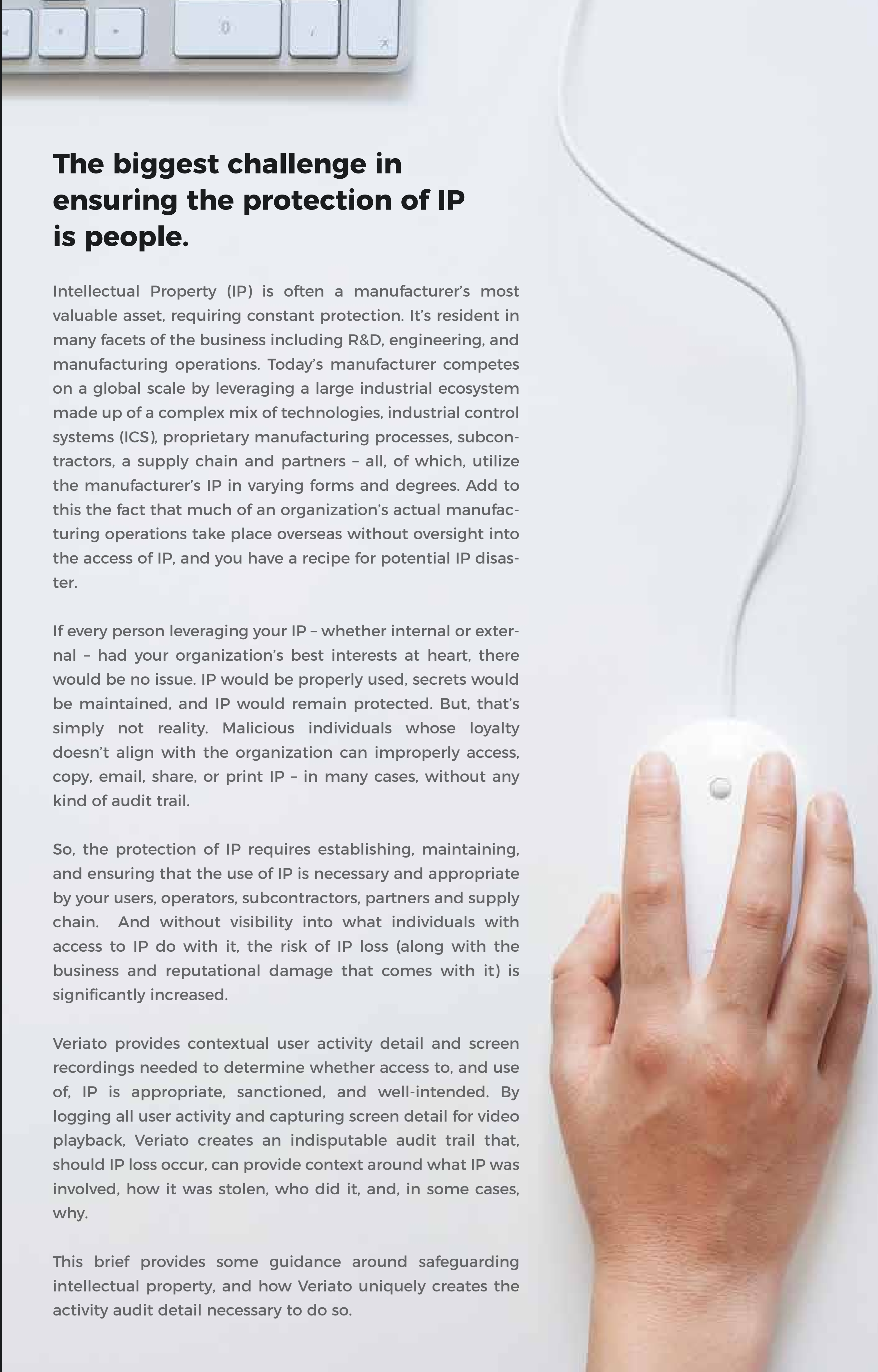
Protecting **Intellectual Property** in Manufacturing

Veriato

www.veriato.com



The biggest challenge in ensuring the protection of IP is people.

Intellectual Property (IP) is often a manufacturer's most valuable asset, requiring constant protection. It's resident in many facets of the business including R&D, engineering, and manufacturing operations. Today's manufacturer competes on a global scale by leveraging a large industrial ecosystem made up of a complex mix of technologies, industrial control systems (ICS), proprietary manufacturing processes, subcontractors, a supply chain and partners – all, of which, utilize the manufacturer's IP in varying forms and degrees. Add to this the fact that much of an organization's actual manufacturing operations take place overseas without oversight into the access of IP, and you have a recipe for potential IP disaster.

If every person leveraging your IP – whether internal or external – had your organization's best interests at heart, there would be no issue. IP would be properly used, secrets would be maintained, and IP would remain protected. But, that's simply not reality. Malicious individuals whose loyalty doesn't align with the organization can improperly access, copy, email, share, or print IP – in many cases, without any kind of audit trail.

So, the protection of IP requires establishing, maintaining, and ensuring that the use of IP is necessary and appropriate by your users, operators, subcontractors, partners and supply chain. And without visibility into what individuals with access to IP do with it, the risk of IP loss (along with the business and reputational damage that comes with it) is significantly increased.

Veriato provides contextual user activity detail and screen recordings needed to determine whether access to, and use of, IP is appropriate, sanctioned, and well-intended. By logging all user activity and capturing screen detail for video playback, Veriato creates an indisputable audit trail that, should IP loss occur, can provide context around what IP was involved, how it was stolen, who did it, and, in some cases, why.

This brief provides some guidance around safeguarding intellectual property, and how Veriato uniquely creates the activity audit detail necessary to do so.

Introduction

The theft of intellectual property is likely at the top of your list of concerns. The manufacturing industry generally shares your concern – IP theft is considered the #1 cyber threat facing manufacturers today, as well as being the top data protection concern . With 90% of data breaches in the manufacturing industry involving IP[2], the focus on IP is justified.

A material 39% of manufacturing organizations experienced a breach in the last 12 months[1], with 38% of organizations affected incurring losses of more than $1 million[1]. While breaches aren't necessarily related to IP, 35% of executives stating they believe IP theft was the primary motive for the cyberattacks experienced by their company[1].

So, what's needed is a means to have complete visibility into every action performed by anyone interacting with IP – every application used, webpage visited, record copied, file saved, print screen generated, and page printed. Only then will the organization truly know whether their IP is secure.

[1] *Deloitte, Cyber Risk in Advanced Manufacturing Report (2016)*

[2] *Verizon, Data Breach Investigations Report (2017)*

IP Protection Key Stakeholders

Ensuring the security of IP isn't just a technical battle; it's as much a responsibility of operations as it is of IT. It takes working together to create policies and procedures, in conjunction with agreed upon technology, to see that users receive appropriate use training, access to IP is correctly granted, and that use and processing of IP is appropriate and can be demonstrated.

Most organizations see a member of IT as the person responsible for protecting IP. But, in many organizations (42%), this responsibility falls to a position within operations[1], demonstrating the need to have both parts of the business working together. Below are the challenges faced by the four most common positions responsible for IP[1]:

CIO – Needs a proactive approach leveraging people, processes, and technology that ensures the protection of IP from both a security and operations perspective.

CISO – Wants a plan to evaluate and manage cyber risks related to IP.

Head of R&D – More concerned with creating IP than protecting it, but desires to keep it secure by relying on IT.

Head of Manufacturing - Is aware of where IP resides, and how it is used – and, generally, by whom - in the manufacturing process. May be overwhelmed by the task of trying to keep IP secure given the complexity of the people and process involved in manufacturing..

What's needed is a technology that cost-effectively addresses IT's need for IP security and Operation's need to maintain the efficiency of the manufacturing process. It should monitor any activity involving IP, aligning with established policy and processes, providing visibility into how IP is used or misused. In the case of misuse, it should also provide context in determining the scope of a breach.

How Veriato Helps Address Protection of Intellectual Property

Veriato helps manufacturing organizations of all sizes assess risk related to IP, ensure safeguards are in place, demonstrate access is appropriate, and providing context should a breach occur. It does so by recording and providing access to detailed user activity data – both within applications used to access and utilize IP, as well as in any other application – combined with robust screen recording and playback.

All of Veriato's activity data is searchable, making it easy for key stakeholders, an auditor, security teams, or IT to find suspect actions, with the ability to playback activity to see before, during, and after the activity in question. Reports can be produced in minutes – typically a fraction of the time needed – and don't require pulling critical resources from other tasks.

Veriato assists with every facet of IP protection, utilizing its detailed visibility into specific user actions related to accessing and processing IP. The following sections breakout how Veriato can assist with ensuring the security of your organization's IP.

Inventory, Classify, and Maintain IP and Corresponding Assets

Before you can protect your IP, you need to have an understanding of what is considered IP, where it resides, how it's used, and who has access to it, whether its distributed and, if so, to whom. This provides critical details to help the organization determine how it should be protected and who should have access to it.

Below are some examples of how Veriato can assist in addressing the managing of IP:

✓ **Where IP Exists** – Veriato can use keyword searches (representing project names, products, etc.) to identify when these IP assets are accessed, which applications are used to interact with it, and where files containing IP reside.

✓ **Who Accesses IP** – Veriato's powerful reporting can quickly identify all users that interact with IP. Activity detail can also be reviewed to understand how the data is shared (e.g. via email, using cloud-based collaboration, cloud storage, etc.) and to whom.

Implement Security and Operational Safeguards

Once you know where your IP is and how it's being used, the next step is to implement safeguards that fall into two distinct areas - cyber security and operational security. Cyber security falls on IT – preventing external attacks, network intrusions, etc. leveraging technical safeguards. Operational security is generally the responsibility of Manufacturing, R&D, and other operations-focused departments and involves establishing employee and contractor policies and procedures for handling IP. The two also work together to define functional roles within the organization in relation to the ownership of and access to IP. Doing so establishes appropriate risk levels with each role and ensures accountability between both groups setting up safeguards.

Below are some examples of how Veriato can assist in addressing the protecting of IP:

✓ **Review Appropriate Use** – Upon establishing roles and access, it's critical to review use to ensure the definitions are correct and do not allow for improper access. Veriato's reporting can identify who is accessing specific IP, providing the ability to drill down into activity data, if needed.

✓ **Analyze User Behavior** – Veriato can look for leading indicators of insider threat activity by analyzing shifts in users behavior and communications, alerting security teams to the potential.

✓ **Delegate Visibility –** Those in charge of operational security may desire to review the activity of employees and contractors themselves, rather than waiting or relying on IT. Veriato makes it easy to delegate the ability to review subsets of monitored users, providing complete visibility into the actions of delegated users.

✓ **Monitor for Inappropriate Use –** Veriato can alert security teams of abnormal activity – such as copying of data, sending of large emails, use of specific keywords, etc. - based on established thresholds to begin the process of investigating a potential breach.

INCIDENT RESPONSE

Manage IP Loss Incidents

It's a statistical probability that your organization will experience an IP data breach. When that happens, it become critical to immediately move into action to minimize the impact of the breach. Understanding what actually transpired brings clarity to determining an appropriate response.

Below are some examples of how Veriato can assist in responding to a breach involving IP:

✓ **Understand the Context of the Breach**

Understanding the means by which an IP asset has been compromised is critical, as it will help determine your remediation efforts. Veriato can pinpoint when IP has been accessed and what was done with it. If a user opens a CAD drawing, takes a screenshot, pastes it into a personal webmail account and sends it off, Veriato is there to see it all happen. Detailed video playback provides visibility into what happed before, during, and after the accessing of IP to help you understand the who, what, and why around the breach.

✓ **Determine the Scope of Loss**

Establishing the extent of loss and its severity is key. Was it a single document or all of the organization's IP? Activity logging, along with playback can provide you with the answers necessary to ascertain the scope of the loss.

Protecting Intellectual Property with Veriato

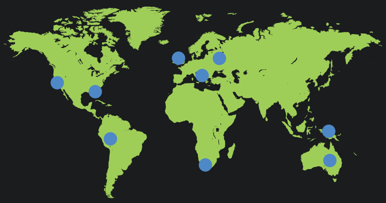
IP in manufacturing is somewhat unique, in that it's shared with so many entities and individuals around the globe in order to create a product. But, even so, it's reasonable for a manufacturing company to desire to take appropriate steps to ensure IP remains as secure as is possible. As long as the only access to and use of IP is performed by someone who both has a legitimate need and only uses that information for the purposes of the organization, your IP is safe.

But, because users with access to IP utilize that data every day, it becomes nearly impossible to tell if and when your organization's may be used inappropriately. Add to that the fact that, while the access to IP may seem appropriate, the cutting and pasting of information into a Word doc saved up on a cloud drive certainly isn't – which means your organization needs to be monitoring and recording all user activity, regardless of application.

Veriato assists with safeguarding intellectual property by providing those in IT and operational security teams with complete visibility into every action taken by the organization's users – and without impacting the operational ability of the manufacturing process. Veriato solutions help to analyze risk; test safeguard policies, procedures, and measures; and review user activity – all in an effort to ensure IP remains protected and to assist with the response when IP data is breached.

To learn more about how Veriato can help you protect your **IP**, contact a Veriato representative today.

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions



Our solutions are deployed in **110+ countries**

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410

Veriato EMEA
3rd Floor, Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL   United Kingdom

https://plus.google.com/+Spectorsoft

https://www.linkedin.com/company/veriato

https://twitter.com/veriato

https://www.youtube.com/SpectorSoft

https://www.facebook.com/VeriatoInc/