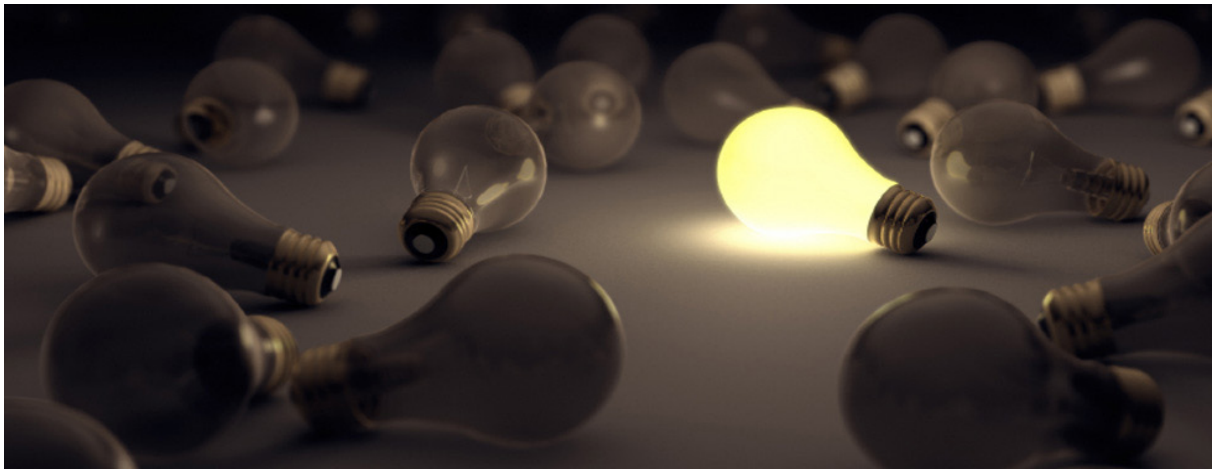
The Age of Enlightenment in Cybersecurity



Securing your data requires an enlightened view of what exactly you're trying to protect.

The Age of Enlightenment that began in the 1600s was about new ways of thinking and of seeing the world. As a result, there were advancements in science, medicine, literature, technology, and philosophy across Europe. Similarly, the Age of Enlightenment for cybersecurity signals a return to first principles. As John Locke wrote in 1690's An Essay Concerning Human Understanding, "It is one thing to show a man that he is in error, and another to put him in possession of truth."

To find this truth, cybersecurity measures must start with visibility–visibility into the thing that organizations are trying to secure. Security teams cannot secure applications, clouds, or SaaS services when they lack visibility into them.

Hackers know this. These visibility gaps are a godsend to attackers–and they have feasted. According to a June 2022 survey from Enterprise Strategy Group, 79% of organizations have experienced a ransomware attack within the last year. According to Surfshark, data breaches increased 70% in Q3 2022.

Enterprises find themselves in a vicious cycle. IT's continuous investments in infrastructure and tools create more opportunities for blind spots, which result in more sophisticated attacks. As enterprises reinvest profits to drive digital transformation, attackers are doing the same. As a result, we are no longer dealing with simple malware. Attack targets and techniques have grown to include account compromise using credentials gained through leaks, attacks, social engineering or spraying, compromise of exposed services such as remote desktop, phishing attacks -- the list of sophisticated hacking techniques is long. With this complexity, the average ransomware payment during the

first five months of 2022 was $925,162, 71% higher than 2021.

Once inside the target, hackers can have patience because they know time is on their side. They move laterally, expanding until they have domain admin and root access. They target servers and other systems. With more access, they target backup systems to delete or compromise files. They exfiltrate data and conduct data mining for valuable information. Then they go for the most obvious targets -- those that are encrypted. Today, hackers have three objectives: decrypt your data, exfiltrate and delete data, and gain control of your domain.

Discovery Tools

Today, tools that aid in discovering these blind spots can provide the source of truth. The latest breeds of security platforms focus on proactive mitigations to increase readiness and resilience and are rapidly adding capabilities for real-time detection and response. These include data security posture management (DPSM) tools to protect the data itself; cloud-native application protection platforms (CNAPP) to protect the infrastructure and network; and secure access services edge (SSE) solutions to apply real-time protections.

Steps for Gaining Visibility

Security leaders now understand that if they can't see it, they can't secure it. This vision must be extended more broadly to encompass additional platforms and more deeply to provide context on the nature of the risk and dangers so security teams can take action to protect the business, including increasing awareness of security needs.

• **Ensure you have a cloud inventory**. Invest in developing a comprehensive inventory of your public cloud workloads and infrastructure so you understand your application landscape. Look for a cybersecurity asset management platform that provides a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies.

• **Improve your cloud security posture**. Ensure you understand your cloud security posture, workloads, and application exposures. For example, use CNAPP solutions that deliver complete visibility and context for your cloud so your teams can proactively identify, prioritize, remediate, and prevent risks to your business.

• **Conduct a data risk assessment**. Gain visibility into your data, determine whether any of it is exposed, and develop a plan to secure sensitive data from exposure and vulnerabilities. Achieve least privilege by pinpointing overly permissive access and minimize sprawling sensitive cloud data.

• **Improve your data security posture**. Be sure you understand your data security posture, including where sensitive data exists, who can access it, where it flows, and critical exposures that increase your threat surface and impact your cyber resilience. A DSPM solution can deliver complete visibility and context of your data so your teams can proactively identify, prioritize, remediate, and prevent the risk that sensitive data exposure represents.

By now, we may suspect that the drive to transform has left us more exposed and vulnerable than ever. Gaining visibility is the first step to enlightenment in cybersecurity, and this will empower organizations to better protect their most critical assets and improve their security postures.