Infoblox

SOLUTION NOTE

Application Discovery

Discover and regulate malicious and inappropriate applications (*shadow IT*)

FACTS & FIGURES

- **1 in 5 organizations experienced a cyber event** due to an unsanctioned IT resource.[1]
- **40% of employees** use are using communication or collaboration tools that aren't explicitly approved by their company. [2]
- **65% of those working remotely** before the pandemic use tools that are not company-approved. [2]
- **61% of employees aren't completely satisfied** with their company's technologies. [2]
- **Shadow IT** may cause organizations to run afoul of regulations (i.e. PCI-DSS, GDPR, HIPPA, SOX) [4]

Challenges

Once a feared unknown to be feared and blocked, Shadow IT has become something that organizations are striving to monitor and understand. User preference for alternatives to official applications often reflects a need for education or an opportunity to improve productivity, be more competitive, and better achieve the organization's mission.

But defenders must still address the risk of intentional or unintentional use of malicious or inappropriate applications. Are limitations of the official VPN driving workers to experiment with potentially dangerous VPN alternatives? Is an insider attempting to steal IP or simply backing up to cloud services with good intentions? Could users be exposed to malware through an unapproved social, file storage, or other application or service? Is a vendor or partner with less mature security practices requesting collaboration using a high-risk tool?

BloxOne™ Threat Defense Advanced

"Application Discovery" is a key feature of the BloxOne Threat Defense Advanced package that addresses these challenges. It starts by providing organizations with visibility to help them identify high-risk applications in use across the network, and by who or what device. It then provides a summary description of each detected application to provide decision-makers with important details so they can perform the necessary risk/benefit analysis for continuing to allow users access, or not.

> ***"Visibility is the first priority; discover what apps are actually in use on your networks."*** [3]
>
> 'Don't Fear Shadow IT: Embrace It', Forbes, May 18, 2022

While most organizations will wisely take time to understand the information revealed through Application Discovery, they typically need to take a range of actions to safeguard the organization and support regulatory requirements. BloxOne Threat Defense Advanced allows security teams to mark applications as 'Approved' or 'Unapproved' to simplify future monitoring and, when necessary, implement security controls to block or take other actions when a specific application is uses by select users, groups, or company wide.

1 - "Perception Gaps in Cyber Resilience: Where Are Your Blind Spots?", Forbes, 2019 (https://www.ncsc.govt.nz/assets/NCSC-Documents/Perception-Gaps-in-Cyber-Resilience.pdf)
2 – "2021 Digital Workplace Trends & Insights", Breezy, 2021 (https://www.beezy.net/blog/rise-shadow-it)
3 – "Don't Fear Shadow IT: Embrace It", Forbes, 2022 (https://www.forbes.com/sites/forbestechcouncil/2022/05/18/dont-fear-shadow-it-embrace-it/?sh=6264e4027192)
4 – "How Shadow IT Can Keep Compliance Efforts In The Dark", Forbes, 2022 (https://www.forbes.com/sites/forbestechcouncil/2022/07/19/how-shadow-it-can-keep-compliance-efforts-in-the-dark)

More than Shadow IT: Even Good Applications Can Go Bad

From SolarWinds to Microsoft, we have plenty of evidence about the potential risks posed by any vendor's application. So, while there is a clear risk of compromise through the use of a malicious or high-risk application, it can also happen from using a legitimate 3rd party application when the vendor is breached.

One of the first questions the organizations must ask is "do we use that applications, and BloxOne Threat Defense Advanced can provide those answer, on-demand". And it enables immediate, effective response options, even if they are only temporary while additional threat and risk assessments take place.

A good example of a high-risk application category is cloud backup and storage, which is more commonly used for file sharing, an essential part of business and government operations. Despite your organization's preferences for file storage or sharing services, each organization you do business with will have its own preferences, posing both inbound (i.e. malware) and outbound risk (i.e. data loss). This reality limits the amount of control that can be placed on these kinds of services without impacting the user performance. Being able to quickly identify the applications that may have been involved can be key to a fast and effective threat investigation or incident response.

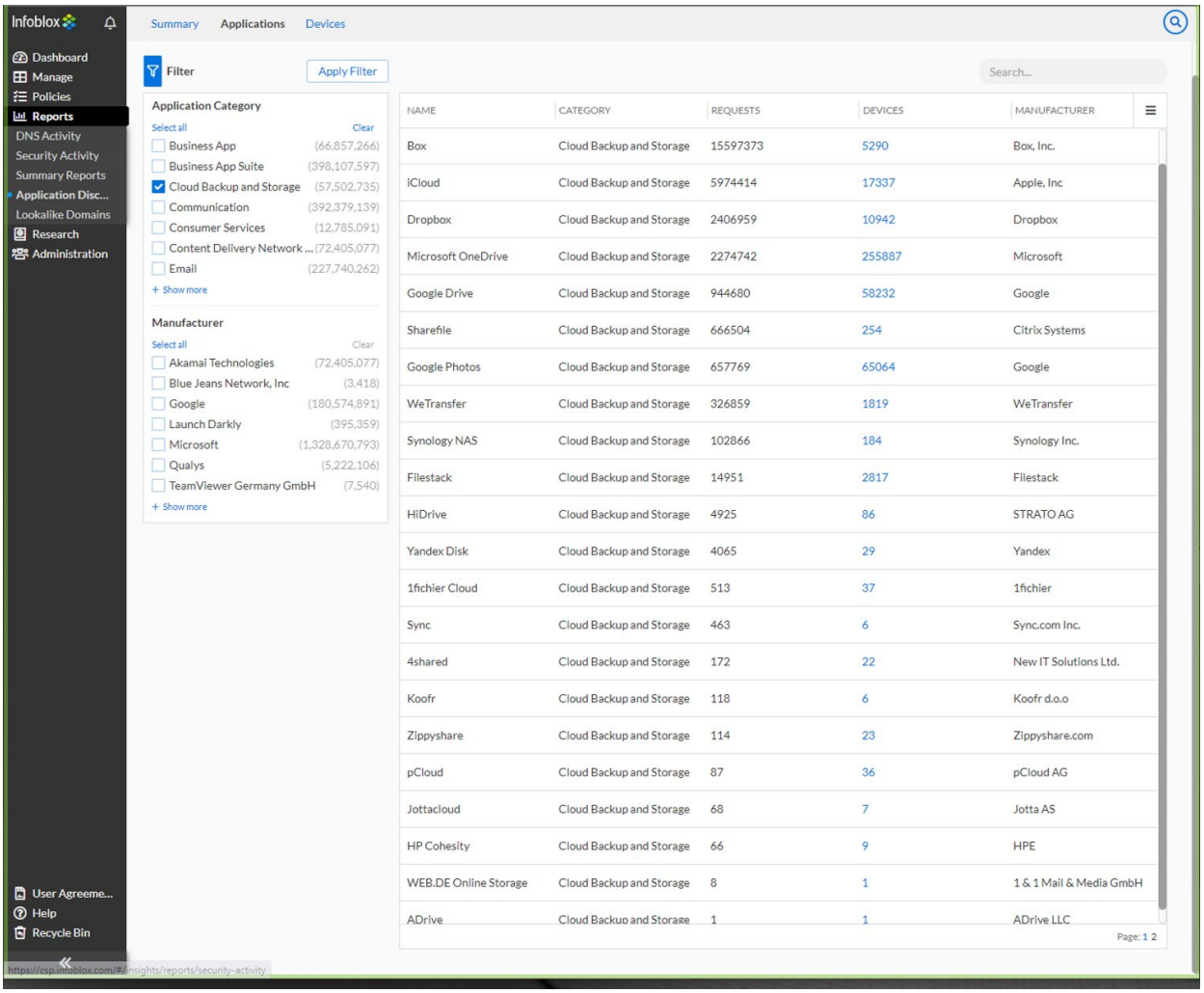

Figure 1: Customer screenshot revealing more cloud storage services in use than anticipated, including the Russian-based Yandex Disk service that presented unacceptable security and compliance risks. But comprehensive application visibility also helps defenders respond to other situations, such as when a serious vulnerability is found in a legitimate, but unofficial/unmanaged, application.

Insider Threats, Intentional or Accidental

Security tools need to be woven together into a cohesive defensive strategy. Yet DLP, NGFW, SWG and other defenses have a limited view of common Insider Threat activities such as the use of encrypted social networking applications, personal email, alternative VPNs, and other cloud services.

Operating at the DNS-layer, BloxOne Threat Defense Advanced can reveal when these high-risk services are in use, providing the necessary details to help SecOps or NetOps to monitor activity, drive compliance, and prevent malicious behavior.

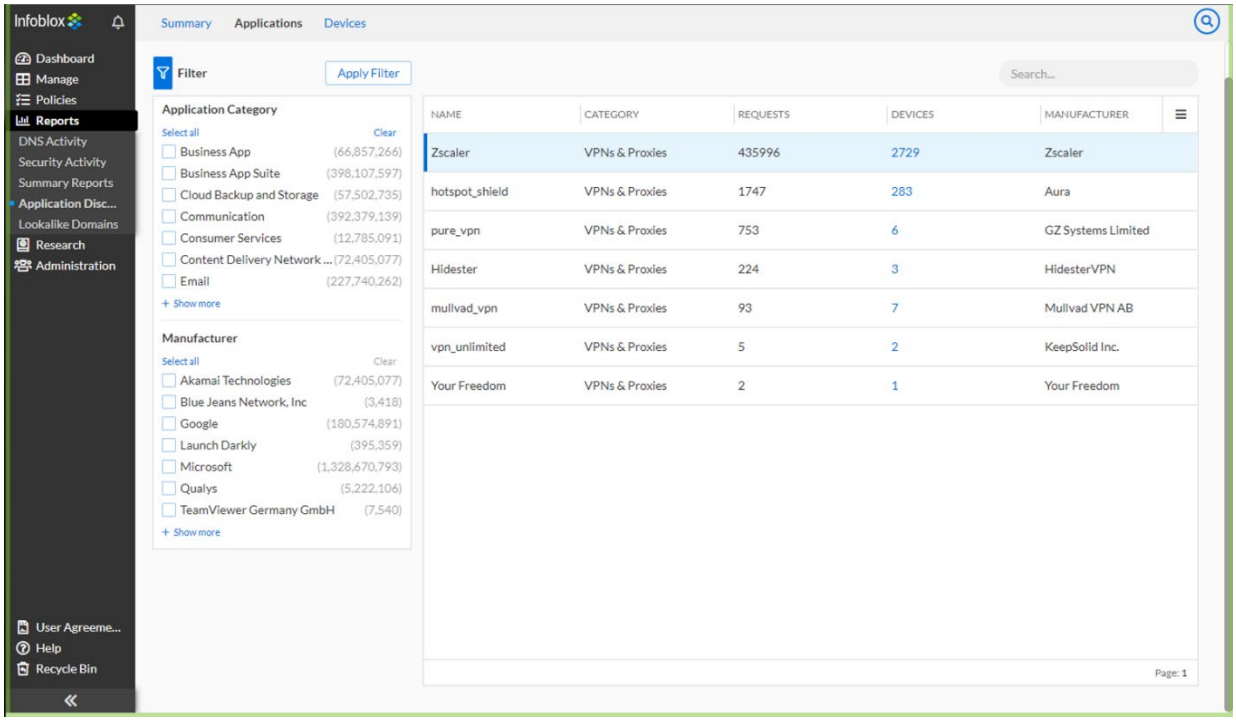

Figure 2: On-demand access to up-to-date app usage helps defenders respond to many situations, such as when a vendor reports a serious application vulnerability in an otherwise unmanaged app.

Endless Scenarios and Unending New Risks

Existing applications are constantly evolving, and new services frequently enter the market. Combined with the boundless creativity of users and cybercriminals, the risks to the enterprise are plentiful and varied. BloxOne Threat Defense Advanced provides a breadth of capabilities to deliver the visibility and control needed to protect the organization while supporting productivity needs.

In addition to Application Discovery, BloxOne Threat Defense Advanced uses extensive DNS visibility with machine learning and AI capabilities to detect threats other defenses never see. Meanwhile, the Threat Intelligence Data Exchange (TIDE feature can share threat intelligence across the security stack to uplift all defenses, while also offering to automate incident response to leverage other parts of your security ecosystem.

Check here for more information on BloxOne Threat Defense Advanced and how it can fill gaps in your defenses even as it makes your existing security tools more effective and efficient.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com