The Future of Real-Time Monitoring

Mike Kelly
CEO | ProcessBolt
Gaurav Gaur
CTO | ProcessBolt

Cloud computing and coronavirus are among the most consequential forces impacting cybersecurity today. Together, they have created an "endpoint explosion." Yesterday's periodic measures are important; however, the only way to manage today's cyber risks is with a paradigm shift to real-time monitoring.

CORONAVIRUS ACCELERATES CLOUD MIGRATION

Cloud computing was one of the fastest-growing IT spend categories at the start of 2020, with a forecasted CAGR of 29%. Then the coronavirus pandemic hit. While global IT spending is now expected to decline by 8%, cloud spending grew 37% in Q1 of 2020.

Clearly, the pandemic is accelerating cloud migration. Almost by definition, cloud computing facilitates social distancing. It also supports the broader move towards a reimagined, reduced-density work environment, a trend that is likely to continue even after the pandemic ends.

ENDPOINT EXPLOSION

Cloud migration and coronavirus are creating an explosion of endpoints. More endpoints mean more risk exposure. The cloud makes it easy to quickly create internet-facing assets such as websites and databases, all of which have vulnerable attack surfaces. The cloud creates more digital access points for employees, customers, and vendors. It facilitates new and wider application adoption, adding additional cyber risk endpoints.

Coronavirus contributes even more to the current endpoint explosion. By June 2020, 42% of the U.S. labor force worked from home full-time. It is now estimated that 25 to 30% of the labor force will work from home multiple days a week by the end of 2021.

These new endpoints introduce an overwhelming number of new cyber vulnerabilities and new attack surfaces on which threat actors can prey.

FROM PERIODIC TO REAL-TIME

Periodic cybersecurity measures are a necessary foundation. Security enhancements such as employee training, stronger passwords, access controls, firewalls, pentesting, and vendor risk scoring are important. But they cannot keep pace with the growth in attack surfaces initiated by cloud computing and the pandemic. Now, the best hope for effective cybersecurity management is real-time monitoring.

CONTINUOUS MONITORING

Real-time monitoring cross-checks against aggregated threats, identifies red flags, and continuously monitors for potential risks. Ideally, these systems:

- Take a hacker's view of the gaps across all potential attack surfaces.
- Pinpoint blind spots and vulnerabilities across the full digital ecosystem: enterprise, customers, and vendors.
- Run 24/7.
- Provide immediate notification of unauthorized activity.
- Enable rapid remediation and stop potential threats before privileged data is lost.
- Are cloud-based with no software to install.
- Are easy to launch. Administrators can load their internet-facing assets into a dashboard, and the system takes it from there.

MID-TERM TRENDS

Three additional trends tell us the move toward real-time monitoring will accelerate. This is due to the demand for digital interconnectedness, growing cyber threat sophistication, and the declining relevance of threat attribution.

DIGITAL INTERCONNECTEDNESS

The need for digital connections among companies, customers, and vendors will continue to grow. This underlies the strategic mandate of digital transformation. The cloud serves this need by making it cheap and easy to create websites and databases.

Digital transformation, however, exposes enterprises to a broader threat landscape. While digital ecosystems are a strategic business necessity, they also introduce a broader range of cyber risks.

CYBER THREAT SOPHISTICATION

Cyber threat levels will continue to rise faster than enterprise defense capabilities, leading to growing cybersecurity risks. Threat actors, ranging from autonomous individuals to nation-states, will continue to successfully find and exploit gaps in the increasingly connected global landscape.

State-sponsored adversaries now employ some of the world's best minds. They hijack proprietary wireless protocols and connected devices (IoT, VoIP phones, wireless mice and keyboards, printers) to penetrate corporate networks or capture keystrokes and mouse actions. They even use rival nation-state infrastructure to house, deploy, and disguise their attacks.

DECLINING THREAT ATTRIBUTION RELEVANCE

It is increasingly difficult to attribute cyber threats to specific actors. Advanced threats increasingly originate from userland malware. Expertise in userspace tactics, techniques, and procedures are far more relevant than the ability to identify malware creators. Every node in the digital ecosystem, from enterprise to customer to vendor, is a potential point of an incursion. Real-time threat anticipation, detection, and response at any endpoint are now the front lines of cybersecurity.

STRATEGIC IMPLICATIONS

Cybersecurity is adapting to the globally connected landscape and the associated threats in six ways. These six ways are as follows:

1. Speed: Increasingly, the driving success factor in cybersecurity is speed. How quickly can we detect and respond to an emerging threat? Even better, how quickly can we detect anomalies in our cyber ecosystem and launch effective responses before the threat spreads?
2. Real-Time Monitoring and Streaming Analytics: The key to cyber defense speed is real-time endpoint monitoring and streaming analytics. Periodic pentesting, vendor cybersecurity surveys, and vendor risk scoring will decline in relevance. They are slow relative to real-time risk detection and assessment across an ever-changing risk landscape.
3. Increasing Role for AI: Companies cannot quickly respond to every cyber alert they receive. Manual alert triage processes are often overwhelmed by alert volumes. AI is increasingly a viable solution, especially for real-time streaming analytics. It can be used to automate threat-hunting and first-round alert triage. This in turn reduces the number of false positives and helps security operations teams focus on high-priority threats.
4. Cybersecurity Integration: Cybersecurity complexity necessitates the utilization of a diverse range of technologies. Endpoint cyber threat management processes vary for the enterprise versus customers versus third-party vendors. Within the enterprise, threat management varies for employees, employee devices, manufacturing and distribution control systems, IoT-enabled

products, and so on. These diverse cybersecurity sub-systems will increasingly be integrated. Data ingestion will be integrated through data lakes. AI and streaming analytics will be applied to these data lakes. Digital ecosystem monitoring and insights will be aggregated by unifying platforms.

5. Cybersecurity Partnerships: Enterprises will increasingly establish agreements with vendors and customers to detect and respond to cyber threats. Business contracts will increasingly require both parties to share real-time threat intelligence.

6. Outsourcing: Security Operations Centers (SOCs) already struggle with staffing. They can be overwhelmed by alert volumes and manual processes. SOC staffing problems will intensify with the growing importance of real-time, AI-enabled, streaming analytics. As a result, more companies will outsource aspects of their real-time security monitoring needs that cannot be sufficiently staffed in-house.

CONCLUSION

As cyber threats become more numerous and sophisticated due to cloud migration and coronavirus, companies will increasingly look to real-time monitoring for cyber protection. More broadly, cybersecurity will play an increasing role in creating and protecting competitive advantage. Companies that better understand and respond to their ever-changing cyber threat landscape will be favored by customers, vendors, employees, and investors. They will experience lower data breach costs and higher returns on their cyber risk management efforts. Cybersecurity strategy must embrace real-time endpoint monitoring and streaming analytics. Companies that lag here surrender a powerful competitive opportunity. IT budgets in 2021 should not only favor cloud computing. They must also fund real-time monitoring enhancements.

ABOUT THE AUTHORS

Mike Kelly *is the CEO of ProcessBolt, Inc., a SaaS company that automates regulatory compliance and third-party risk assessments both for companies issuing assessments and those responding to assessments (www.processbolt.com). Prior to joining ProcessBolt, Mike led and ultimately grew and sold several software and analytics businesses in a variety of industries from healthcare to business and legal services.*

Gaurav Gaur *is the CTO and co-founder of ProcessBolt. He has an extensive background in cybersecurity, vendor management and software engineering. Before starting ProcessBolt, Gaurav was the VP of Software Development at NetSPI Inc., a cybersecurity-focused software and consulting firm, and he was responsible for the overall software development strategy and product roadmap of enterprise-grade cyber vulnerability management systems.*

ProcessBolt