Mike Kelly
CEO | ProcessBolt

Gaurav Gaur
CTO | ProcessBolt

Digital transformation has been a driving component of business strategy for the last several decades. Every business function was impacted, from finance to human resources and from manufacturing to sales and service. Current global dynamics such as climate change and COVID have increased the demand for digital transformation. For example, cloud computing can reduce a company's carbon footprint, and expansive remote access supports work-from-home practices.

For decades now, the risks associated with digital transformation are consistently assessed as low relative to the rewards. However, the growing onslaught of cybercrime is forcing businesses to reevaluate. Cybercrime frequency and severity are alarming. Enterprises are moving urgently to close the security gaps created by rapid technological advancement.

Furthermore, the prevalence of breaches involving third parties means that managing your organization's attack surface may not be enough. You must monitor your vendors' too.

Exposed Flaws

Two traditional approaches to cybersecurity management are vulnerability management and penetration testing. Increasingly, the limitations of these two methods are being exploited by hackers.

Vulnerability management tools require precise inputs, which means they only protect against known vulnerabilities. But what about the unknown risks associated with more rapid digitization, remote workers, SaaS, and a greatly expanded off-premises cloud computing footprint?

Penetration testing digs in and can expose previously unknown vulnerabilities; however,t semi-annual pen testing is insufficient when confronting adversaries who continuously scan corporate exposures. They discover long-forgotten touchpoints with the internet, identify new touchpoints or vulnerabilities within

minutes of their creation, and launch potentially crippling attack vectors within hours. Current vulnerability management and pentesting practices are struggling to meet the challenge.

An Emerging Cybersecurity Enhancement

A new approach is rapidly gaining momentum in cybersecurity. It is called Attack Surface Management (ASM). Its growing popularity is rooted in its ability to reach beyond known and controlled assets. ASM identifies forgotten assets and quickly generates alerts on new vulnerabilities as they emerge.

ASM readily scales as companies add employees, vendors, customers, equipment, software, SaaS services, networks, and so on. It only needs to be pointed in a general direction—just load one or more of your domains. Then ASM looks for your other domains and all internet-facing assets associated with all your domains. Since ASM is essentially continuous, new assets are found and evaluated as they emerge.

An abbreviated table of attack surface or internet-facing assets is provided below. It sorts assets into five categories and gives examples for each.

Attack Surface or Internet-Facing Asset (Abbreviated)

Category	Asset
Network Infrastructure	Network Servers
	Data Storage
	Routers, Switches
	WiFi Access Points
	Firewall / Intrusion Prevention System (IPS)
	VPN Gateway
	Intrusion Detection System (IDS)
Applications	Active Directory
	Identity and Access Management Services
	DNS and DHCP
	Mail and Messaging
	LOB Applications
Endpoints	Windows, OSX, Linux Clients
	Employees, Customers
	Virtual Desktops
	Smartphones & Tablets
	Printers
	POS Devices
	VoIP Phones & Video Conference
	Physical Security Equipment
	IoT
Cloud	Cloud-Based Messaging
	Cloud Storage
	Virtual Private Cloud
	SaaS
Supply Chain	3rd Party Vendors: 1st Tier
	3rd Party Vendors: 2nd Tier (4th Party Vendors)

Most organizations have many thousands of cyber exposures, from remote workers and supply chain vendors to servers and subdomains, from APIs and bad security certificates to forgotten cloud storage buckets and vulnerable web applications. While the list goes on and on, ASM continuously explores the entire attack surface and alerts you to new assets and vulnerabilities. It maintains the attack surface inventory for you.

The above table often represents many thousands of vulnerabilities per company, and it is in a constant state of flux and growth. The sheer volume and complexity of a company's attack surface create a tremendous opportunity for . The challenge is to choose and deploy tools and methods that fully match the magnitude of this exposure.

The Hacker's Perspective
ASM does not stop with a comprehensive, up-to-date picture of your attack surface. It takes a hacker's point of view and asks: Which tools can a hacker apply to this attack surface to maximize damage or ill-gotten gain?

The hacker's perspective is created in two steps. First, a comprehensive list of attack vectors is maintained. An illustrative list is provided in the table below.

Potential Attack Vectors (Abbreviated)

Unpatched/Obsolete Systems or Software	Weak or Shared Passwords
Misconfigured/Unconfigured Systems or Software	Denial-of-Service (DoS)
Misconfigured Network (e.g., database publicly available on the internet)	Spam
Shadow IT/Rogue Assets	Phishing
Invalid or Stolen Certificates	Social Engineering
Zero-Day Vulnerability	IP Leakage

Second, each attack vector is assessed relative to each point on the attack surface. The ASM constantly asks:

- Is point "X" on the attack surface vulnerable to attack vector "Y?"
- Has point "X" on the attack surface been breached?
- Is point "X" experiencing suspicious activity, such as increased scanning?
- What is the level of risk associated with each vulnerability?

By asking the right questions, ASM can pinpoint which assets are most vulnerable, help you remediate potential threats before they occur, and identify unauthorized or suspicious activity. In other words, ASM finds your blind spots, helps you repair them, and alerts you to emerging threats.

Alert Fatigue

The latest generation of ASM tools helps to reduce "alert fatigue." Prior generations of vulnerability management software were too reliant on generic inputs such as "bad" IP addresses that were not scrutinized. Cybercrime is now far too complex and fast-paced to rely on IP addresses to generate alerts. It is far more effective to screen for potentially malicious activity at your attack surface. When you assess potential threats from a hacker's perspective, you are more likely to prevent or detect intrusions and generate fewer false positives in the process.

The Cyber Priority

Recent high-profile breaches teach several hard lessons. First, digital security lags digital enablement. Very few firms can claim the reverse, where their security sophistication is better than their digital enablement of functional processes.

The implication is straightforward: your cybersecurity learning curve must accelerate to catch up with your digital enablement. If digital enablement continues to outpace your cybersecurity development, then your cybersecurity risks are too high.

Unknown and Forgotten Risks

Second, many recent or high-profile breaches are linked to unknown or forgotten vulnerabilities. In other words, companies are not aware of such exposures until it is too late. The recent Colonial Pipeline breach is a good example. DarkSide gained access via an unused or forgotten employee VPN. The simple solution would have been to detect and close the unused port. Sure, the port should have had stronger password protection and monitoring, but the higher priority is to have no forgotten ports in the first place!

The Equifax breach is a classic example of a forgotten exposure. Although Equifax knew Apache Struts, a web-building application, had prior security risks and released subsequent patches, they lost track of some legacy Apache Struts components on older yet still active websites, thus exposing Equifax to hackers.

Vendor Cyber Risk

Third, if you are not watching your vendors closely, you have a severe risk exposure. They represent a major attack surface vulnerability. The most notable recent example of this risk is the SolarWinds hack, where a remote access tool was inserted into a software update. When SolarWinds customers installed it, a malicious backdoor into their networks was created.

But the high sophistication behind the SolarWinds attack makes it a less relevant example than the California DMV hack. One of their vendors, Seattle-based Automatic Funds Transfer Services (AFTS), was used by the CA DMV for address verifications. When hackers gained access to AFTS, they also accessed 20 months of California DMV data, including name, address, license plate, and VIN files.

The ParkMobile breach is similar. A third-party software vendor's vulnerability was used to gain access to ParkMobile's data.

The Blackbaud ransomware attack illustrates another form of the severe risk posed by supply chain vendors. Blackbaud is a cloud technology company used by colleges, universities, and non-profits. Customer data, including bank account data, was stolen from dozens of universities, hospitals, and other high-profile organizations like NPR.

Even though Blackbaud paid the ransom to protect its customers, there is no guarantee the hackers destroyed the stolen data after they were paid. In the end, the legal consequences could be even more consequential for Blackbaud, as 28 class actions are now moving forward in a unified legal case against them.

Embrace ASM

Companies must adopt a sophisticated, multi-dimensional approach to cybersecurity. Yes, employee, customer, and vendor access to company assets must be carefully managed. And of course, the latest firewalls and website security systems are critical.

But hackers have made it abundantly clear: traditional access protection methods are not enough. To beat hackers, you need a system that thinks like a hacker. You need to crawl your site like a hacker, find internal and vendor vulnerabilities, assess their severity, and address them. And you need to do all of this in real-time. This approach not only discovers forgotten or newly created vulnerabilities, but also detects suspicious activity from new hacker attack vectors.

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 to 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. He was responsible for the overall software development strategy and product roadmap of enterprise-grade cyber vulnerability management systems.*

ProcessBolt