Lookout®

WHITEPAPER

Integrating security from endpoint to cloud

Your security infrastructure has changed

Apps and data once resided in data centers and everyone worked from an office. Your employees connected to internal networks using company-issued laptops or desktops. With a security perimeter, you were able to control data flow and protect critical assets. By managing endpoints, you knew what was stored and used on them.

All that changed with cloud technology and remote work. Today, data goes wherever it's needed. Workers now expect effortless access to whatever they need from anywhere and on any device. To tap into this boosted productivity, many organizations relaxed their security stance in favor of greater cloud access.

This is a total inverse of cybersecurity as we knew it. The data center and your corporate perimeter are no longer the center of the universe. Instead, users, endpoints, devices and apps are in the middle of the cloud.

Consequently, even though your apps and data have left the building, you're still the gatekeeper and shoulder the responsibility for protecting sensitive corporate data and devices while respecting the privacy of users.

Cybersecurity has been turned upside down

It's impossible to see the risks when you don't know what you're up against. The legacy approach to security relies on your perimeter for visibility. But users are now everywhere and using networks and devices you don't control to access your data in the cloud. Whatever visibility you had is now gone. Left unresolved, little – if anything – is under your control.

Currently, security from endpoints to the cloud involves multiple standalone tools that solve specific problems. This creates complexity and inefficiency. Juggling dozens of security tools – with each unaware that the other exists – increases the risk of unintentional misconfigurations that leave organizations vulnerable.

With users no longer working from their offices, many organizations relied on virtual private networks (VPNs) to enable access. While they connect users to on-premises apps from anywhere, VPNs perilously assume that every user and device is trustworthy. Unfortunately, this is a false and dangerous premise. VPN leaves your entire infrastructure – and everything connected to it – extremely vulnerable.

The traditional security approach offers no unified visibility or insight into the security posture of users, endpoints, apps and data. As a result, it cannot deploy dynamic access that adheres to a zero-trust framework, a critical component of modern security.

Mired in the momentum of mediocrity, the traditional approach to security offers only a fraction of what's required to effectively secure enterprise organizations from endpoint to cloud.

> "Your users, workloads, applications, and data are in the cloud. Why isn't your security?"

Neil MacDonald
Vice president, distinguished analyst and fellow emeritus
Gartner

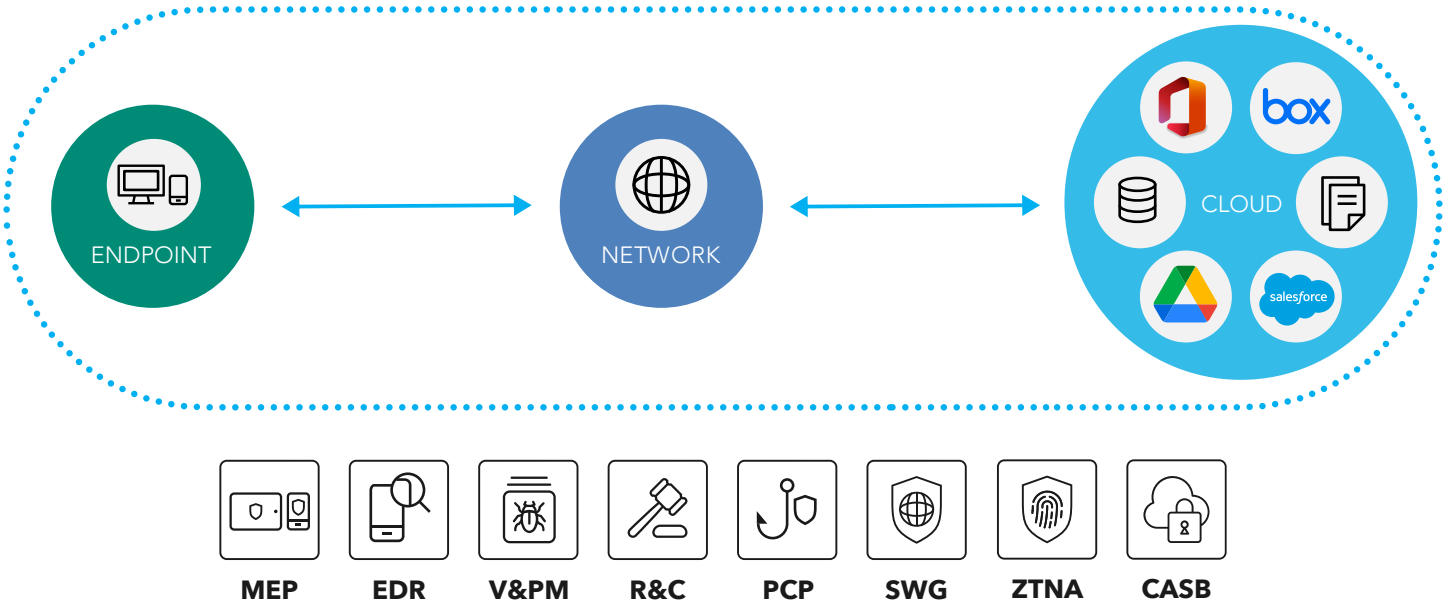
The Gartner Security & Risk Summit 2020.

Minimize business risk

With data going wherever it's needed, organizations require security that provides the visibility and control once existed inside the perimeter. This is the only way to minimize business risk. Achieving this requires integrated security that protects your enterprise data from endpoint to the cloud and ensures user privacy.

There are three essential factors to consider that will minimize your business risk:

1. Complete visibility. The first step to securing your data is knowing what's going on. This requires visibility into the risk levels of your users, endpoints, apps and data, ensuring that you have control and comply with regulations.
2. Unified insights. Standalone tools make cybersecurity unnecessarily complex. As a result, threat telemetry must be consolidated into a single platform so you can write consistent policies across your organization. This also enables you to hunt for threats and investigate advanced cyberattacks with ease.
3. Dynamic secure access and collaboration. Your workers demand quick and seamless access to whatever data they might need to stay productive. To ensure your data stays secure while enabling productivity, it is important for you to be able to dial-in dynamic zero-trust access controls from anywhere and on any device.



Integrated endpoint-to-cloud security

"Why would I have a cloud access security broker, another product for secure web gateway, and yet another for zero-trust network access? I don't need three or four different products cobbled together. They will converge."

Neil MacDonald
Vice president, distinguished analyst and fellow emeritus
Gartner

The Gartner Security & Risk Summit 2020.

Data protection from endpoint to cloud

To achieve endpoint-to-cloud visibility, insights and control, organizations require perimeter security capabilities delivered from the cloud. In 2019, Gartner introduced the Secure Access Service Edge (SASE), a framework that addresses these challenges and calls for rolling multiple security solutions into one integrated architecture.

As a result, vendors have taken it upon themselves to define which best-in-class security capabilities to roll into their SASE models. Unfortunately, most fall short by only addressing one aspect of the complete work-from-anywhere security challenge.

Some offer cloud and network security but do not include endpoint security. Others have basic access controls without understanding user behaviors. And most don't offer advanced data protection that works no matter how data is accessed or shared.

Your goal is to secure data, comply with data protection regulations and respect user privacy. This can only be achieved by a unified platform that delivers security from endpoint to cloud. You need rich telemetry from endpoint security, user behavior analytics from the cloud, on-premises apps to be included in the new security model, and advanced data protection throughout.

"These are not separate problems, nor should they require separate vendors and separate solutions."

Neil MacDonald
Vice president, distinguished analyst and fellow emeritus
Gartner

The Gartner Security & Risk Summit 2020.

Continuous risk assessment: Mobile endpoint security

Tablets, smartphones, Chromebooks, and other personal mobile devices are now an essential part of how we work and manage our personal lives. As a result, mobile security is critical to your overall security posture.

For example, personal mobile devices are much more susceptible to phishing attacks, making them a prime target for threat actors looking to take over accounts and invade your infrastructure.

This illustrates why the zero-trust approach to mobile endpoint security is essential. Mobile endpoints are now commonly used by your workforce to connect and access enterprise data. By continuously monitoring mobile endpoints to assess their risk, you can enforce zero-trust access immediately when something goes wrong.

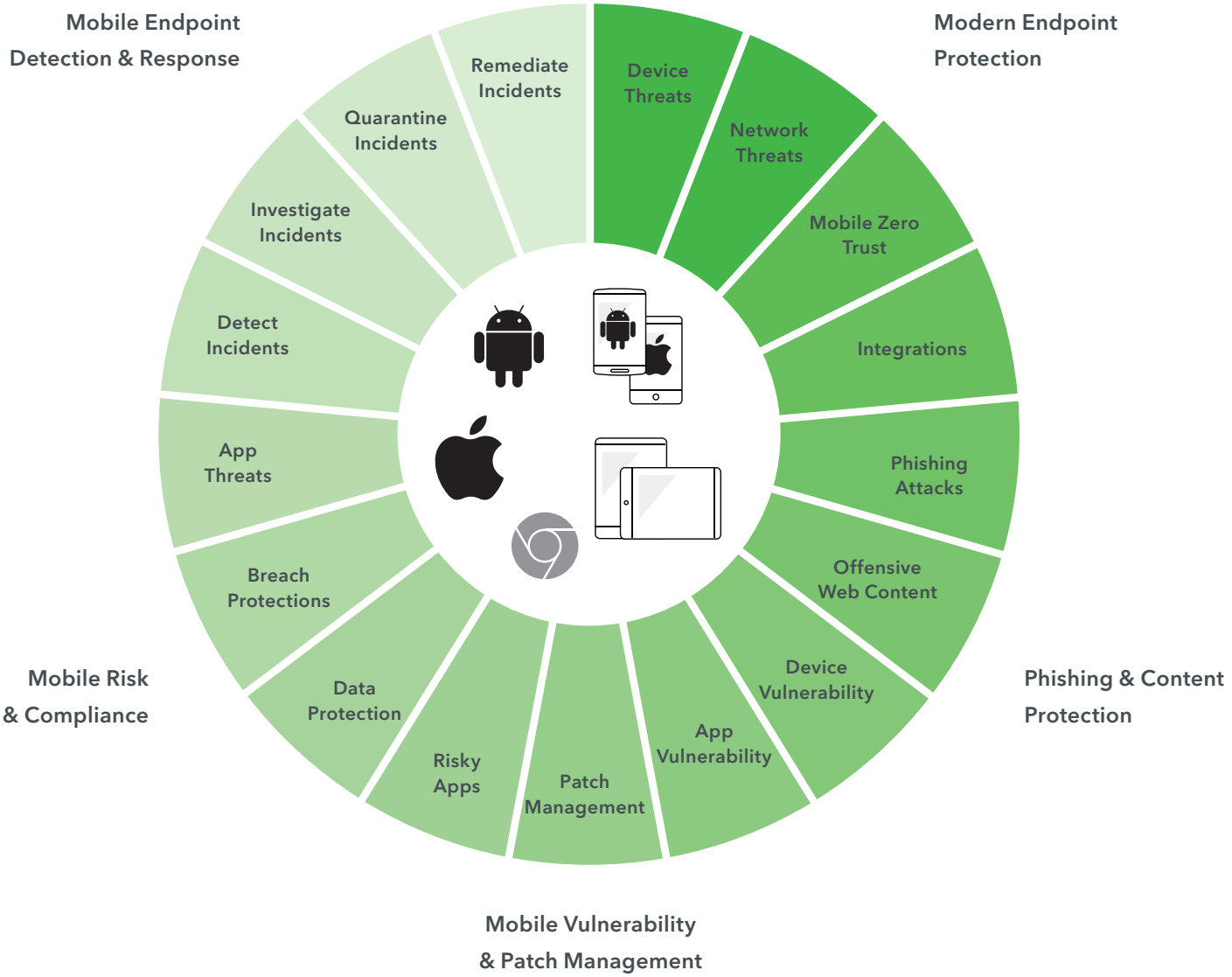
Endpoints also provide rich telemetry that enables you to leverage big data and machine intelligence. This lets you detect and respond efficiently to cyberthreats, even if you've never encountered them before. And by leveraging data, you don't need to scan content for threats and compromise user privacy.

"Gartner forecasts that over the next five years, the SASE market will grow at a CAGR of 42%, reaching almost $11 billion by 2024."

Gartner

Forecast Analysis: Gartner's Initial Secure Access Service Edge Forecast, 26 August 2020

The critical role of mobile device security in the endpoint-to-cloud model



Understanding user behavior: Cloud access security broker

Cloud apps are the reason your employees can work from anywhere using any device. But each app handles data differently and has unique settings. Your organization needs complete visibility and control across all your cloud apps and services to secure your enterprise data and prevent data loss.

Cloud access security broker (CASB) gives all this back to you. A cornerstone of endpoint-to-cloud data security, CASB provides insights into how users normally behave so you can detect and respond to anomalous behaviors and stop insider threats and unintentional malicious actions. It also scans inbound and outbound content to detect viruses, malware and ransomware and infected content is automatically quarantined.

User and entity behavior analytics

UEBA is another important CASB capability. UEBA continuously assesses users, devices and activities to establish a baseline of acceptable behaviors.

When behaviors exceed baseline thresholds, CASB alerts you in real time so you can investigate potential indicators of a malicious insider or compromised account credentials. Other indicators include excessive file downloads, multiple unsuccessful login attempts, logins from new or restricted locations.

Know the security posture of your clouds

With visibility into the security posture of the cloud infrastructure and apps, it's simple to enforce data protection policies. Cloud security posture management (CSPM) and software-as-a-service security posture management (SSPM) automatically assess and remediate SaaS and IaaS environments to detect misconfigurations and maintain security guardrails to stop account compromise.

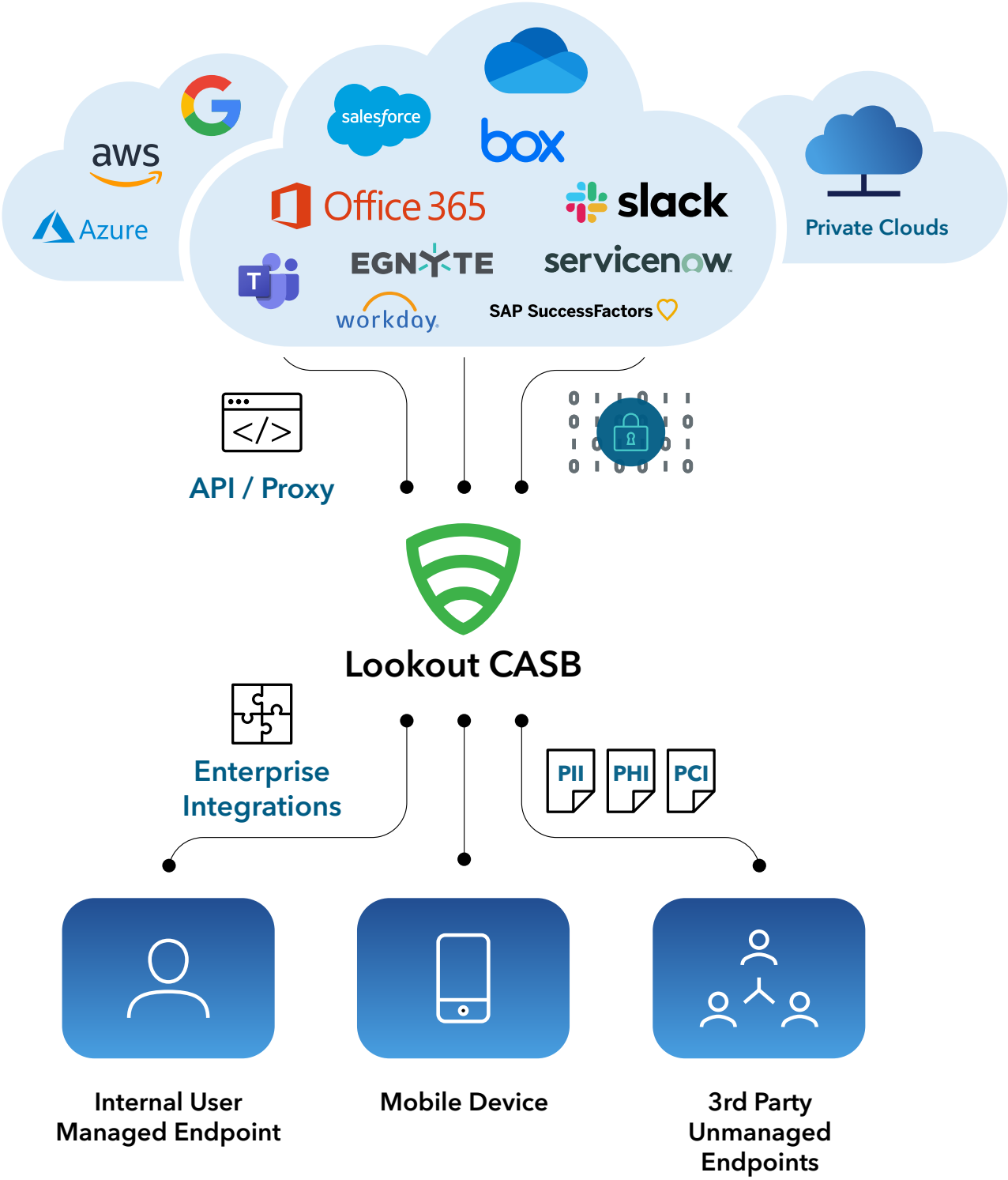
Secure against shadow IT

Today's CASB limits the risk of exposure caused by shadow IT groups. By integrating with existing network devices, firewalls and proxy services, CASB assesses cloud service usage and offers complete visibility into cloud services used by corporate organizations.

> "The interface is uncluttered and the workflow for creating new policies is easy to understand and manage. Administrators can get up to speed and create effective policies quickly."

Craig Lawson and Steve Riley
Gartner Magic Quadrant for Cloud Access Security Brokers, October 2020

The critical role of CASB in endpoint-to-cloud security



Modernize on-premise apps: Zero-trust network access

Many organizations still require some apps to run in their data centers and private cloud infrastructure. But by nature, these on-premise legacy apps are difficult to secure, access and maintain.

With users now working remotely, many organizations rely on virtual private networks (VPNs) to enable access. While they connect users to on-premise apps from anywhere, VPNs perilously assume that every user and device is trustworthy. They are not. This leaves your entire infrastructure – and everything connected to it – extremely vulnerable.

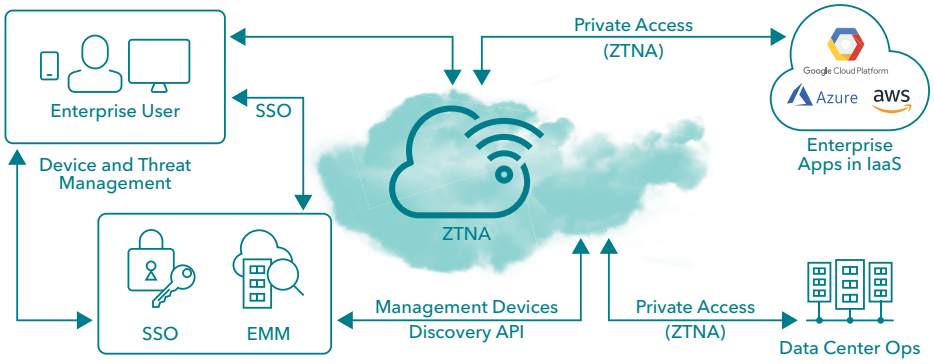
Your goal is to protect on-premise legacy apps and ensure that they perform just like cloud apps. This requires zero-trust network access (ZTNA), another cornerstone of endpoint-to-cloud security. It provides dynamic, precise access on an application level to protecting your entire security infrastructure, including on-premise legacy apps.

With ZTNA, the same security controls that you apply to your cloud apps and services are applied to on-premise legacy apps. It also integrates with multifactor authentication and other identity solutions to reduce user friction and dramatically improve overall access control.

Unlike VPNs that give users unfettered network access, ZTNA leverages dynamic identity- and context-aware access policies based on the risk level of individual users and devices. This significantly reduces security risks associated with malicious users and compromised devices and accounts.

Equally important, ZTNA distinguishes app access from network access. This mitigates the risk of breaches caused by the overentitlement of services. Identity, context and policies are applied to individual users before access is granted. Critical apps and services are hidden from anyone who isn't authorized to access them.

ZTNA greatly reduces the overall attack surface, preventing threat actors and malicious insiders from stealing or compromising high-value data and intellectual property. It also prevents cyberattackers who gain control over endpoints and stolen account credentials from moving laterally to compromise apps and services in adjacent clouds.



"The perimeter is now everywhere an enterprise needs it to be – a dynamically created policy-based Secure Access Service Edge."

Neil MacDonald
Vice president, distinguished analyst and fellow emeritus
Gartner

The Gartner Security & Risk Summit 2020.

Advanced data protection

In addition to mobile endpoint security, CASB, and ZTNA, your organization requires integrated data protection that works anywhere – from endpoint to cloud. A common way to lose data is through cloud sharing. Although it's easy to share content internally and externally, employees can also share that content with unauthorized users.

Often integrated with CASB, data loss prevention (DLP) understands what types of data you have across your entire organization and classifies them according to their business importance and confidentiality.

DLP provides advanced data matching, document fingerprinting, analysis of structured and unstructured data, and protections against the offline sharing of information and files with unauthorized users.

This knowledge allows you to encrypt sensitive content – while at rest, in transit and uploading – using enterprise digital rights management (EDRM). It delivers added protection by ensuring that only authorized users can decrypt information and files.

DLP also scans historical data in the cloud to discover unprotected information and open file shares, which prevents data exposure. With centralized DLP policies, you can consistently detect, classify and secure sensitive data across any cloud deployment, from emails to apps.

> "By the end of 2023, more than 50% of enterprises will have replaced older antivirus products with combined EPP and EDR solutions that supplement prevention with detect and response capabilities."

Paul Webber, Prateek Bhajanka, Mark Harris and Brad LaPorte
Gartner Market Guide for Endpoint Detection and Response Solutions, December 2019

Conclusion

Integrated endpoint-to-cloud security streamlines operations and minimizes business risk. With no perimeter, you have zero visibility and no control over your data across users, devices, networks, and cloud apps.

What's needed is an advanced security platform. It starts with the Gartner SASE architecture, along with CASB and ZTNA and a deep understanding of how your users behave. But that's not enough. You also need mobile endpoint security providing continuous risk assessment, and advanced data protection that works from endpoint to cloud.

This modern zero-trust approach to security protects your data from endpoint to the cloud by providing all-important visibility into users, devices, networks, access privileges, and cloud apps.

Lookout®

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit **www.lookout.com** and follow Lookout on its **blog**, **LinkedIn**, and **Twitter**.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo