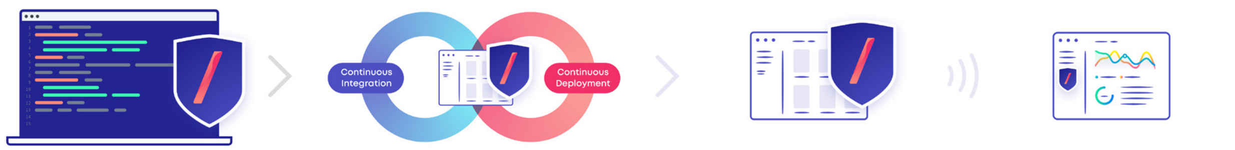
Autonomous Application Protection (AAP)

Applications are prime targets for cyberattacks because they handle troves of personally identifiable information, financial information, and other critical data. Over the past decade, app-targeted attacks have become more common and sophisticated. In fact, applications are now the number-one attack vector of major breaches. Traditional application security tools have failed to protect organizations from attack because they rely on past signatures that are irrelevant to zero-day attacks, lack real-time context and situational awareness, and suffer from high false positive and negative rates. At Prevoty, we believe that securing applications requires radical thinking: Applications must defend themselves. Prevoty has developed the first and only completely autonomous runtime application self-protection (RASP) solution that enables applications to monitor and protect themselves in real-time, at runtime, neutralizing attacks and protecting against both known and unknown threats.

Securing Applications by Default

Prevoty Autonomous Application Protection enables applications to protect themselves from attack using a lightning-fast, attack detection technique called Language Theoretic Security (LangSec). LangSec is the formal process of understanding how data such as content payloads, database queries, operating system commands and more will execute in an environment. Prevoty employs LangSec via autonomous plugins that can be attached to applications at any point in the software development life cycle, and travel with the apps wherever they are deployed. Prevoty inspects all incoming payloads, neutralizing threats in real-time. In short, Prevoty protected applications are secure by default.



Shift Left
AAP plugin attached from the start

SSDLC
AAP is part of the app throughout SSDLC

Hardened App
Applications are secure by default

Data Analytics
Log data for insights in SIEM / analytics platform

Benefits of Autonomous Application Protection

- Protected applications in production are secure by default, no matter where they are deployed.
- Buys you time to fix and patch vulnerabilities, because your applications are secure regardless of latent vulnerabilities in original or third-party software.

Additional Benefits

- More efficient vulnerability management
- Unprecedented visibility into application attacks, events & risks
- A new context-enriched perspective on security from the inside of your applications
- Real-time, actionable intelligence
- DevOps & DevSecOps scalability
- Efficient SSDLC

Prevoty Protects Against

- Command injection
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF/ XSRF)
- HTML injection
- JSON injection
- SQL injection
- Database access violation (Advanced SQLi)
- XML injection
- XML external entity injection (XXE)
- Weak authentication
- Weak browser cache management
- Logging sensitive info
- Insecure transport protocol
- Uncaught exceptions

Deployment

Security tools should solve problems, not create new ones with heavy, burdensome deployments. Prevoty deploys quickly and quietly via autonomous plugins that live inside the applications themselves, and stay with them no matter where they are deployed – whether on-prem, in the cloud, in containers, virtual environments, or micro-services. Deployment is unobtrusive, allowing business to go on as usual without disrupting user experience, and delivers real tangible value on day one.

About Prevoty

Prevoty delivers powerful Autonomous Application Protection via its runtime application self-protection (RASP) technology. It enables fast, efficient and secure software development life cycles, monitors and protects applications at runtime, and neutralizes known and zero-day attacks.

For more information, visit **prevoty.com**