Network as a Service | India

Digital Assets Risk Management

Protect your digital assets

We track and flag unknown threats and help you **implement effective controls and countermeasures to reduce the impact of external risks.**

Service overview

Identify and counter the risks to your digital assets

Digital data sprawl puts your organizational security at risk. Our Digital Assets Risk Management services use an external, intelligent context to track down and flag unknown threats. By covering the depths of the darknet (deep web), we help reduce the impact of potential threats by implementing the appropriate controls and countermeasures.

Our advanced security capabilities ensure your digital assets, intellectual property and sensitive data are protected round the clock. You get assured protection through collective security and threat intelligence to react to new and emerging threats, with 24x7 incident response.

Business outcome	Benefits
Secure your websites and online applications	Detect and block unwanted threats and intrusions to keep your sites and applications operating online, securely.
Limit the risks created by shadow IT	Identify and address exposure created by shadow IT infrastructure and applications.
Enhance your application security	Mitigate insecure coding practices with a comprehensive application code review.
Optimize the bots used on your digital platforms	Control your organization's interactions with different types of bots to maximize business benefits and minimize the negative business or IT impacts.
Enhanced compliance	Implement mandatory controls and enable compliance with regulations such as PCI DSS.

Our advanced security capabilities offer **round-the-clock protection for your digital assets, intellectual property and sensitive data.**

> **Digital Assets Risk Management comprises five key services:**
>
> **Web Application Firewalls**
> Detect and block unwanted threats and intrusions
>
> **ShadowMap**
> Identify and build an inventory of organization-wide exposures
>
> **Web Application Testing**
> Identify dangerous code to avoid exploitation
>
> **Risk Monitoring**
> Improve your detection capabilities with targeted, highly specific intelligence
>
> **Bot Manager**
> Manage malicious or "bad" bots with a highly effective framework

Web Application Firewalls

We help you protect your websites and online applications against current and emerging threats by detecting and blocking unauthorized intrusions. These include SQL injection, cross-site scripting (XSS), illegal resource access, malicious bots, and other Open Web Application Security Project (OWASP) threats.

Our Web Application Firewall service offers:

- Easy deployment and go-live through a simple change to your website Domain Name System (DNS) settings (the service is webserver-platform independent)

- Almost no management and maintenance overheads

- Simple commercial models and Software as a Service-based pricing

- Multiple value-adding services, like distributed denial of service (DDoS) protection, web application penetration testing and Secure Sockets Layer (SSL) certificates

- Intuitive and contextual security that automatically learns web application structure and user behavior

- A low false-positive ratio and protection from zero-day and emerging threats using correlation

- Integration with VA and PT scanners

- Jointly developed with Imperva, our cloud-based service, SecureAT, provides up to 40% reduction in total cost of ownership compared to a dedicated appliance solution

ShadowMap

This big data analysis and machine learning service continuously maps your shadow IT infrastructure and applications to give you visibility of publicly exposed services, applications, assets and security bypass issues.

We're able to detect new network services, web and mobile applications that are exposed across the world. Through virtual host detection, we can identify hosts and configure mappings, even those with no DNS entry.

ShadowMap is a purely external solution that requires no data or deployment of agents. It provides a comprehensive inventory, generates daily differential gap reports and maps your environment across your global hosting footprint. It offers complete integration with VA/PT/AppSec scans and third-party governance, risk and compliance (GRC) tools, and modules for integration with WAF/IPS/SIEM detection and reporting.

With ShadowMap, we deliver:

- **Internet-wide scanning:** Our proprietary technology and platform scan 4 billion global IP addresses daily and extract 22 different data points for machine-learning analysis.

- **Big data analysis and machine learning:** These scans generate a massive dataset that we process to extract key parameters. Algorithms create client profiles that identify all assets belonging to your organization.

- **Risk analysis:** We run scripts on shortlisted assets to reconfirm their identity. Routine checks and an addition 20-step process flag all exposed apps by functionality and risk.

- **Reporting:** Scheduled email alerts, a real-time dashboard and API integrations are used to report on finding and track closures. Service reports can be customized to your objectives and requirements.

Web Application Testing

Web Application Testing combines our proprietary in-house scanning tools with internal expertise to help you identify vulnerabilities in the code of your business applications and mitigate insecure coding practice.

Our service includes

- **Mapping of logic and workflow:** We thoroughly understand your applications' business logic and workflows and create a logical map of relationships between modules, back end and other related elements.

- **Fixing information with examples:** We provide fix information for your development language, framework and platform. Detailed instructions, proofs of concept and source code examples are given.

- **A wide range of integrated tools:** Our proprietary, open-source commercial tools bring security and cost efficiency. Output is cross-referenced, correlated and fed to manual auditors.

- **Test cases created by experts:** Our large internal test-case database is referenced based on various identifiers, allowing our experts to create test cases specific to your priorities and challenges.

- **Identifying vulnerabilities:** Our approach identifies design and logic issues in applications –high-impact issues that aren't generally found by automated scans.

Risk Monitoring

Our Risk Monitoring service provides specific, targeted intelligence to improve detection. We also offer expertise on enhancing preventive capabilities in your existing security products.

Targeted attacks are increasingly sophisticated. Organization-specific threat intelligence is required to ensure near-zero false positives, avoid critical information compromise and enhance security posture.

Risk Monitoring can assist with:

Advanced analytics

- Predictive analytics deployed early in the kill chain
- Trend analysis over time

Actionable intelligence

- Identify your real weaknesses and reduce false positives
- Augment threat-hunting and incident response

Exposure monitoring

- Continuous monitoring of the dark/deep web to detect attacks
- Enrich log data; offer threat intelligence on brand, infrastructure, surface, deep/dark web

Bot Manager

Our Bot Manager service provides a flexible framework for managing the wide array of bots that access your websites every day.

Good bots make your digital platforms interactive and reduce time and resources to improve user experience. Bad bots perform fraudulent activities that hamper the performance of legitimate users and increase your overall IT costs. But how do you know which is which?

With Bot Manager, you can identify bots as they arrive, categorize them, ad apply an appropriate management policy for each category.

Our service includes:

Detection on the web

- Detect non-evasive scrapers targeting web applications
- Detect large-scale credentials, gift-card and coupon checking on browser and native mobile application endpoints

Advanced techniques

- Multiple categories of bots and detection techniques for customizable configurations
- Mobile SDK for native mobile app protection

Why NTT?

Extensive global track record
NTT security specialists mitigate billions of security threats every year

Superior customer experience
Access to comprehensive analytics, service delivery and process development

Financial stability
We're an integral part of NTT Ltd., a leading global technology services company

Deep investment
We invest in innovative solutions and groundbreaking service development

Get in touch

We understand how digital data sprawl puts your organizational security at risk. Contact us or visit our website to learn more about our solutions for protecting your digital assets.