Netcracker
An NEC Company

Netcracker Security

Whitepaper

Netcracker
An NEC Company

1 Market Drivers

Regulatory complexity

Operators are striving to grow beyond connectivity services to become digital service providers, but achieving this transformation requires new revenue streams, partnerships and security models. Security is especially paramount to protect the increasingly vast and vulnerable volume of customer data involved in the digital services of the cloud era. Regulatory bodies around the world have introduced strict security standards to help service providers protect sensitive data and infrastructure. Service providers must now find the right security tools and expertise to comply with diverse regulations while consolidating the number of security products and vendors to minimize cost and complexity.

Remote workforce vulnerability

The global pandemic has significantly impacted CSP operating models as the majority of the workforce has shifted to working from home. While remote work started as a temporary solution, it is becoming a permanent reality and creating new security challenges such as an increase in the number of vulnerable endpoints and greater complexity for access management control. Operators must cope with these new challenges by completely reevaluating their security policies to ensure the integrity of customer data regardless of access point.

Cloud security threats

The proliferation of cloud technologies has opened up vast opportunities for operators in the digital era. However, the widespread implementation of cloud strategies has exposed service providers to new risks and endangered customer data integrity. The most common threats include reduced visibility, limited control, shadow IT and vulnerable cloud applications. Traditional security approaches have proven to be obsolete and ineffective in complex IT landscapes with hybrid cloud environments. Because many IT assets are now outside traditional enterprise perimeters, organizations need to revise their security strategies and extend their security controls to distributed assets.

Netcracker
An NEC Company

2 Netcracker Security

A holistic approach for compliance

Netcracker's service teams have utilized decades of delivery expertise in developing an Enhanced Security Framework to ensure the integrity of client solutions and compliance with local security regulations. The comprehensive Enhanced Security Framework incorporates best practices, procedures and tools to tackle modern security challenges with E2E protection across environments, networks, applications and processes. The holistic approach makes it applicable to operators worldwide regardless of their security compliance needs. Netcracker's Security Operation Centers (SOC) eliminate the need for selecting separate security tools with an entire library of the best industry technologies so that SOC experts can:

- Protect applications and personal devices.
- Control infrastructure access.
- Perform continuous scans for breaches and vulnerabilities.
- Detect and analyze threats.
- Conduct real-time network forensics.

Figure 1: SOC technologies

Data protection methodologies

Netcracker's security services employ two unique methodologies to protect sensitive customer data.

First, we introduce our customers to a DevSecOps approach to minimize vulnerability risks. DevSecOps integrates Netcracker's security team into development and operational processes for multilayer security across the entire partnership lifecycle with in-house and third-party security tools. This methodology helps deliver reliable solutions that meet customer security requirements and provide robust data protection from day one.

Second, we introduce strict access management controls to protect sensitive data from unauthorized use and extraction. Our approach provides crucial support for remote workforces by verifying user identities with multifactor authentication, single sign-on services and zero trust policies. These measures enable Netcracker to provide transparent data handling, protect endpoints and minimize the risk of data breaches in both remote and onsite work environments.

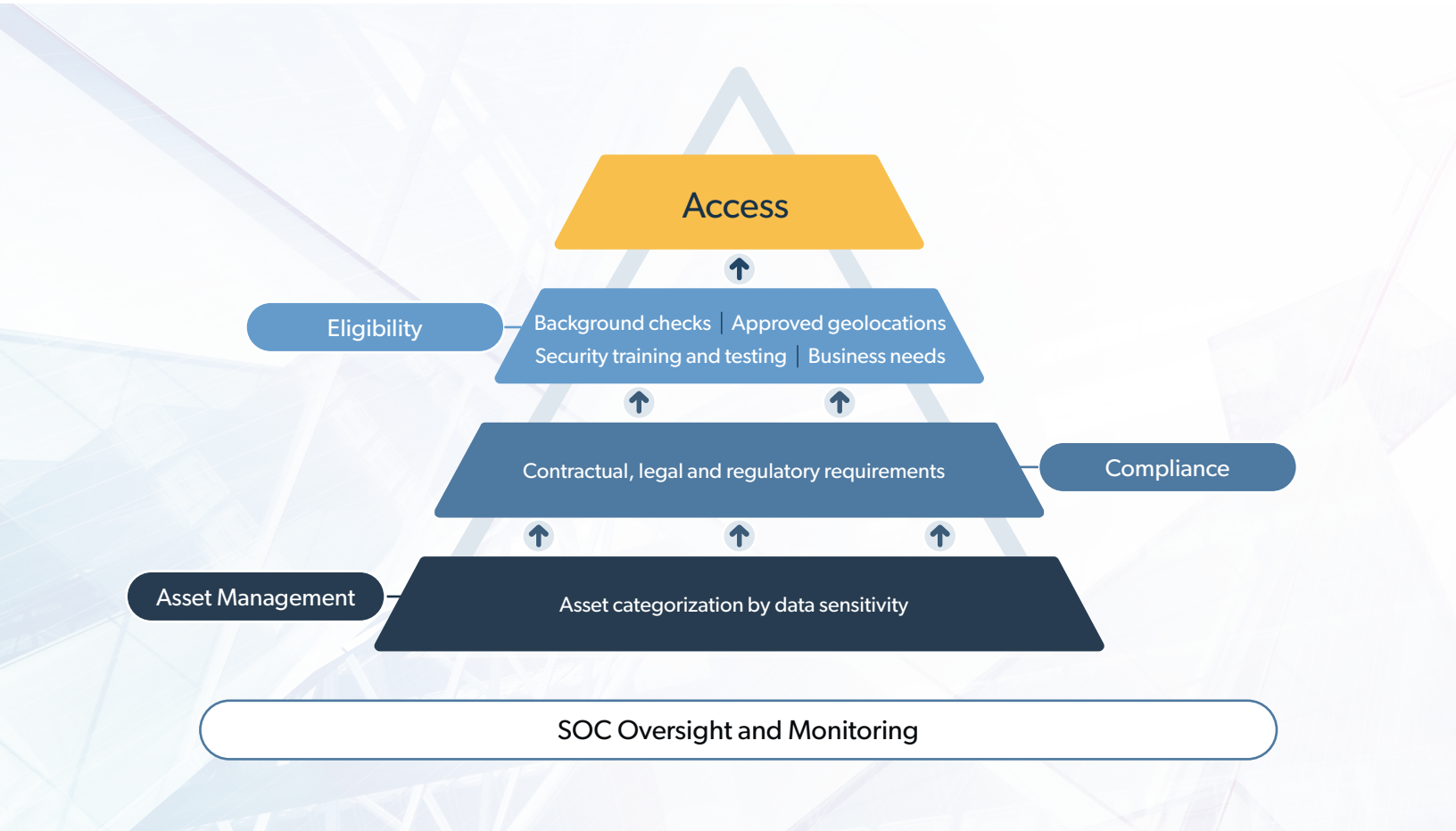

Figure 2: Netcracker access management

Security perimeter extension

Netcracker customers can enjoy the benefits of the Enhanced Security Framework beyond their own premises with Netcracker Enclave. Enclave combines the best practices, methodologies and toolsets to provide secure cloud operations for our customers regardless of data residency. Its secure work environment leverages physical and logical isolation layers to protect sensitive customer data across public, private and hybrid clouds. The primary components of Enclave include:

- Geolocation-based access restrictions and data anonymization to prevent non-anonymized data from leaving the isolated environment.
- Real-time management of events and security information with unified dashboards to avoid security risks and data loss while ensuring stable performance.
- Virtual desktop infrastructure to centralize data and IT control.

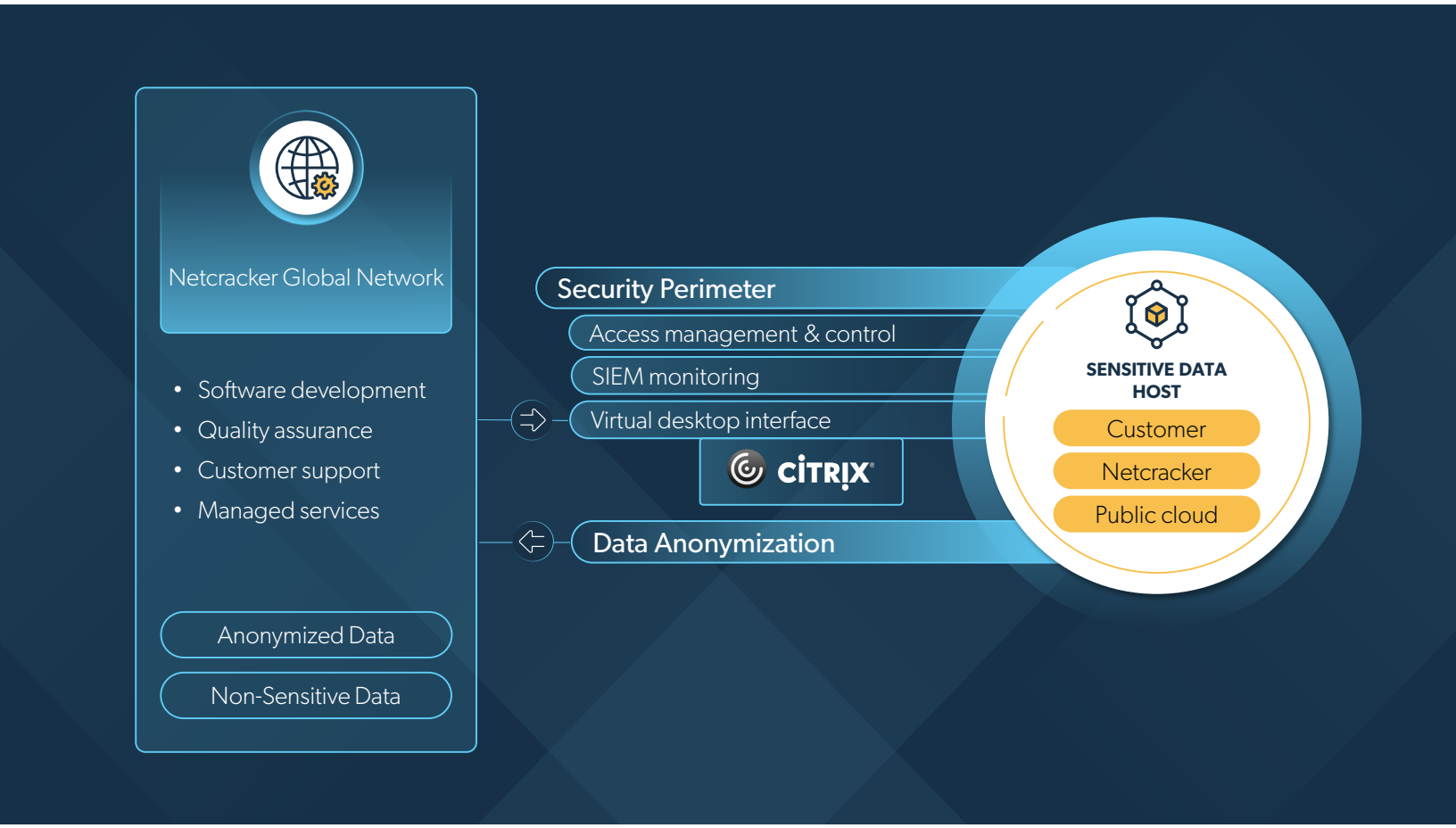

Figure 3: Netcracker Enclave

3 Industry Recognition

Netcracker follows a comprehensive program for compliance management to align Netcracker security practices with the highest industry standards. It includes:

- External audits, including PCI DSS, ISO 27001/27018/22301 and SOC reporting.
- Independent vulnerability assessments and penetration testing of Netcracker networks by third-party organizations.
- Additional audits as required by customers.

We have completed a security assessment program conducted by the U.S. government and received approval from the U.S. Department of Justice, confirming the government-grade reliability of our products and services.

In 2021, the effectiveness of Netcracker security practices and performance was further verified when we received top cybersecurity scores from leading security evaluation platforms BitSight, UpGuard and RiskRecon.

Netcracker's cybersecurity scores

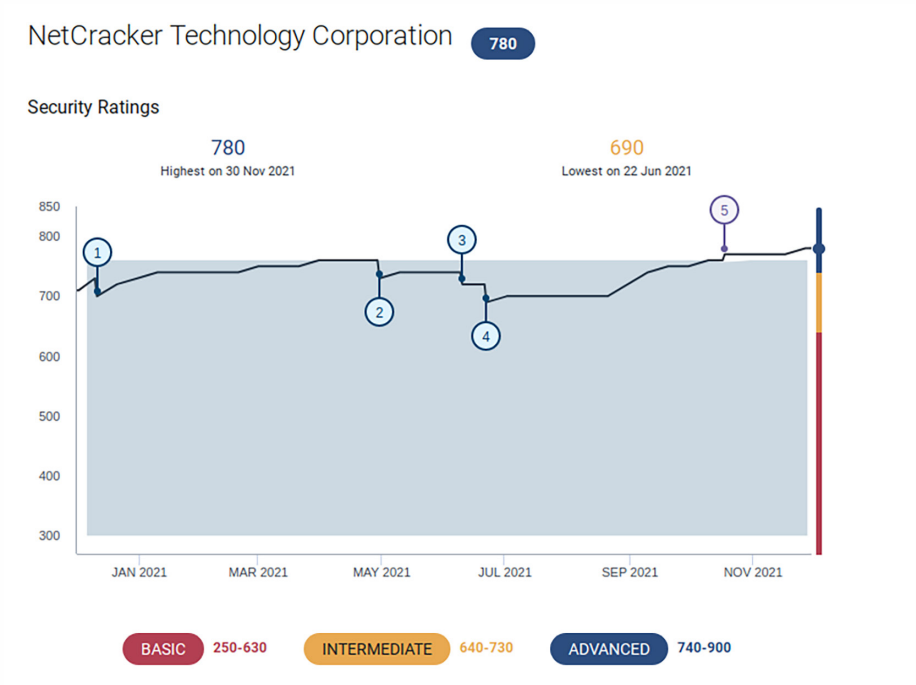

Figure 4: BitSight

Figure 5: UpGuard

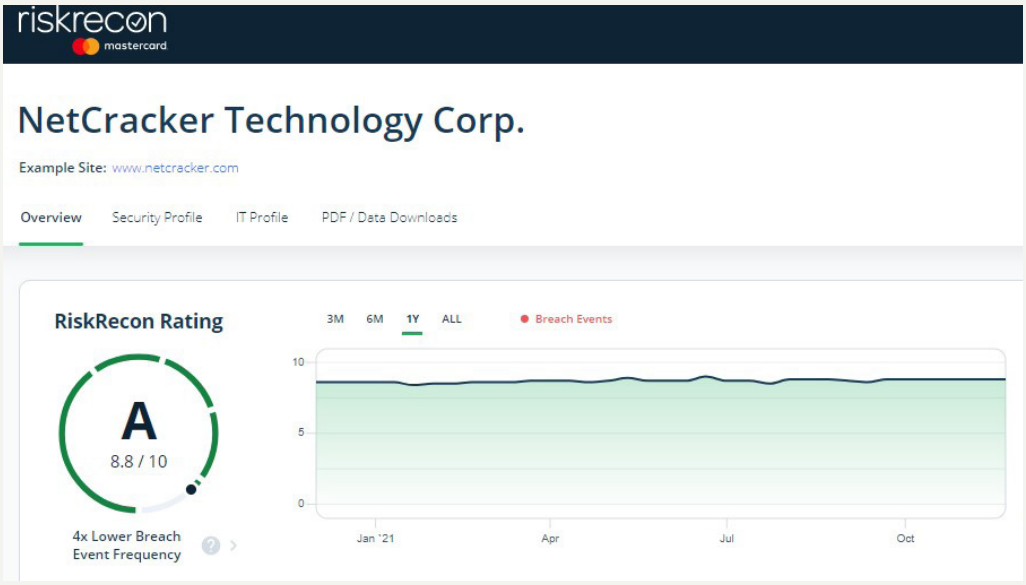

Figure 6: RiskRecon