COLORTOKENS

Xtended ZeroTrust Platform

Zero trust. Zero complexity. Zero compromise.

Ari Chakrabarti, Sr. Sales Engineer CCIE, VCX-NP

CISOs rely on a variety of security technologies…

Email Security
Prevent malware propagation via attachments, phishing and social engineering

Barracuda · proofpoint.

Perimeter Security
Defend against network level threats at ingress/egress points

Check Point SOFTWARE TECHNOLOGIES LTD · paloalto NETWORKS · FORTINET

EDR / NGAV
Continually monitor and respond to endpoint threats

Symantec. · CROWDSTRIKE · SentinelOne

CASB
Monitor and enforce policies for SaaS applications

netskope · bitglass · PRISMA

Web Security
Enforce corp policies and protect from malicious websites

zscaler · Symantec.

IAM
Define and enforce fine-grained access based on identity and role

onelogin · Azure Active Directory · SailPoint

Defense-In-Depth

CSPM
Identify and remediate risks in public clouds

PRISMA · FIREEYE · orca security

Vulnerability Management
Identify, prioritize, remediate and mitigate software vulnerabilities

Qualys. · RAPID7 · Nessus

Network Access Controls
Provide visibility to and enforce access policies to networks and applications

FORESCOUT · cisco · aruba

Event Monitoring
Aggregate and analyze events and alerts generated by various systems

splunk> · IBM Radar · sumo logic

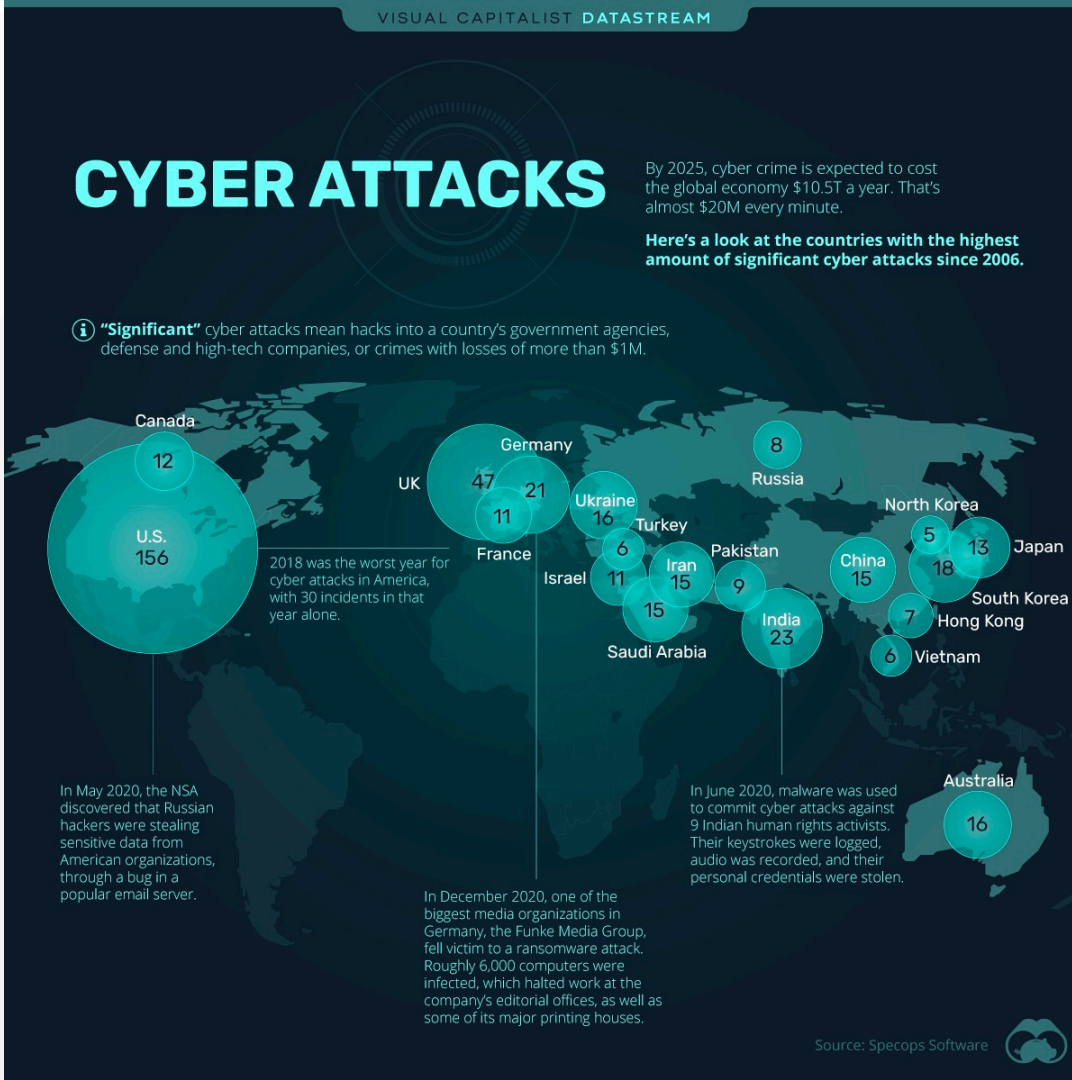
Threat Intelligence
Provide defensive actions by combining alerts with threat intelligence from multiple sources

ANOMALI · Recorded Future · FIREEYE

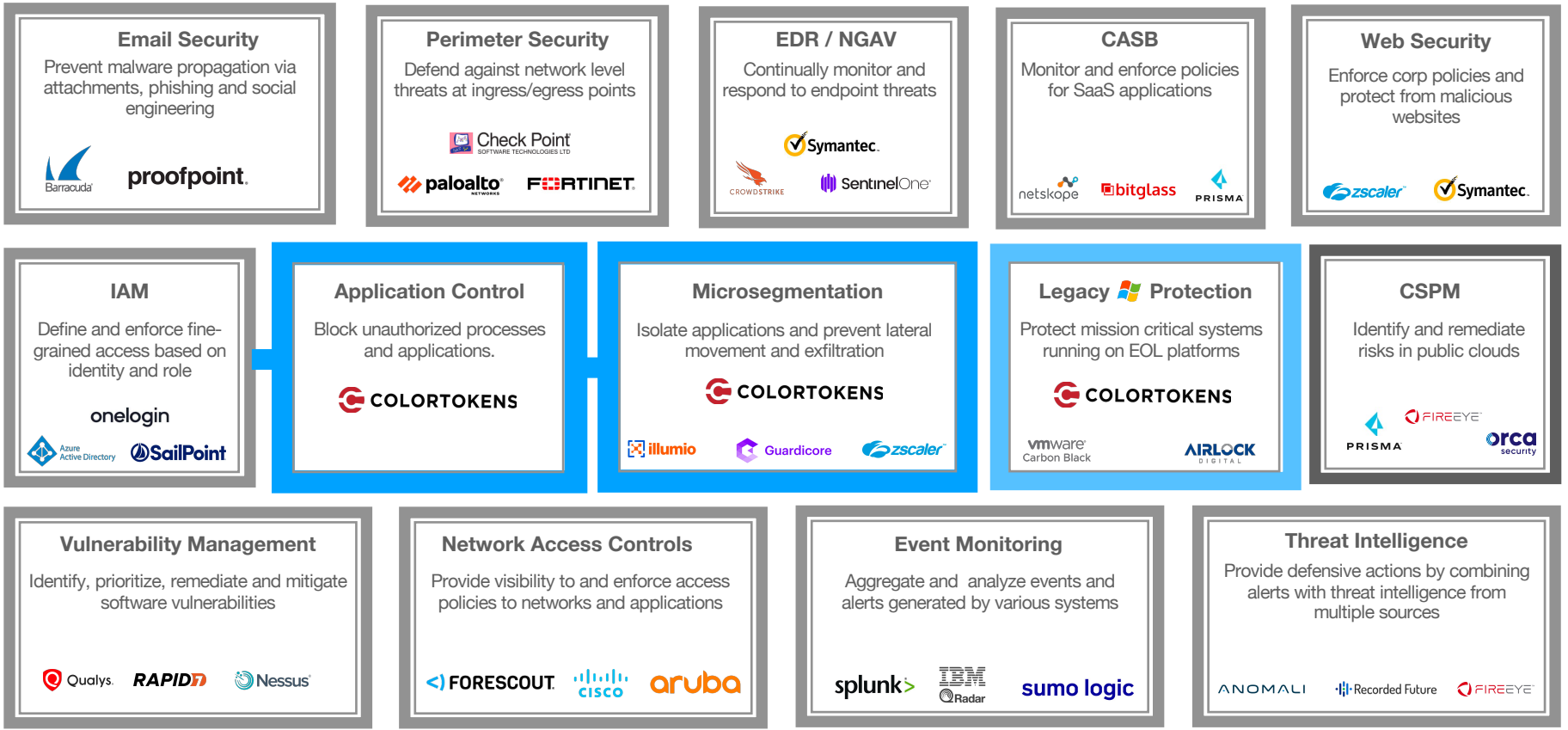
And yet hackers have breached networks,

held governments and businesses hostage with ransomware, and

published personal and confidential information on the Dark Web.



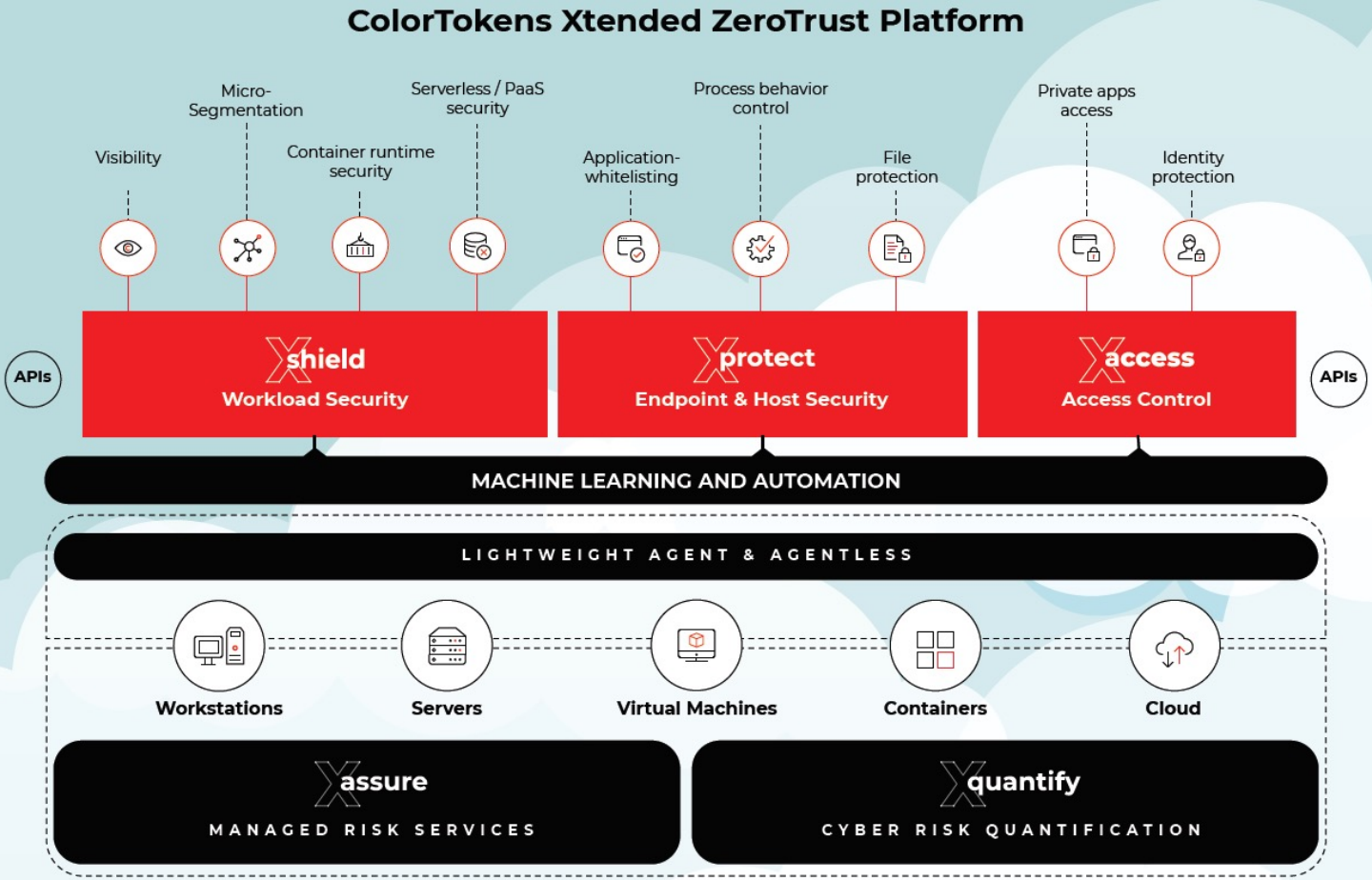
ColorTokens provides both solutions and is NIST-compliant



COLORTOKENS

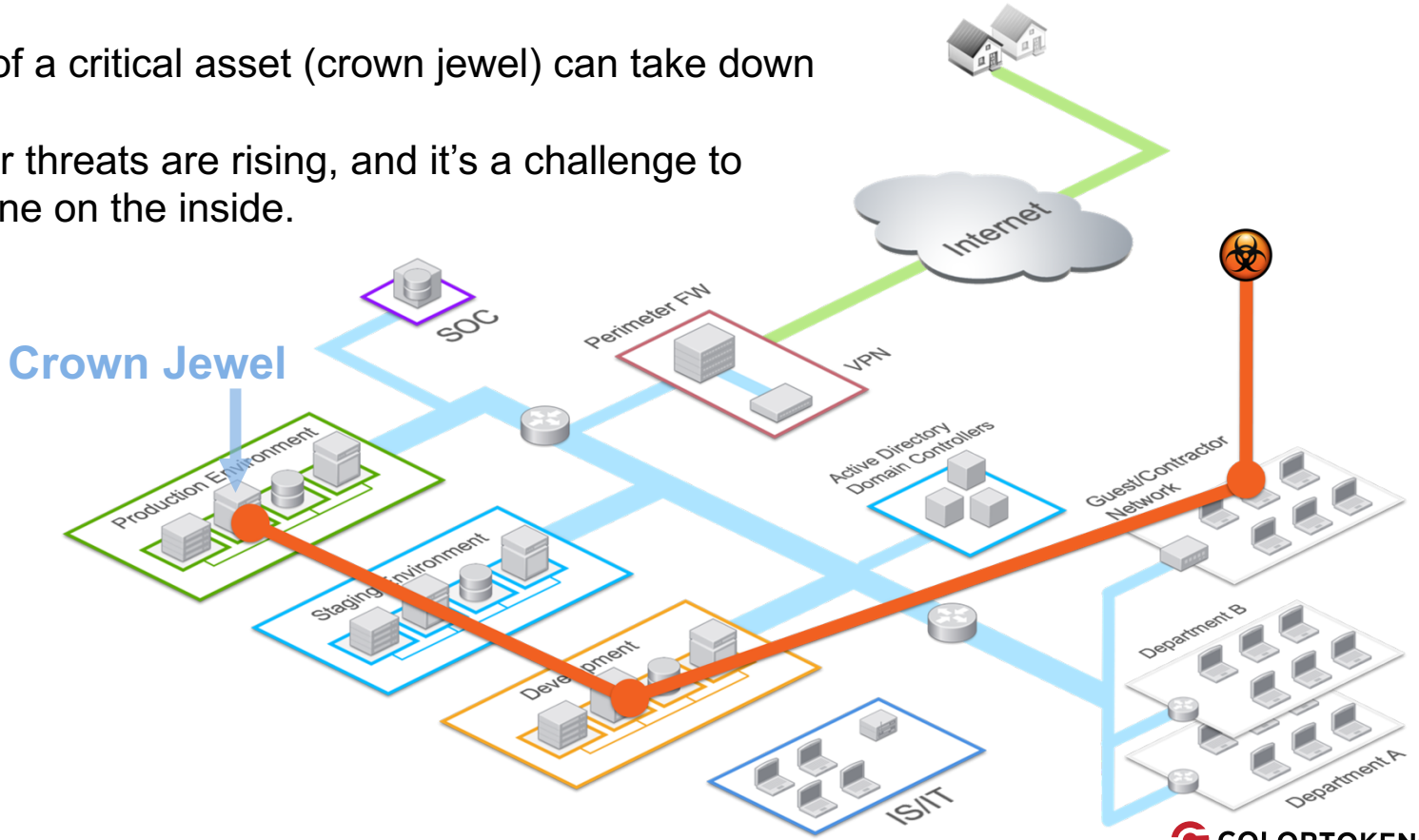
Xtended ZeroTrust™ Platform

Software Defined
Hybrid
Multi-cloud
Protection



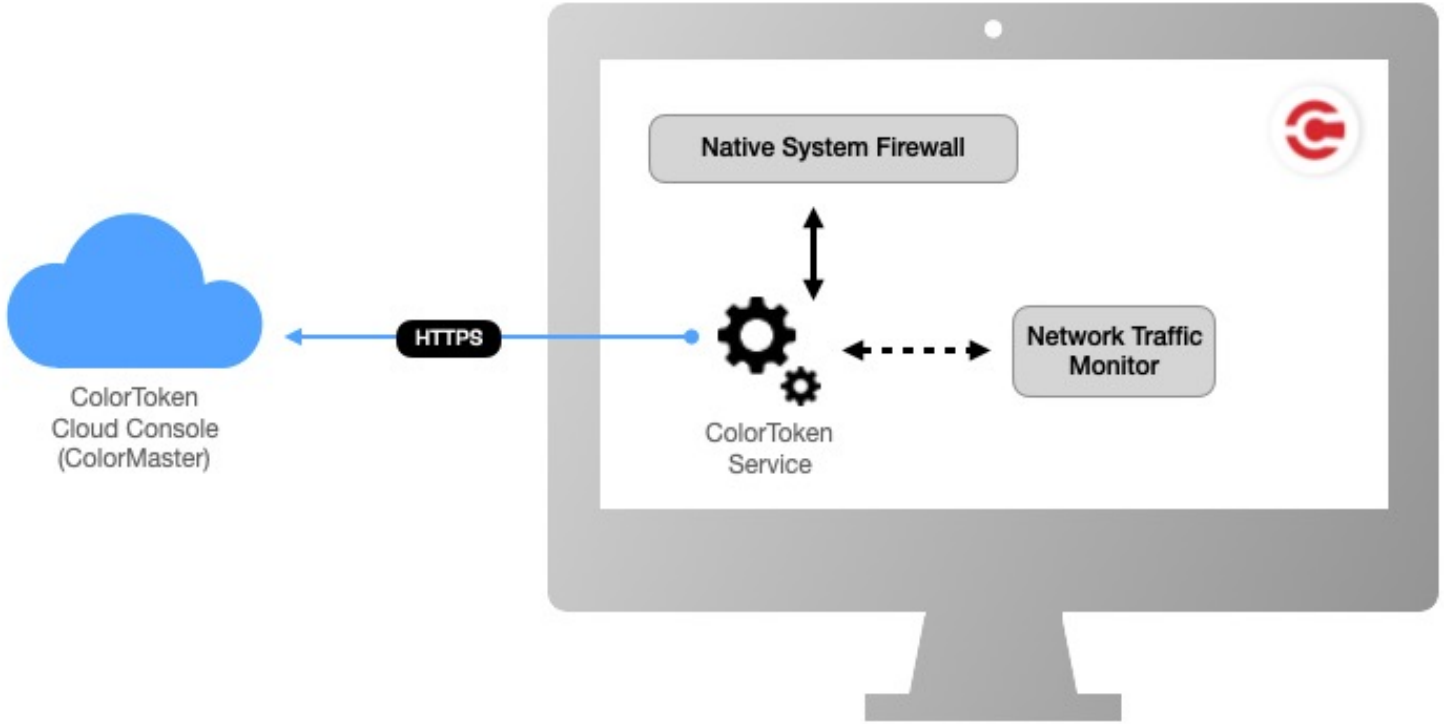
XSHIELD - Why Zero Trust Architecture?

1. Facts: Loss of a critical asset (crown jewel) can take down business!
2. Facts: Insider threats are rising, and it's a challenge to block someone on the inside.



COLORTOKENS

ColorTokens Service Diagram

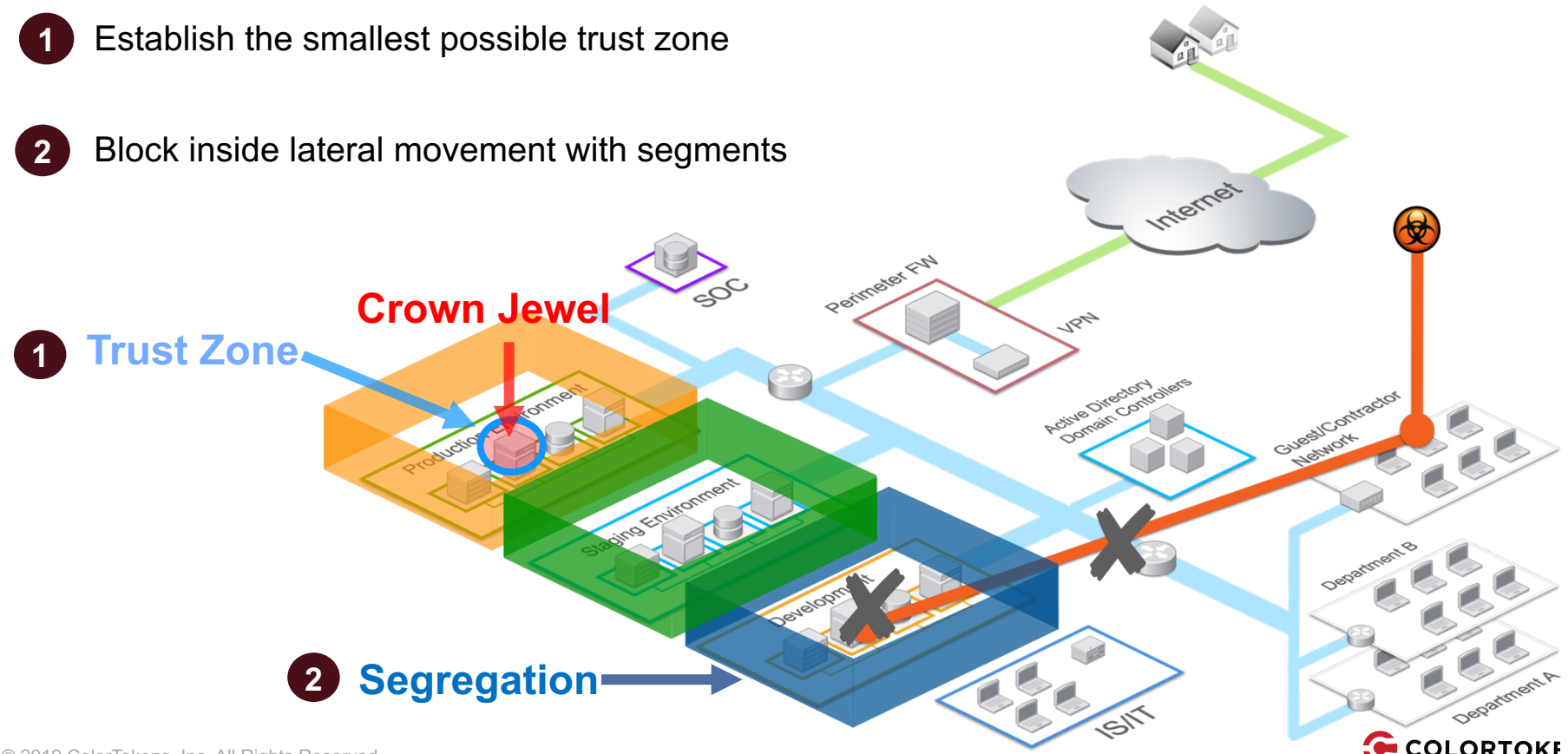


COLORTOKENS

How does Zero Trust Work?

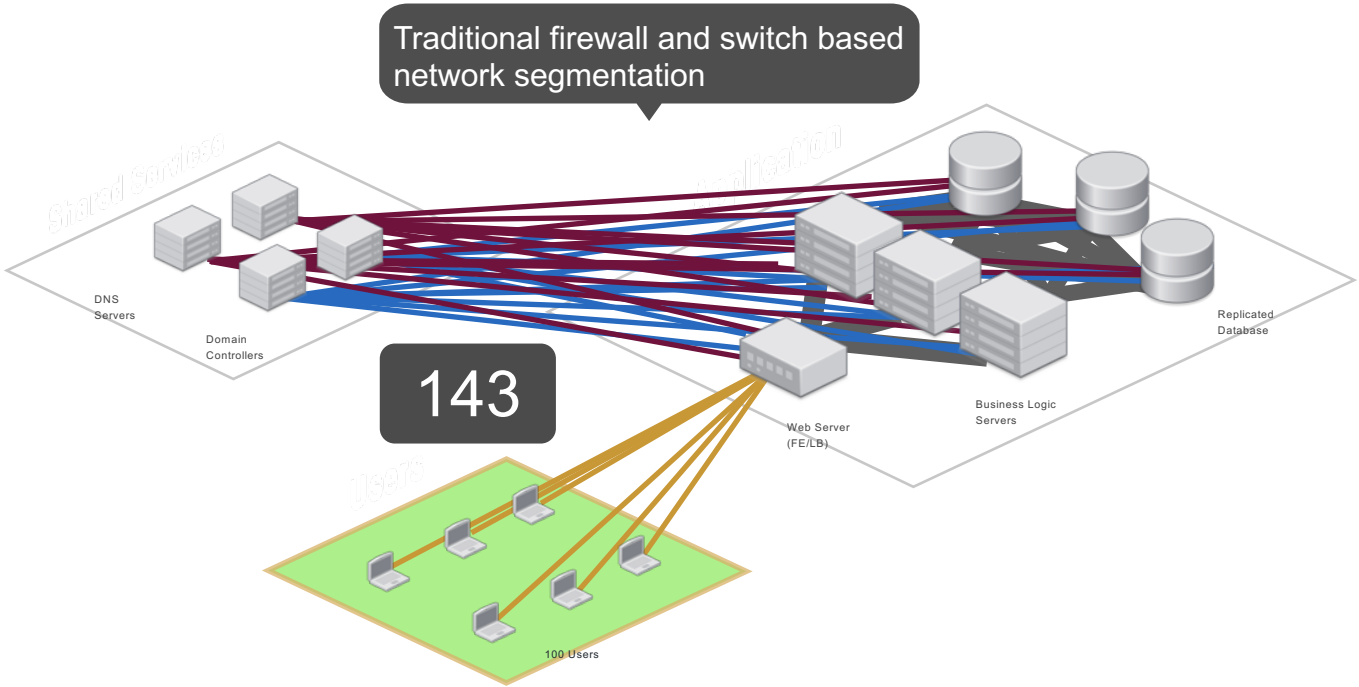
1. Establish the smallest possible trust zone

2. Block inside lateral movement with segments

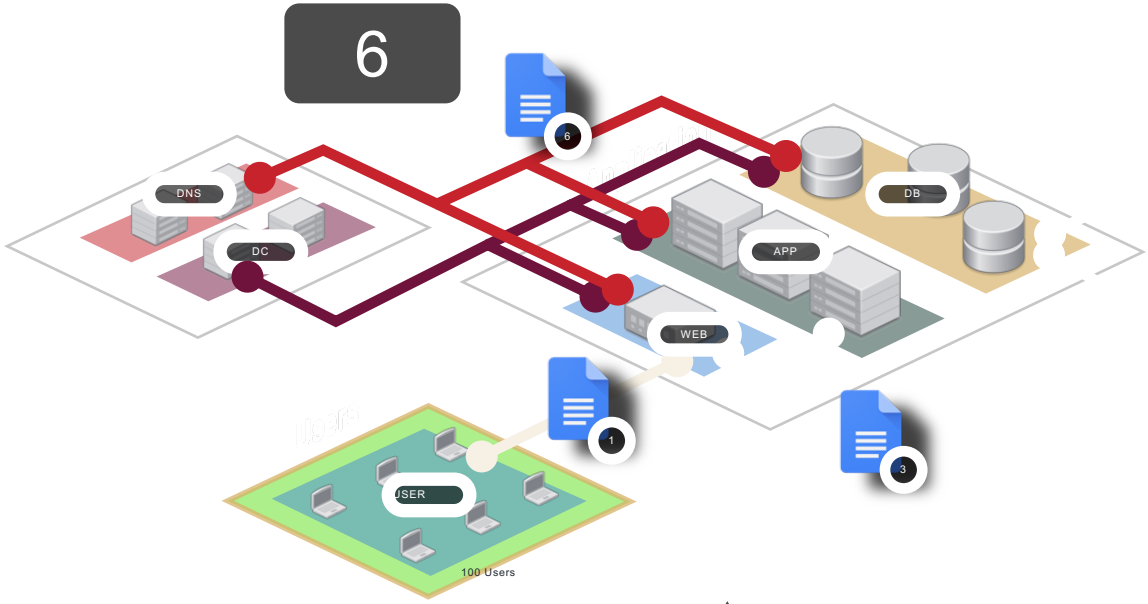


COLORTOKE...S

ACLs and VLANs

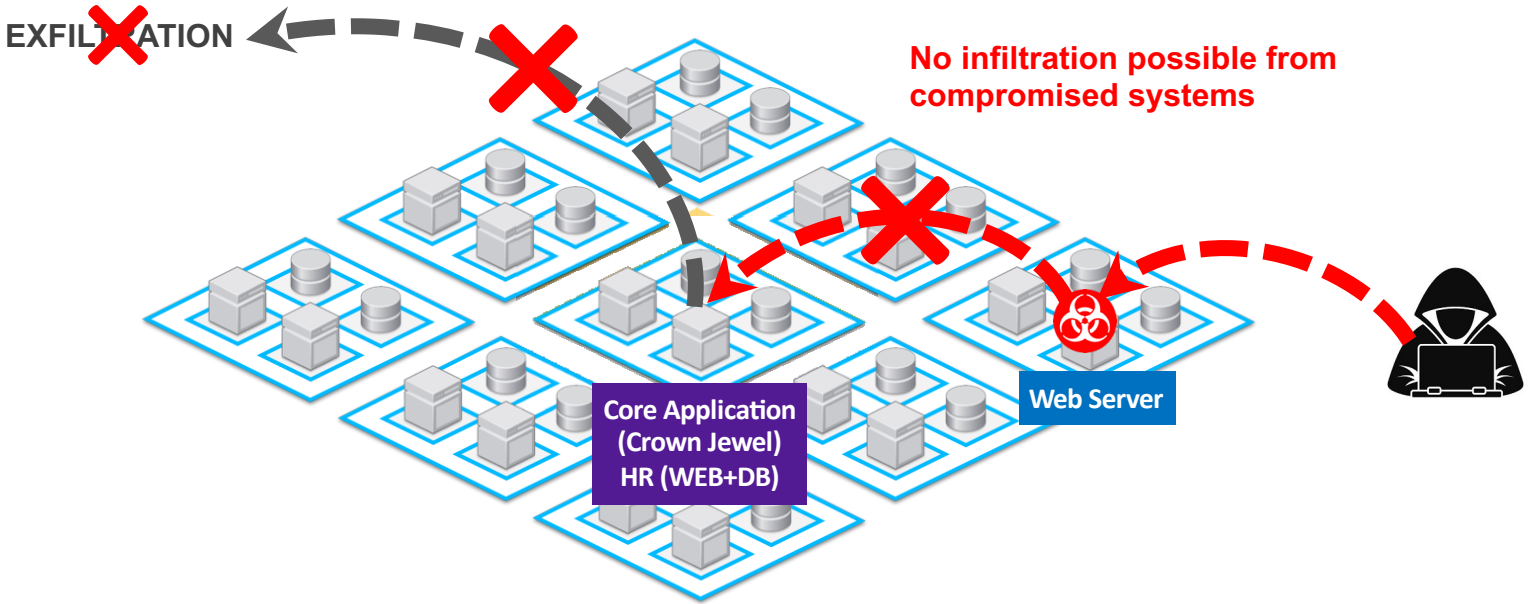


ColorTokens Delivers Micro-Segmentation with 90% Fewer Policies, 10 Times Faster.



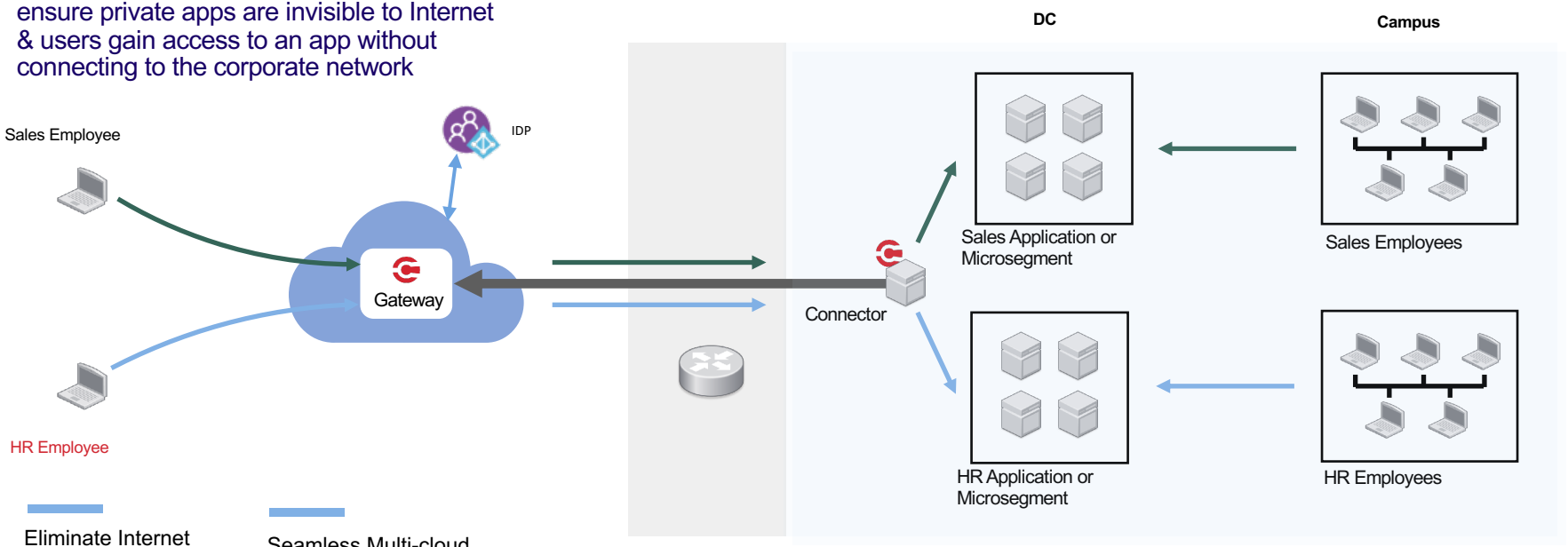
ColorTokens policy-based workload segmentation

Protect critical applications and data



Xaccess – Secure remote access without VPN

ZTNA created Inside-out connections ensure private apps are invisible to Internet & users gain access to an app without connecting to the corporate network



Eliminate Internet Attack Surface

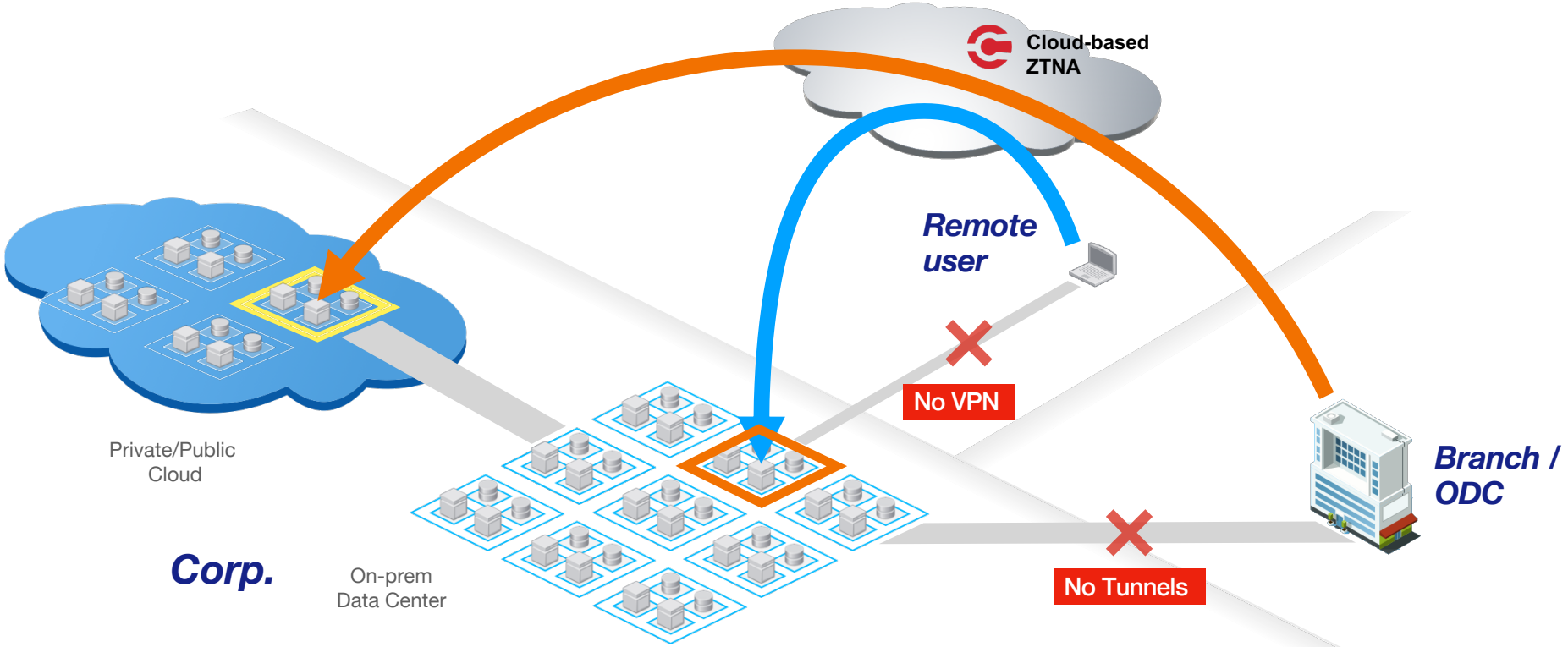
Seamless Multi-cloud Access

Eliminates VPN & DDOS

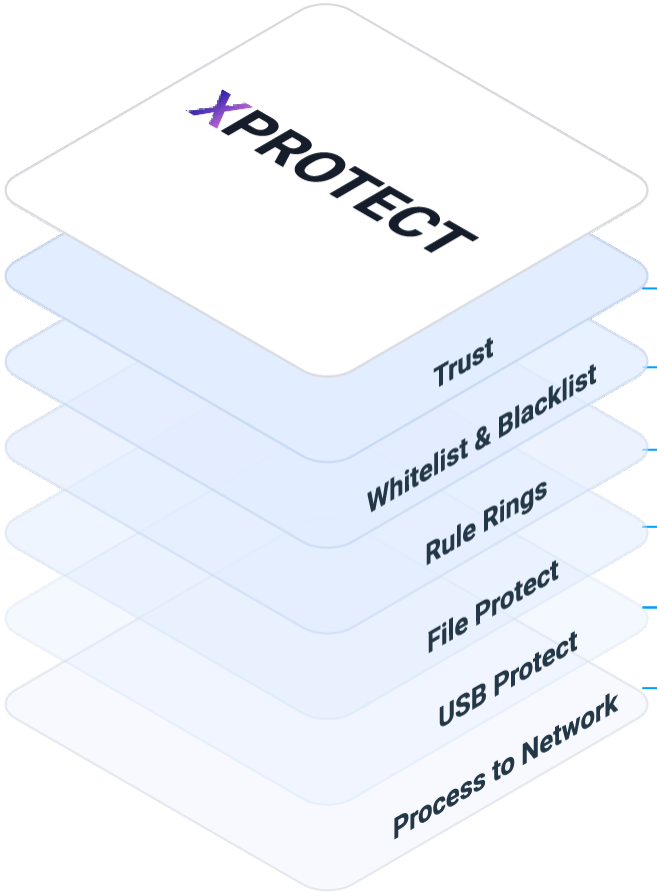
Application Segmentation for least-privilege access

Zero-Trust Network Access (Xaccess)

Secure Remote Access ◆ M&A ◆ Risk Reduction

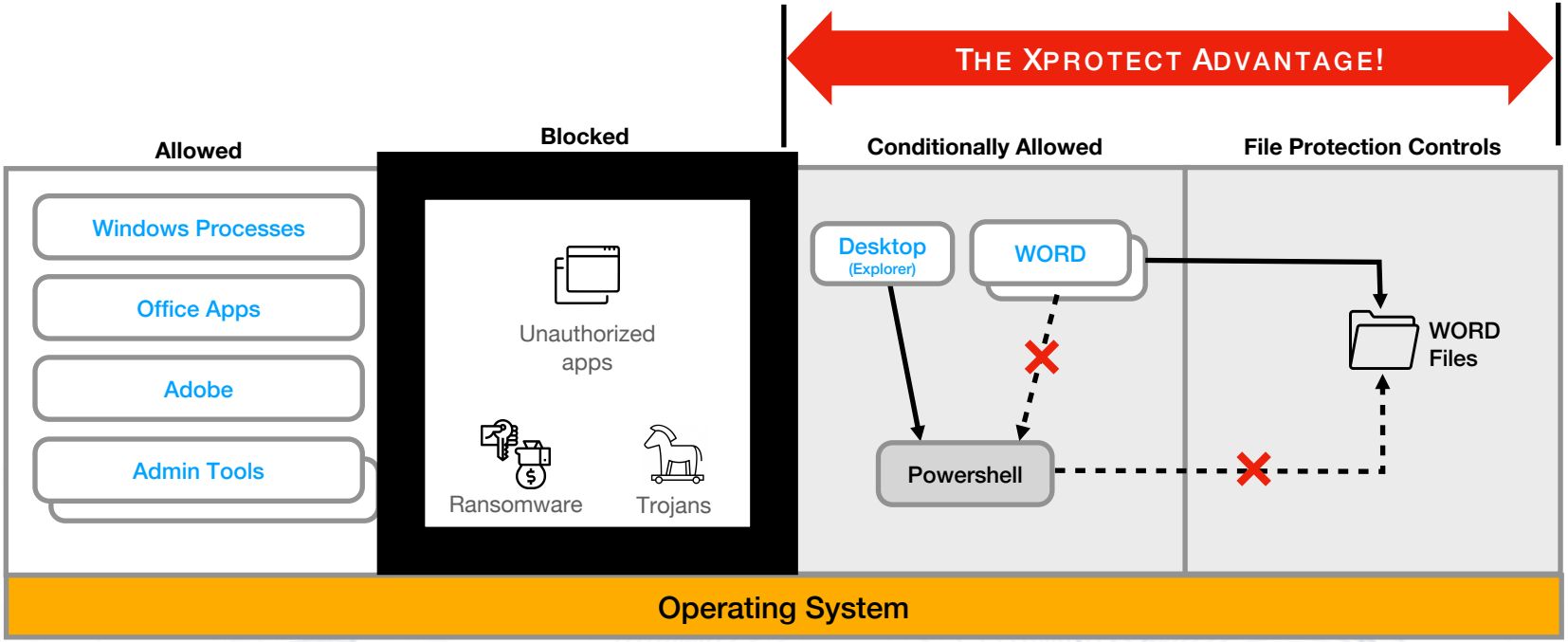


Xprotect

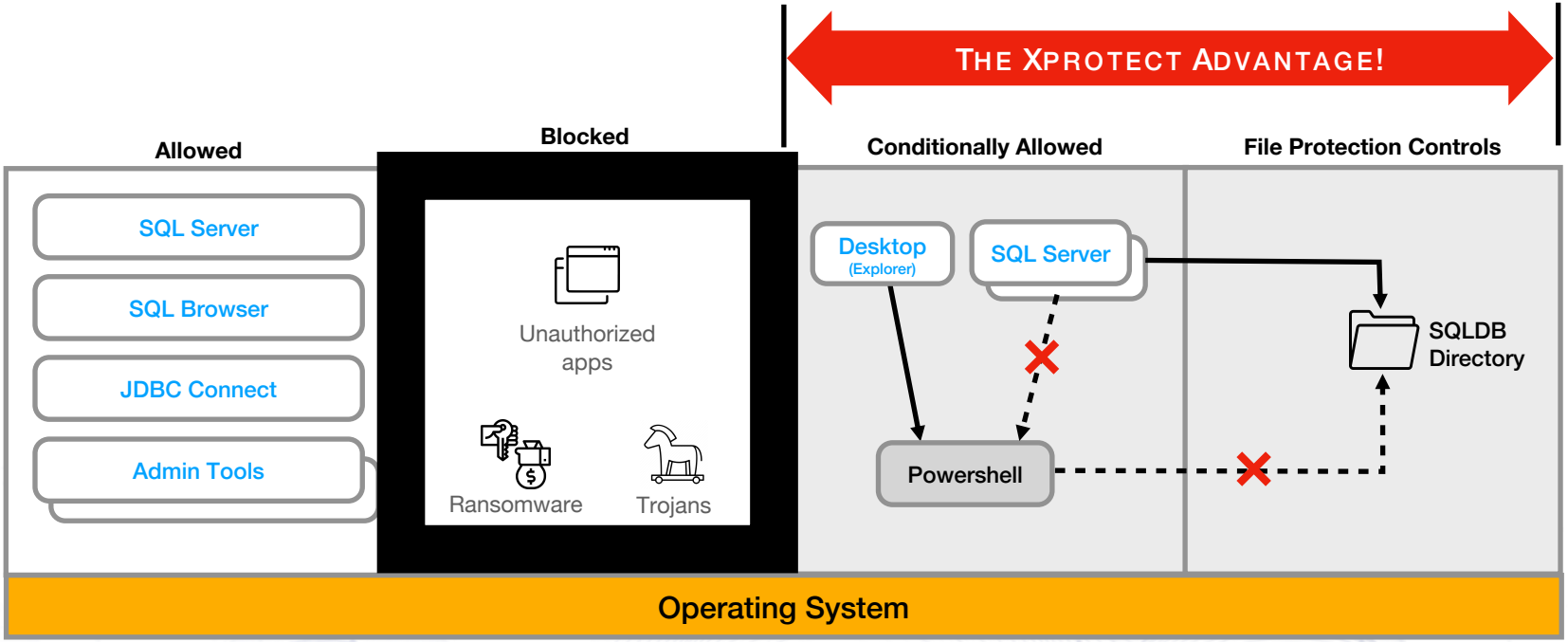


- Light weight threat intelligence
- Allow only company sanctioned applications
- Control process rules - Behavioral attacks
- File to application – Ransomware protection
- Device Control – Stop infections
- Network behavior – Stop exfiltration

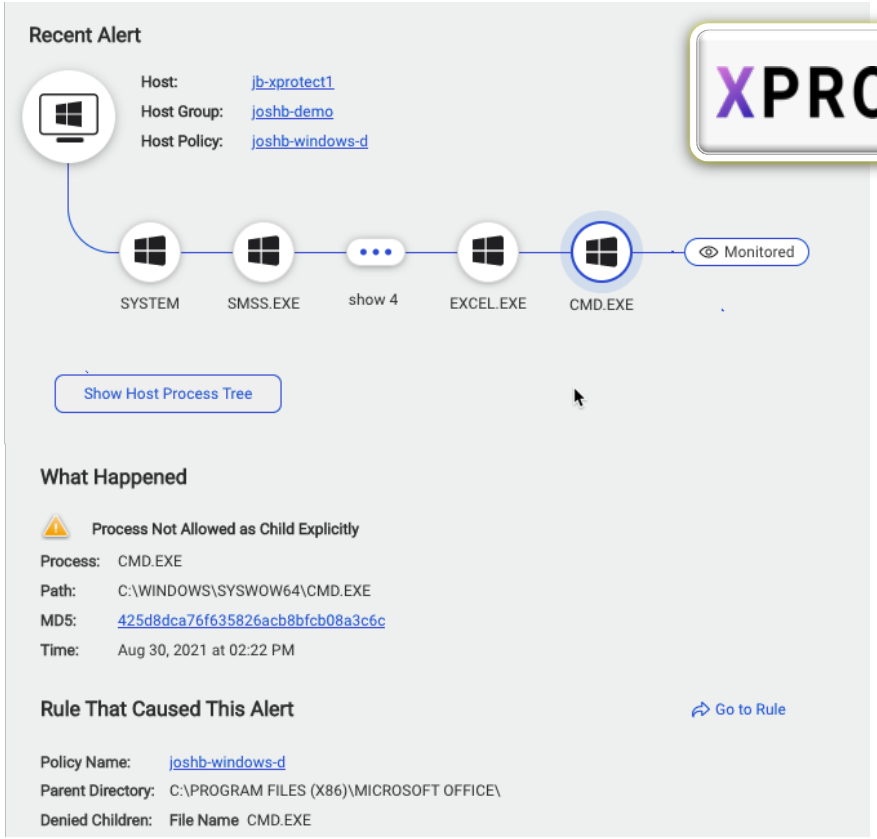
Xprotect – Process Tree Control – End User



Xprotect – Process Tree Control - Workload



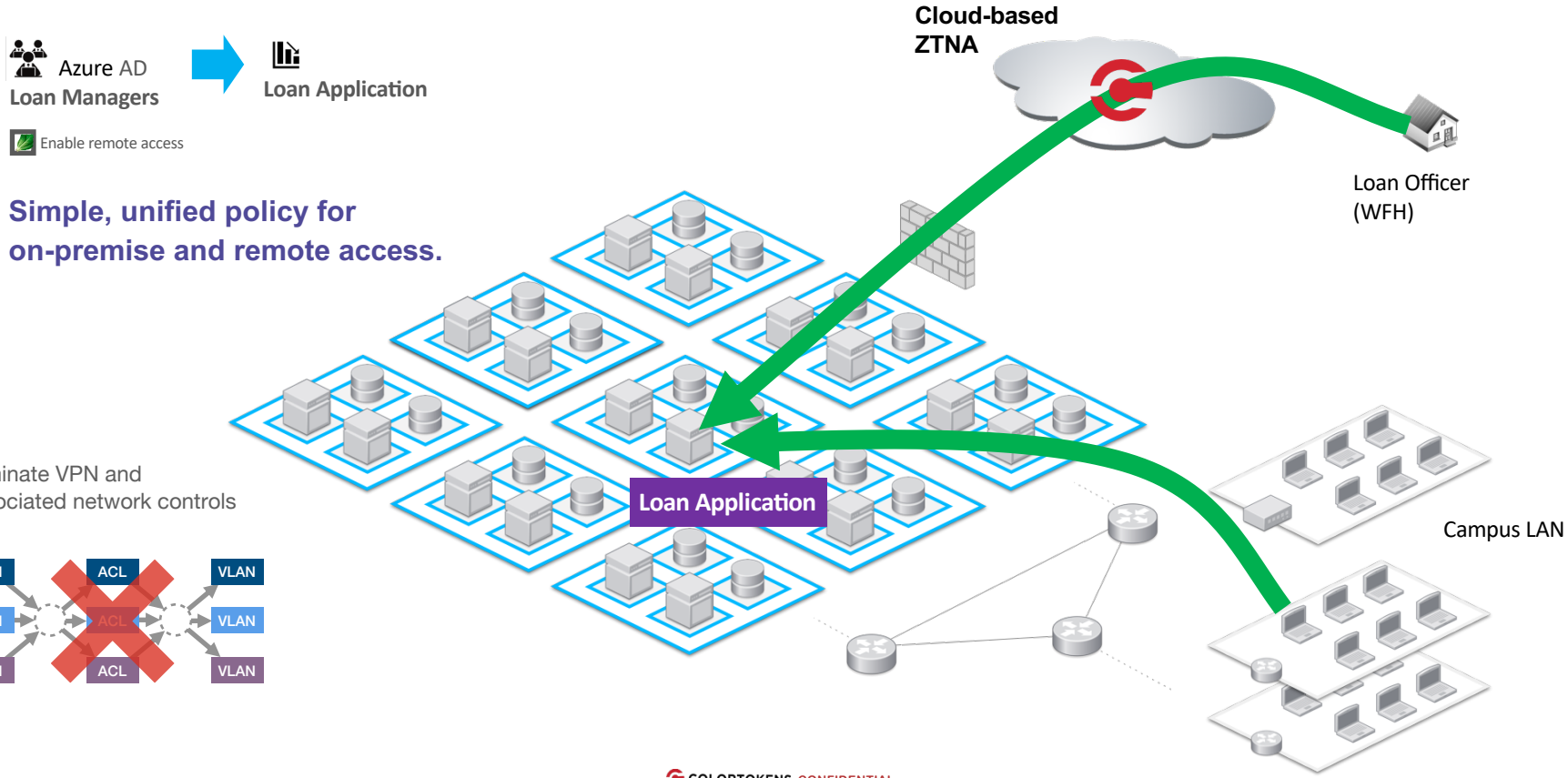
Critical Asset Lockdown



XPROTECT

- Stop Workload Attacks
  - Stop malware by limiting allowed apps
  - Stop legit app hijacks by monitoring Parentage and Network access
- No updates needed
- Coexists with all security solutions

Xaccess - Enable secure remote access



Xshield & Xaccess – For Crown Jewel Protection

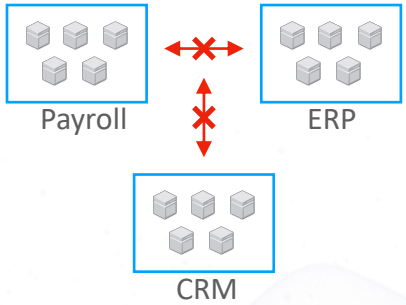
ZERO TRUST

Micro Perimeter around crown jewels controls Inbound / outbound access

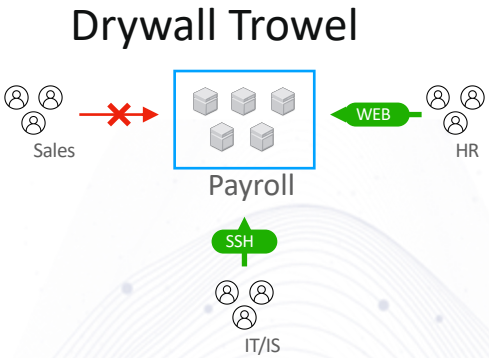
Least Privilege principle blocks unauthorized access to crown jewels

Provides Vulnerabilities and its exposure details and blocks communications with C2 domains

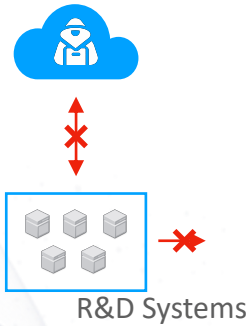
Xshield Micro Segmentation



Ring-fence Crown Jewels to prevent lateral movement

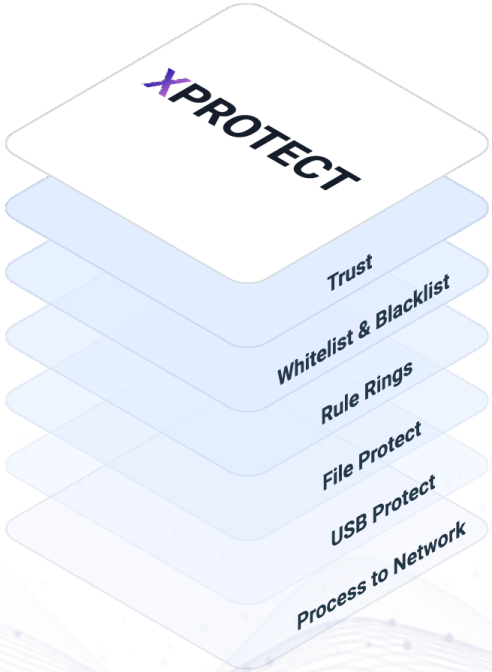


Ensure least privilege access via attribute-based controls



Prevent C2 communications and limit malware propagation

Xprotect – For Crown Jewel Protection

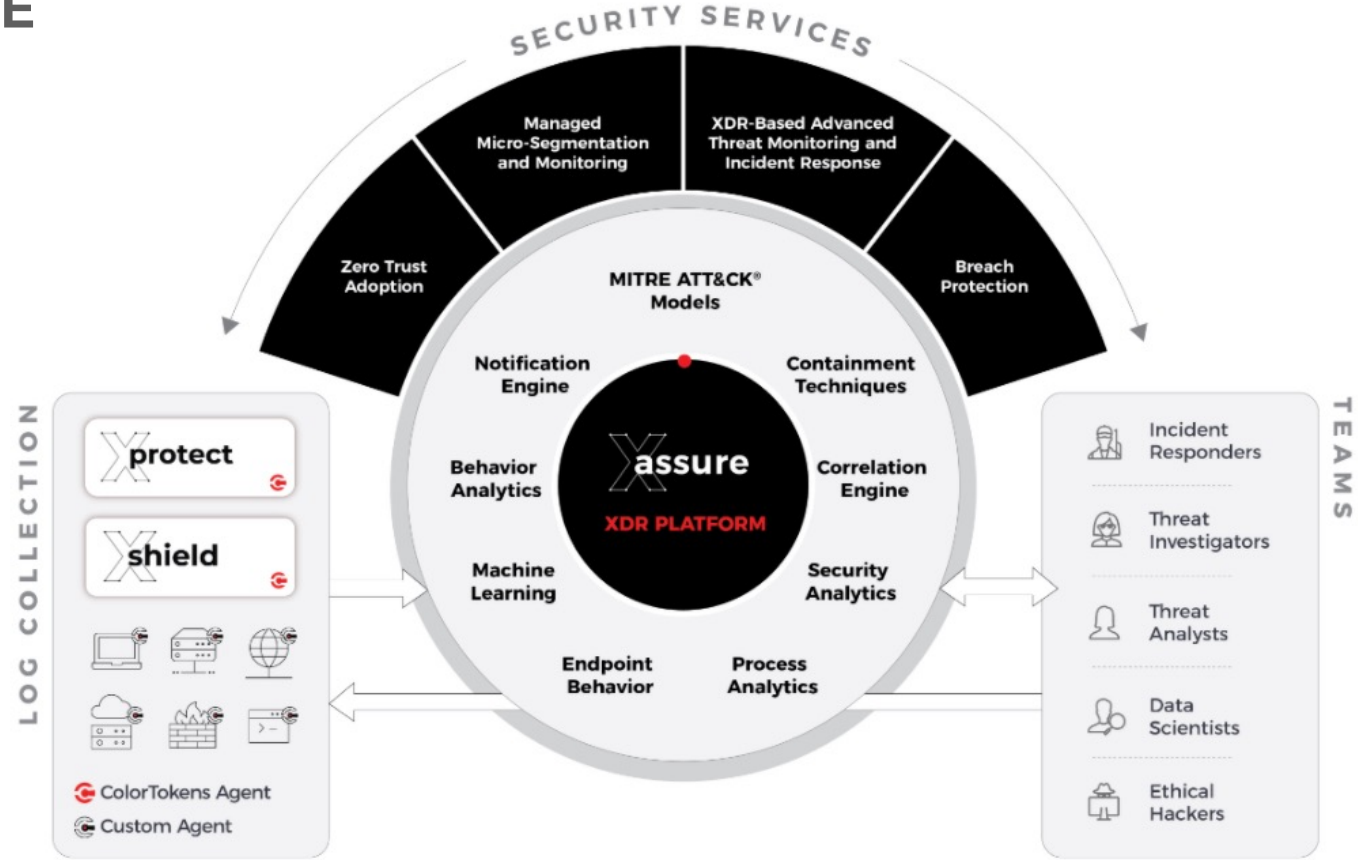


- Threat intelligence
- Application Control
- Behavioral attacks
- Ransomware protection
- Stop infections
- Stop exfiltration

Benefits

- ✓ Application/Process whitelisting blocks unknown processes and locks down the endpoint preventing attacker attempts
- ✓ File protect prevents attacker data destruction attempts
- ✓ Parent child control of processes blocks malware attempts of privilege escalation and execution

XASSURE

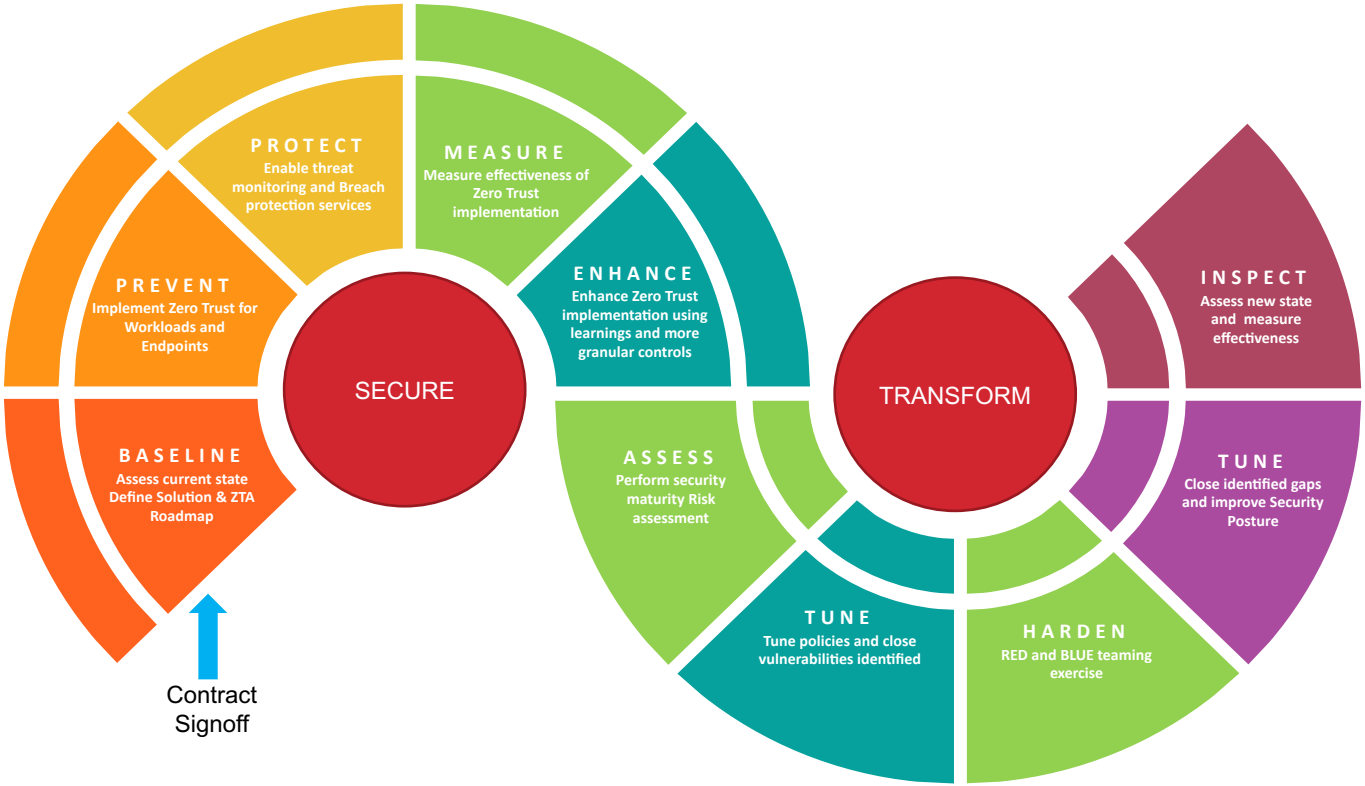


COLORTOKENS

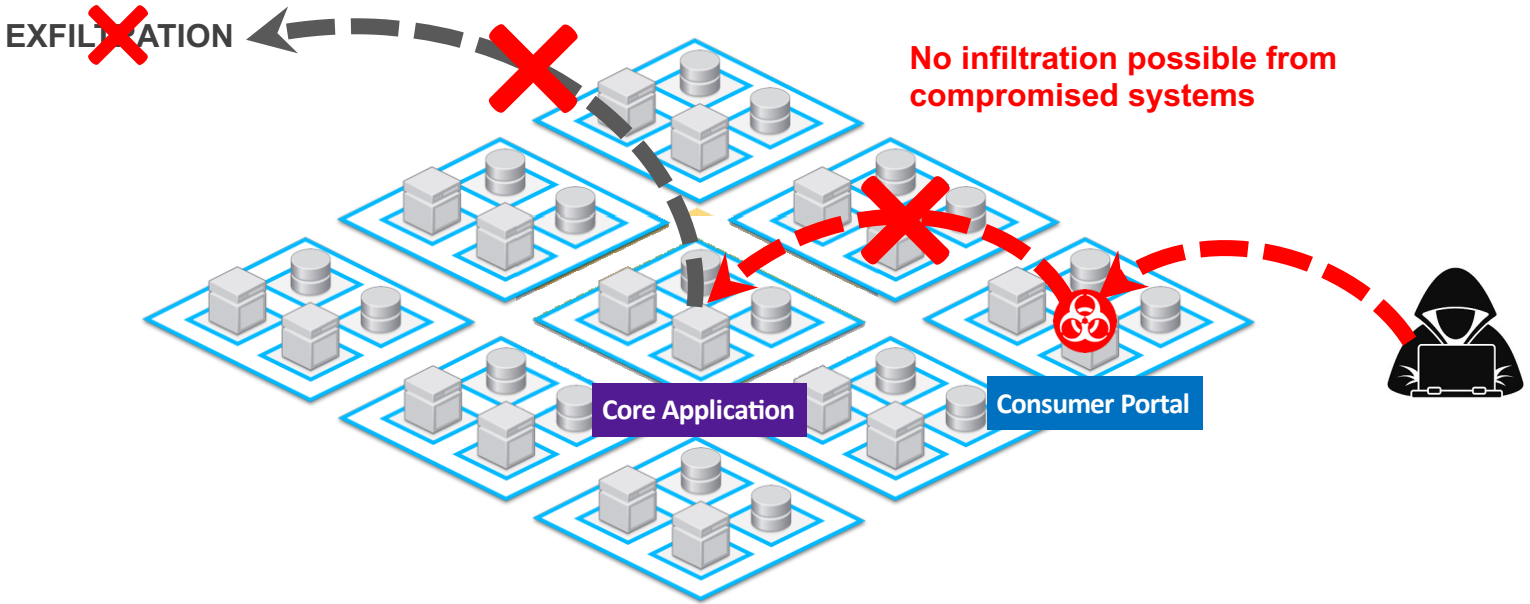
Xassure service packs and what they mean to you

		Xassure Essentials	Xassure Prime	Xassure Prime +
Zero Trust Adoption	Installation and configurations on Workloads and Endpoints	√	√	√
	Micro segmentation and Endpoint security profile design and implementation	√	√	√
	Product Subscription for Xshield and Xprotect	√	√	√
Managed Microsegmentation & Monitoring	Management of ColorTokens Products	√	√	√
	Manage day to day security operations of ColorTokens Products	√	√	√
	Threat Alerting of Common and High Occurring Threats	√	√	√
	Product Support	8X5	24X7	24X7
Advanced Threat Monitoring	Deep Monitoring using Patterns, Signature, and Reputation check		√	√
	Custom Threat Alerts		√	√
	Threat Intelligence covering Bad Hash, Bad IP, Bad Domain		√	√
	Validation of Threats using Analysis and Investigation		√	√
	Managed Incident Response		√	√
	Managed Breach Response for Threat Containment		√	√
	Regular Review of Operations Effectiveness		√	√
	Detection of APTs using MITRE ATT&CK Framework		√	√
Breach Protection	AI/ML Based Detection for Ransomware, Data Theft and Hidden Attacks			√
	Behavioral based detection attacks leveraging known good process and Apps			√
	RED and BLUE Teaming / Penetration Testing Exercises			√
	Regular monitoring and measurement of security posture			√
	Periodic Vulnerability Assessment			√

Xassure method to elevate your security posture



Protect critical applications and data



COLORTOKENS

Thank You!

www.colortokens.com