WHITE PAPER

RANSOMWARE AND THE PLEX SMART MANUFACTURING PLATFORM

AT A GLANCE

With high-profile ransomware attacks on the rise, manufacturers have questions. Plex's security strategy leaves no stone unturned, protecting customer data with a number of precautions and processes.

This overview provides background information and answers your questions about Plex's security posture when it comes to ransomware.

Ransomware Is More Sophisticated Than Ever Before

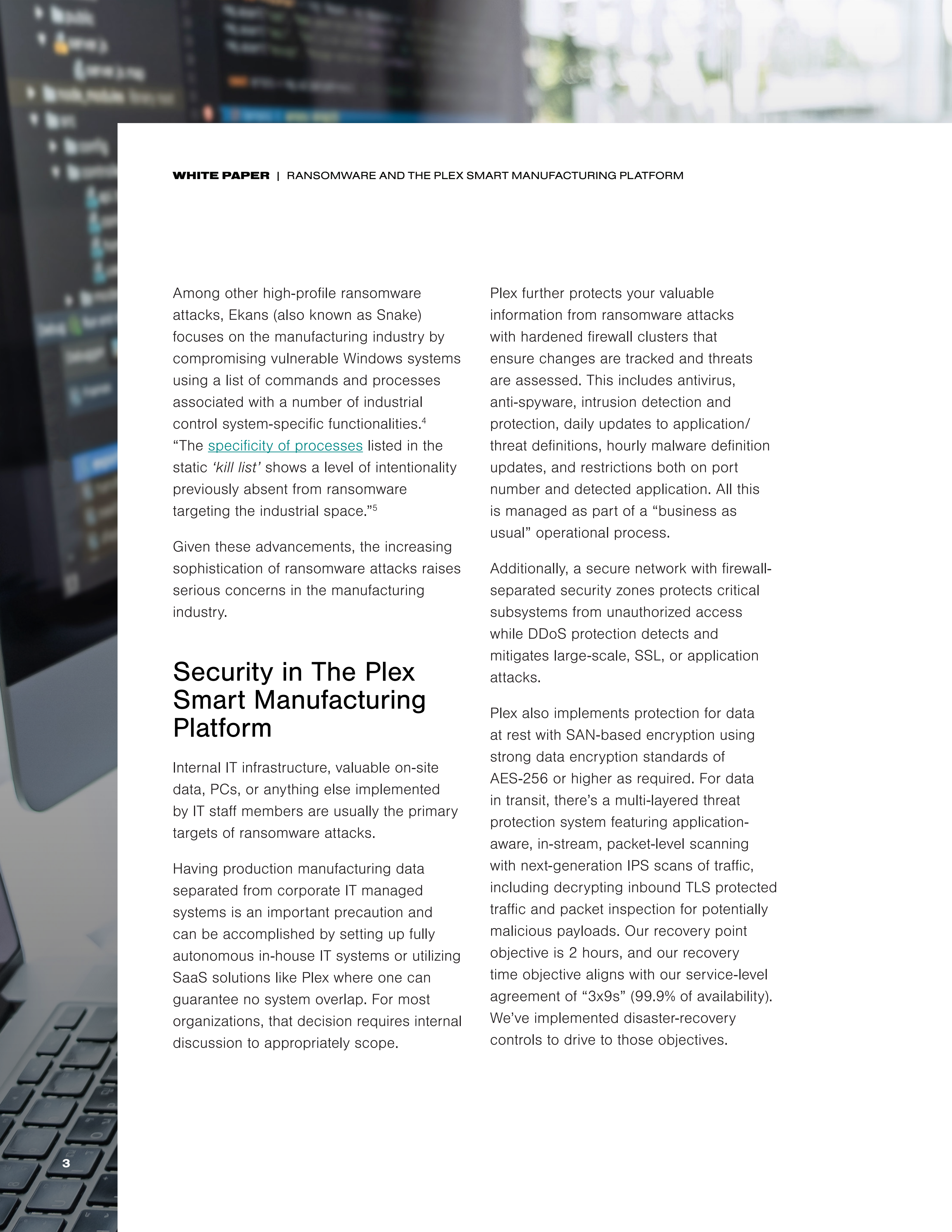
Ransomware has been around since 1998 and has since become the most pervasive type of cyber-attack since 2005.[1] Because bad actors receive a relatively high return on minimal investment, the number of ransomware attacks is increasing while their complexity continues to evolve.

Successful attacks can cost a company hundreds of thousands or even millions of dollars. Financial losses are counted in terms of billions of dollars per year in ransomware payments, and even more in recovery costs. Some forecasts indicate the damages could soon reach into the trillions. No longer just for highly sophisticated bad actors, ransomware-as-a-service means that even an untrained person can profit from ransomware attacks simply by buying a subscription to an attack service and sharing the ill-gotten profits with a ransomware service provider![2]

Fewer than a quarter of ransomware victims actually get their files back after paying up.[3]

Today's ransomware can do more than just encrypt critical data until a decryption key is purchased from the attacker; some attacks first look for user and admin credentials, remove or encrypt backups, and exfiltrate valuable data *before* it's encrypted, threatening the data owner with selling or publicly exposing the data if the ransom isn't paid or *even after the ransom has been paid*.

Ransomware is even being used as a cover for more damaging attacks. The term *"wiperware"* is used to describe the use of a simple ransomware attack, usually sent through a phishing email, that distracts the organization from a much more serious attack happening in the background.



Among other high-profile ransomware attacks, Ekans (also known as Snake) focuses on the manufacturing industry by compromising vulnerable Windows systems using a list of commands and processes associated with a number of industrial control system-specific functionalities.[4] "The specificity of processes listed in the static *'kill list'* shows a level of intentionality previously absent from ransomware targeting the industrial space."[5]

Given these advancements, the increasing sophistication of ransomware attacks raises serious concerns in the manufacturing industry.

Security in The Plex Smart Manufacturing Platform

Internal IT infrastructure, valuable on-site data, PCs, or anything else implemented by IT staff members are usually the primary targets of ransomware attacks.

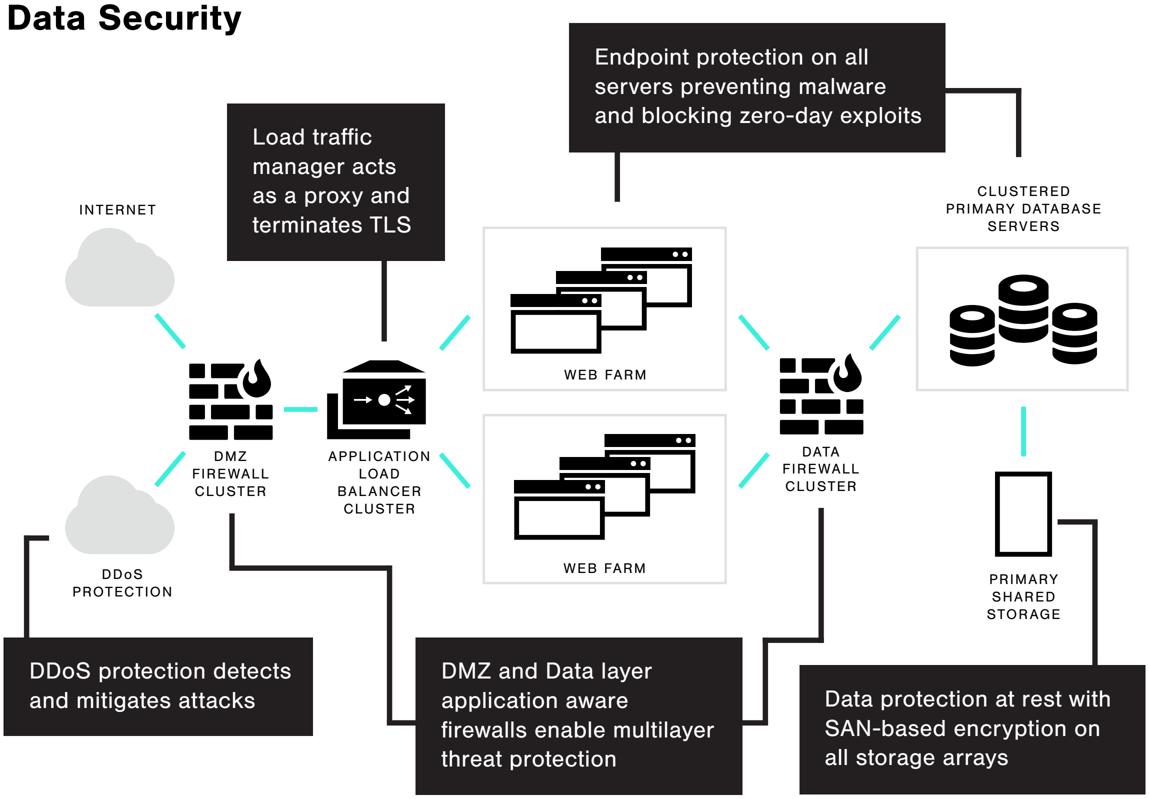
Having production manufacturing data separated from corporate IT managed systems is an important precaution and can be accomplished by setting up fully autonomous in-house IT systems or utilizing SaaS solutions like Plex where one can guarantee no system overlap. For most organizations, that decision requires internal discussion to appropriately scope.

Plex further protects your valuable information from ransomware attacks with hardened firewall clusters that ensure changes are tracked and threats are assessed. This includes antivirus, anti-spyware, intrusion detection and protection, daily updates to application/ threat definitions, hourly malware definition updates, and restrictions both on port number and detected application. All this is managed as part of a "business as usual" operational process.

Additionally, a secure network with firewall-separated security zones protects critical subsystems from unauthorized access while DDoS protection detects and mitigates large-scale, SSL, or application attacks.

Plex also implements protection for data at rest with SAN-based encryption using strong data encryption standards of AES-256 or higher as required. For data in transit, there's a multi-layered threat protection system featuring application-aware, in-stream, packet-level scanning with next-generation IPS scans of traffic, including decrypting inbound TLS protected traffic and packet inspection for potentially malicious payloads. Our recovery point objective is 2 hours, and our recovery time objective aligns with our service-level agreement of "3x9s" (99.9% of availability). We've implemented disaster-recovery controls to drive to those objectives.

Data Security



Endpoint protection on all servers preventing malware and blocking zero-day exploits

Load traffic manager acts as a proxy and terminates TLS

DDoS protection detects and mitigates attacks

DMZ and Data layer application aware firewalls enable multilayer threat protection

Data protection at rest with SAN-based encryption on all storage arrays

Other controls include

- Vulnerability, compliance, and patch-level scans are executed internally and externally continually.
- Data backups support recovery of production data at alternate site, restore of point-in-time archival data, and restore from immutable, secure snapshot.
- Daily third-party application vulnerability testing, weekly automated vulnerability testing, and biannual third-party manual network and application penetration testing provide an external view of our security.

Keeping Your Organization Protected

Today, most infections like ransomware are the result of phishing emails with links to malicious websites that infect a user's computer. Becoming infected by using Plex is unlikely due to the private cloud nature of Plex and our strong defense-in-depth strategy. Ransomware can also be propagated as a worm or a virus requiring always-on anti-malware and endpoint detection and response, which Plex has implemented.

The Plex Smart Manufacturing Platform and the data that resides in your Plex instance are highly secured with strong measures in place to prevent such cyber-attacks from happening. Plex accomplishes this robust security posture through a multi-layered, in-depth defense practice along with a strong auditing and compliance focus that ensures we follow all of our controls. In order to implement and maintain this level of security focus, Plex employs a dedicated security team made up of architects, engineers, managers, and a CSO.

Finally, while Plex provides the main line of defense for users of the platform, it's not the only one. Ransomware will target any vulnerability it can, seeking to take advantage of human errors. You can rest easy knowing Plex has your back, but you'll be even more protected by checking to make sure you're following a number of best practices that reduce the threat of ransomware.

[1] https://www.csoonline.com/article/3095956/the-history-of-ransomware.html
[2] https://www.zdnet.com/article/ransomware-as-a-service-for-allows-wannabe-hackers-to-cash-in-on-cyber-extortion/
[3] https://www.courant.com/opinion/op-ed/hc-op-kozloski-west-haven-cyber-hack-20181022-story.html
[4] https://www.zdnet.com/article/ransomware-attacks-are-now-targeting-industrial-control-systems/
[5] https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

ABOUT PLEX

Plex, by Rockwell Automation, is a leader in cloud-delivered smart manufacturing solutions, empowering the world's manufacturers to make awesome products. Our platform gives manufacturers the ability to connect, automate, track, and analyze every aspect of their business to drive transformation. The Plex Smart Manufacturing Platform™ includes solutions for manufacturing execution (MES), ERP, quality, supply chain planning and management, asset performance management, production monitoring, process automation and analytics to connect people, systems, machines and supply chains, enabling them to lead with precision, efficiency and agility. To learn more, visit **www.plex.com**

YOUR RANSOMWARE DEFENSE CHECKLIST

☑ Arm yourself with knowledge. There are countless whitepapers, seminars, and articles on ransomware that will help you defend your company.

☑ Implement stronger passwords and multi-factor authentication.

☑ Constantly review your access controls and privilege escalation with a "need-to-know" mentality.

☑ Segment your network. Don't leave all of your valuable eggs in the same basket.

☑ Secure your security systems as you would other highest-value systems.

☑ Run intrusion detection and anti-virus software and keep them up to date.

☑ Encrypt data at rest and wherever possible, in transit.

☑ Backup critical systems and data and secure them separately from everything else. For your most sensitive data, back it up to multiple locations.

☑ Patch. Many systems in industrial settings are aging, so weigh the cost of upgrading against the cost of recovering from an attack. Understand that a failure to act means you will eventually be breached.

☑ Discontinue use of vulnerable protocols like TLS 1.0/1.1 as well as older, less secure ciphers.

☑ Know your environment. Maintain up-to-date architectural diagrams and asset inventory so you can quickly determine what devices may be vulnerable or need patching.

☑ Build an aware and empowered workforce that knows how to handle suspicious emails or activities, has quick access to an expert security team, and actively looks for problems.